Comitê Gestor da Internet no Brasil

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

CONTRIBUIÇÃO TÉCNICA – BLOQUEIOS NO CONTEXTO DO ECA DIGITAL E DO DECRETO Nº 12.622/2025

Esta contribuição técnica discute a eficácia, os limites e os impactos técnicos, jurídicos e sociais das medidas de bloqueio de aplicações, serviços e conteúdos no contexto da implementação da Lei nº 15.211/2025 (ECA Digital) e de sua regulamentação pelo Decreto nº 12.622/2025. A partir da análise da arquitetura da Internet, de experiências nacionais e internacionais e dos riscos associados a diferentes modalidades de bloqueio, o documento examina as condições sob as quais tais medidas podem ser consideradas legítimas, proporcionais e tecnicamente adequadas. Ao final, apresentam se as recomendações do Comitê Gestor da Internet no Brasil (CGI.br) com vistas a orientar a implementação de ordens de bloqueio de forma fundamentada e alinhada às melhores práticas de governança da Internet, de modo a fortalecer a proteção de crianças e adolescentes sem comprometer a estabilidade da infraestrutura da Internet e os direitos fundamentais de terceiros.

1. Introdução

A implementação do ECA Digital estabelece um amplo conjunto de obrigações voltadas à proteção integral de crianças e adolescentes no ambiente digital. Entre essas obrigações, figuram dispositivos que, em caso de descumprimento reiterado das obrigações previstas na lei, podem resultar na determinação judicial de bloqueio de aplicações, produtos ou serviços digitais. O texto legal, em seu Art. 35, § 6º, prevê que:

> § 6º A suspensão temporária e a proibição de exercício das atividades previstas nos incisos III e IV do *caput* deste artigo, quando não implementadas diretamente pelo infrator, serão realizadas mediante ordem de bloqueio dirigida às prestadoras de serviços de telecomunicações que proveem conexão à internet, às entidades gestoras de pontos de troca de tráfego de internet, aos prestadores de serviços de resolução de nomes de domínio e aos demais agentes que viabilizam a conexão entre usuários e servidores de conteúdo na internet.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

O Decreto nº 12.622/2025, ao regulamentar parcialmente o ECA Digital, detalha as instâncias responsáveis pela execução dessas medidas de bloqueio de aplicações, determinando que ordens judiciais de bloqueio sejam operacionalizadas pela Anatel e pelo CGI.br, cada qual no âmbito de suas competências. Nos termos do referido decreto, caberá à Anatel a distribuição das ordens às prestadoras de serviços de telecomunicações e a outros agentes que viabilizam a conexão à Internet, e ao CGI.br o recebimento de ordens relacionadas à resolução de nomes (DNS) registrados sob o domínio ".br". O decreto também faculta às duas instituições a definição da técnica mais adequada para a implementação dessas medidas. Nos termos da Lei, atribuiu-se ao Poder Judiciário a competência para determinar bloqueios de aplicações nos casos de descumprimento do ECA Digital e, ao CGI.br e à Anatel, a responsabilidade pela execução dessas ordens.

Importante considerar que o bloqueio de aplicações, serviços ou conteúdos no ambiente digital pode constituir, em situações excepcionais, um instrumento legítimo para enfrentar violações graves e reiteradas aos direitos de crianças e adolescentes, especialmente quando outras medidas menos invasivas se mostrarem insuficientes para cessar práticas ilícitas ou abusivas.

O ECA Digital representa um avanço normativo ao reconhecer expressamente o caráter excepcional, temporário e condicionado das medidas de bloqueio, vinculando sua adoção à observância da necessidade e da proteção integral de crianças e adolescentes. Porém, é relevante destacar que o reconhecimento da legitimidade do bloqueio em hipóteses estritas não afasta a necessidade de rigor técnico, cautela, avaliação prévia de impactos e transparência, a fim de assegurar que tais medidas efetivamente contribuam para a proteção de crianças e adolescentes sem produzir danos colaterais desproporcionais à infraestrutura da Internet, a serviços essenciais e a direitos fundamentais de terceiros. Importante, portanto, compreender que **ordens de bloqueio devem ser entendidas como medidas extremas e que cumpri-las de modo a minimizar efeitos (danos) colaterais** que contrariem o objetivo da decisão é tarefa altamente complexa. Trata-se de uma intervenção de última instância, cuja adoção exige demonstrar que alternativas menos invasivas foram tentadas e se mostraram insuficientes, dada a limitada granularidade técnica dos mecanismos de bloqueio e o elevado risco de impactos não intencionais sobre serviços legítimos.

Essa complexidade decorre de princípios fundamentais da arquitetura da **Internet**[1], o que permite a composição de **uma rede altamente resiliente, distribuída, descentralizada e composta por múltiplos pontos de acesso e interconexão**, mantidos por diferentes agentes privados, nacionais e internacionais e com capacidades técnicas distintas. Não existe um ponto único de controle central da Internet, e diferentes camadas e recursos da infraestrutura, como

1 https://principios.cgi.br/

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

provedores de acesso, servidores DNS recursivo e autoritativo, PTT (Ponto de Troca de Tráfego) ou IXs (Internet Exchange)[2], CDNs (Redes de Distribuição de Conteúdos)[3], dentre outros, são afetados, inevitavelmente, de maneiras diversas por tentativas de bloqueio, inclusive de difícil previsibilidade.

Outrossim, é importante destacar que os **Sistemas Autônomos** que compõem a Internet no Brasil são geridos e configurados de formas fundamentalmente distintas, de acordo com as capacidades e os modelos de negócio das organizações gestoras desses Sistemas Autônomos, o que pode reduzir significativamente a eficiência e eficácia de ordens de bloqueio padronizadas e demasiadamente específicas. Dentre os aproximadamente 9 mil gestores de rede de Sistema Autônomos registrados[4] no Brasil, há diferenças quanto ao porte, à disponibilidade de equipamentos de rede, ao tamanho e à qualificação de equipes técnicas, entre outras. Adicionalmente, há provedores de serviços de Internet que não são gestores de Sistemas Autônomos e, por isso, tem autonomia ainda mais limitada quanto à implementação de ordens de bloqueio. Essa heterogeneidade operacional amplia o risco de resultados inconsistentes, fragmentação de comportamentos de rede e impactos divergentes entre regiões ou operadores, dificultando a previsibilidade e a efetividade das medidas.

Um bloqueio tecnicamente adequado deve ser capaz de alcançar a finalidade específica da ordem, ser executado pelos agentes que dispõem de capacidade técnica para tal, sempre orientados pelo princípio fundamental da minimização dos efeitos colaterais sobre usuários, empresas e órgãos públicos que não têm relação com o ilícito e sobre a própria infraestrutura da Internet. Casos concretos de bloqueios de aplicações ocorridos no passado ilustram o potencial social e economicamente danoso da prática e expõem a assimetria entre a intenção de decisões judiciais e seus efeitos sociotécnicos quando não determinados e executados adequadamente[5]. Adicionalmente, é essencial que a devida transparência tanto das ordens

---

2 https://ix.br/sobre

3 https://nic.br/noticia/na-midia/cdn-e-o-caminho-para-melhorar-a-experiencia-do-usuario-em-grandes-transmissoes-online-dizem-especialistas/

4 https://nic.br/noticia/na-midia/no-brasil-50-4-do-trafego-internet-esta-rodando-em-ipv6/

5 Um dos casos mais emblemáticos e notórios ocorreu em 2007, quando uma decisão judicial determinou a indisponibilização integral do YouTube no Brasil até que fossem removidos vídeos envolvendo a apresentadora Daniela Cicarelli. A ordem judicial, além de impossível de cumprir uma vez que o conteúdo já havia se espalhado na Internet de forma incontrolável, gerou efeitos colaterais altamente prejudiciais, resultando em milhões de usuários e empresas prejudicados pela indisponibilização da plataforma sem terem qualquer relação com o caso. Além disso, ao contrário do que se almejava com a ordem judicial (indisponibilizar o conteúdo), o conteúdo ganhou enorme visibilidade, culminando no efeito inverso ao desejado. À época, a situação tornou-se tão danosa que o próprio Tribunal de Justiça competente revisou a decisão, reconhecendo expressamente que o bloqueio de uma aplicação inteira (neste caso, o acesso ao Youtube no Brasil) produzia danos sociais elevados que não justificavam a medida.
Casos mais recentes confirmam que os bloqueios continuam a gerar impactos colaterais severos. Em 2022, a ordem judicial de bloqueio do Telegram resultou em interrupções de serviços de terceiros hospedados na

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

emitidas, quanto das medidas técnicas adotadas pelos provedores de serviços Internet para implementação das ordens seja garantida para a efetiva prestação de contas e controle social, especialmente considerando o potencial impacto direto de ordens de bloqueio no funcionamento de aplicações e da própria Internet.

Importante mencionar que bloqueios de aplicações, serviços e conteúdos produzem impactos sobre direitos[6]. Há muito a Internet deixou de ser apenas um meio de comunicação e entretenimento, tornando-se uma infraestrutura indispensável para uma série de atividades essenciais, como trabalho, educação, acesso a serviços públicos, acesso à informação, dentre outras. Medidas de bloqueio, sobretudo quando afetam milhões de usuários alheios à conduta que se pretende coibir, configuram elevado risco potencial de violação de direitos fundamentais. Experiências internacionais, trazidas no *Policy Brief: Internet Shutdowns*[7] *d*a Internet Society, demonstram que medidas de restrição de acesso à Internet, incluindo bloqueios de aplicações, têm potencial elevado de serem desproporcionais e incompatíveis com os parâmetros do Art. 19 (3) do Pacto Internacional sobre Direitos Civis e Políticos e com resoluções do Conselho de Direitos Humanos da ONU[8]. Embora o ECA Digital trate de medidas pontuais e tecnicamente delimitadas, é imprescindível que sua regulamentação evite reproduzir a lógica mais ampla das chamadas "paralisações da Internet", cuja adoção tem sido reiteradamente desaconselhada no plano internacional por seus efeitos colaterais severos e baixa efetividade.

Também é necessário assegurar que **medidas de bloqueio tenham duração estritamente limitada, sejam periodicamente reavaliadas e cessem tão logo a causa motivadora desapareça**, evitando que permaneçam em vigor após o conteúdo ter sido removido ou deslocado.

Por fim, bloqueios de aplicações promovem um efeito de migração de usuários para aplicações alternativas, ou hospedadas fora do Brasil. Além disso, podem incentivar o uso de ferramentas como VPNs, *resolvers* alternativos ou serviços informais, muitas vezes desprovidos de proteção

---

mesma infraestrutura técnica, uma vez que o bloqueio envolveu endereços IP e recursos compartilhados. Como consequência, aplicações e serviços totalmente legítimos foram bloqueados, evidenciando o risco de medidas de bloqueios de aplicações em ambientes técnicos interdependentes. Importante considerar os danos econômico e social dos bloqueios de aplicações, trazendo prejuízos também expressivos, como ocorreu no bloqueio do WhatsApp em 2015, que atingiu mais de 100 milhões de usuários, muitos deles dependentes do serviço para trabalho, atendimento a clientes, pequenos e grandes negócios e comunicações, causando perdas econômicas de grande escala.

6 https://www.internetsociety.org/resources/policybriefs/2025/internet-shutdowns/

7 https://www.internetsociety.org/resources/policybriefs/2025/internet-shutdowns/

8 https://brasil.un.org/pt-br/57521-o-comit%C3%AA-de-direitos-humanos-da-onu-e-liberdade-de-opini%C3%A3o-e-de-express%C3%A3o

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

adequada. Tal migração pode direcionar usuários, inclusive crianças e adolescentes, para plataformas menos seguras, sem moderação, sem mecanismos de supervisão parental, sem cumprimento da Lei Geral de Proteção de Dados, ou mesmo para ambientes que não cooperam com autoridades brasileiras.

Bloqueios de aplicações são medidas que podem ser necessárias e o CGI.br reconhece a importância de sua aplicação em situações específicas. Saudamos a inclusão da medida no ECA Digital por entender sua importância para a proteção de diretos de crianças e adolescentes quando aplicado em consonância com princípios legais e técnicos. Contudo, é papel do Comitê destacar que se trata de **medida tecnicamente complexa que pode gerar efeitos indesejados e danosos, que deve ser aplicada apenas em situações excepcionais, com base em análises técnica e de impactos prévias** para possibilitar a ciência dos efeitos indesejados que acompanham os bloqueios. Essa avaliação deve ser documentada e, idealmente, considerar cenários de falha, prever mecanismos de monitoramento contínuo e contemplar plano de reversão rápida caso os impactos não previstos venham a ocorrer.

Ressalta-se que o CGI.br tem atuado sempre de forma colaborativa e técnica para o aprimoramento da governança da Internet no país, incluindo a cooperação com o Poder Judiciário e demais autoridades competentes, com vistas à implementação de ordens judiciais, especialmente quando envolvem medidas excepcionais como o bloqueio de aplicações, serviços ou conteúdos. Essa cooperação técnica busca não apenas viabilizar o cumprimento das ordens expedidas, mas também contribuir para a efetividade das decisões judiciais, reduzir riscos de inexequibilidade técnica, minimizar efeitos colaterais indesejados e preservar a estabilidade, a segurança e a integridade da infraestrutura da Internet, em consonância com os princípios do ECA Digital e da proteção integral de crianças e adolescentes.

Nesse sentido, o CGI.br apresenta esta contribuição técnica, com o objetivo de expor esclarecimentos sobre a aplicação de medidas de bloqueio, à luz das melhores práticas nacionais e internacionais, promovendo a proteção de crianças e adolescentes sem comprometer o funcionamento da Internet e os direitos fundamentais de terceiros.

2. A eficácia de bloqueios de aplicação

Estudos técnicos consolidados, como os apresentados pela RFC 7754 do IETF, *Technical Considerations for Internet Service Blocking and Filtering*[9], reforçam que mecanismos de bloqueio implementados na infraestrutura da Internet, pela manipulação de tráfego, de rotas

9 https://datatracker.ietf.org/doc/html/rfc7754

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

ou de sistemas de resolução de nomes, acarretam limitações estruturais de eficácia e geram elevado risco de danos colaterais. Segundo o documento, bloqueios baseados em infraestrutura podem afetar serviços legítimos que compartilham a mesma infraestrutura e introduzem fragilidades adicionais ao ecossistema, inclusive ao comprometer a segurança ponta a ponta de protocolos. A RFC 7754 conclui que, na arquitetura da Internet, medidas impositivas de bloqueio devem ser consideradas como alternativas de último recurso.

Adicionalmente, **a arquitetura da Internet impõe limitações técnicas para a implementação eficiente de bloqueios**. É essencial compreender que bloqueios tendem a gerar apenas degradação parcial do serviço, o que pode ser eficaz para impedir o acesso para quase a integralidade dos usuários, mas é importante ressaltar que parte minoritária continuará acessando por rotas alternativas. A expectativa de que um bloqueio de aplicações impeça integralmente o acesso a uma aplicação ou serviço na Internet pode gerar determinações de bloqueio inexequíveis, com impactos amplos e injustificáveis. Além disso, mudanças frequentes na infraestrutura utilizada por aplicações modernas, como CDNs, balanceamento dinâmico e migração rápida de serviços para novos endereços, tornam a ação de bloqueio instável, sujeita a perda de eficácia em períodos muito curtos e exigindo atualizações constantes. Esse comportamento dinâmico contribui para que bloqueios ora efetivos se tornem rapidamente obsoletos, sem produzir o efeito esperado.

2.1. Determinações de bloqueio a pontos de troca de tráfego (Internet Exchange Points – IXPs)

Solicitações de bloqueio a pontos de troca de tráfego são ineficazes e geram impactos sobre toda a Internet, comprometendo o funcionamento estável da sua infraestrutura. IXP (do acrônimo em inglês *Internet Exchange Point* ou, em português, Pontos de Troca de Tráfego – PTT) é uma infraestrutura onde diferentes redes de Internet, chamadas Sistemas Autônomos (ASNs), interligam-se para trocar tráfego de forma direta. Funciona como um ponto físico de interligação entre roteadores (equipamentos capazes de encaminhar os pacotes de dados) de diversas redes diferentes. É uma infraestrutura de interligação para a Internet, que opera dentro de um *data center* ou de um conjunto deles. Dessa forma, IXPs não possuem nenhuma visibilidade sobre o conteúdo disponibilizado nem capacidade (competência) de filtrar URLs específicas ou contas. A atuação do IX.br – iniciativa do CGI.br e do NIC.br de implantar e operar pontos de troca de tráfego Internet em diversas regiões metropolitanas no Brasil – limita-se ao encaminhamento eficiente de pacotes entre Sistemas Autônomos. Trata-se de uma camada neutra da infraestrutura da Internet, responsável apenas pela entrega técnica de pacotes entre redes, sem qualquer ingerência sobre o conteúdo transportado.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

O acesso à camada IP nesses ambientes é restrito à operação dos chamados *route servers*, equipamentos que facilitam o estabelecimento de sessões BGP (o protocolo usado para troca de rotas entre redes). *Route servers* simplificam a comunicação entre os participantes, mas seu uso não é obrigatório: cada participante pode, se preferir, estabelecer sessões BGP diretas (bilaterais) com outros, sem passar pelos *route servers*. Aliás, muitos participantes da estrutura do IXP preferem estabelecer sessões bilaterais diretas, nas quais negociam entre si o tráfego que irão trocar. Nesse tipo de configuração, o gestor do IXP não tem qualquer ingerência e não consegue aplicar bloqueios de suspensão temporária, mas tão somente fazer a desconexão física de um participante inteiro (literalmente desligar participantes inteiros e, portanto, não apenas o serviço, produto ou conteúdo alvo da decisão judicial de bloqueio). Aplicar bloqueios via *route servers* jamais atingiria o tráfego integral do IX (ou PTT), pois parte relevante das trocas pode ocorrer por acordos bilaterais independentes.

O desligamento integral de participantes é medida extrema que impactaria a confiança no modelo de troca de tráfego na internet gerando efeitos imprevisíveis. Além disso, é importante frisar que as redes na Internet se interligam por diversos caminhos diferentes. Um IXP, por sua natureza, nunca é a única rota disponível para os pacotes de dados trafegarem entre duas redes. O desligamento de um participante pode degradar o acesso às suas redes e aplicações, mas não impede totalmente a comunicação, já que existem rotas alternativas ao IXP. Já a interferência no *route server* pode ser inefetiva, pois seu uso é opcional e muitos participantes trocam tráfego por sessões bilaterais. Em ambos os casos, **há risco de afetar tráfego legítimo de terceiros sem alcançar o bloqueio pretendido**.

O bloqueio de aplicações nesse nível pode resultar na interrupção ou degradação de serviços essenciais, atingindo usuários, empresas, provedores de acesso e órgãos públicos em todo o país, afetando a interoperabilidade geral da rede e a confiança em um sistema que é todo baseado na cooperação. Por essa razão, medidas direcionadas a IXPs frequentemente acabam estimulando a fragmentação da Internet, enfraquecendo propriedades estruturais como resiliência e redundância, que dependem da neutralidade e estabilidade desses pontos de troca.

2.2 Determinações de Bloqueio a Provedores de Conexão (ISPs)

Determinações judiciais de bloqueios baseados em endereços IP ou blocos inteiros de sistemas autônomo, endereçadas a provedores de conexão ou *Internet Service Providers* (ISPs), em inglês, são instrumentos utilizados em determinadas situações. Contudo, apesar de parecerem tecnicamente simples, são medidas complexas que podem gerar impactos amplos e trazer riscos significativos ao funcionamento da rede, a depender de como são solicitadas e implementadas.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Embora ISPs consigam implementar bloqueios no plano de dados, visto que operam roteadores na camada IP, o problema central é a falta de granularidade. Hoje, **um único endereço IP pode hospedar centenas de sites e serviços distintos.** Isso ocorre porque, com o uso de CDNs (*Content Delivery Networks* – Redes de Distribuição de Conteúdos), infraestruturas de nuvem e protocolos modernos, múltiplos domínios e aplicações são servidos a partir de um mesmo endereço IP, ou a partir do mesmo conjunto de endereços IP; o servidor distingue qual serviço entregar apenas após a negociação criptografada no início da conexão.

Como consequência, um mesmo IP pode abrigar desde serviços bancários até aplicações de *e-commerce* ou redes sociais. Bloquear um IP para atingir um único alvo pode resultar na suspensão simultânea e indesejada de múltiplas aplicações legítimas. Além disso, **endereços e rotas associados a aplicações podem mudar rapidamente**, exigindo atualizações frequentes nas listas de bloqueio, o que aumenta a complexidade operacional, reduz a previsibilidade do efeito e compromete a estabilidade da rede.

Destacamos também que listas cumulativas de bloqueios de IPs não escalam bem, porque exigem inserção constante de regras em roteadores e *firewalls* e, consequentemente, consomem recursos valiosos de processamento e memória, aumentam custos operacionais dos ISPs e degradam o desempenho da rede para todos os usuários. Com o aumento da complexidade dessas listas, cresce também o risco de erros de configuração e de impactos acidentais sobre serviços essenciais, ampliando ainda mais os efeitos colaterais indesejados.

2.3 Solicitação de Bloqueios via DNS

Os bloqueios via DNS (*Domain Name System*) tanto em servidores recursivos (nos provedores de conexão), quanto em servidores autoritativos (como o Registro.br ou registradores de *Top Level Domains* – TLDs), precisam considerar seus efeitos amplos, pois **atingem domínios inteiros ou zonas completas**. Em termos práticos, **a suspensão de um nome de domínio no .br implica a indisponibilização integral de todos os serviços atrelados àquele domínio, não apenas de páginas específicas** que contenham algum conteúdo ilegal.

Hipoteticamente, uma ordem judicial de suspensão do domínio “mj.gov.br” para remover uma URL com conteúdo ilegal ou inadequado tornaria inacessível não apenas o site institucional integral do Ministério da Justiça e Segurança Pública, mas também todos os endereços de e-mail terminados em “@mj.gov.br” e subdomínios (por exemplo, o “dados.mj.gov.br”), impactando eventuais serviços ao cidadão atrelados a esse nome de domínio, como o acesso a repositórios de dados externos por servidores e entidades públicas que necessitam dessas informações.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Ao tentar resolver um problema pontual via intervenção no DNS, abre-se a porta para **falhas de segurança, efeitos colaterais em serviços legítimos, fragmentação e perda de confiança** em um dos pilares técnicos da rede, acarretando riscos sérios ao funcionamento da Internet, a saber:

- Quebra da cadeia de confiança do DNSSEC – O DNSSEC é um conjunto de extensões de segurança que garante, via criptografia, que a resposta de um servidor DNS não foi adulterada. Quando um resolvedor é forçado a bloquear ou alterar respostas, ele quebra essa validação: ou ignora assinaturas válidas (violando o protocolo), ou passa a enviar respostas inconsistentes que fazem os clientes rejeitarem a resolução. Isso compromete a segurança global do DNS e mina a confiança dos usuários.

- Bloqueio nos registradores/resolvedores autoritativos – Também se cogita ordenar bloqueios diretamente aos registradores (*registrars*)[10], que gerenciam os domínios em nível autoritativo. Mas essa medida só permite remover completamente o domínio da zona ou redirecioná-lo para outro destino. Não há granularidade: o domínio inteiro é afetado, ainda que apenas uma parte do conteúdo seja considerada ilícita. Além disso, bloquear um domínio não elimina o conteúdo nem impede necessariamente o seu acesso, tendo em vista que tal conteúdo pode estar disponível por meio de outros nomes alternativos. É importante destacar ainda que, no caso de domínios hospedados em registradores internacionais, fora da jurisdição brasileira, tais ordens podem não ser atendidas tempestivamente ou não ser plenamente cumpridas, seja por questões de dificuldades naturais da cooperação internacional seja por questões operacionais.

- Fragmentação e fuga para resolvedores externos – bloqueios recorrentes solicitados aos provedores de conexão incentivam usuários e aplicações a migrarem para serviços externos de resolução (1.1.1.1, 8.8.8.8), inclusive se valendo de transporte criptografado via DoH/DoT, dificultando a gestão nacional e gerando uma Internet fragmentada, onde cada grupo de usuários vê uma "versão" diferente da rede.

Além desses aspectos, bloqueios via DNS frequentemente permanecem ativos mesmo após o conteúdo ser movido para outro domínio ou removido da Internet, gerando um estado prolongado de indisponibilidade sem benefício prático. A manutenção desse tipo de bloqueio por longos períodos aumenta riscos de efeitos colaterais, incentiva usuários a recorrerem a "*resolvers*" alternativos ou inseguros e compromete a uniformidade da experiência de navegação.

[10] Entidade que oferece serviços de registro de nomes de domínio para registrantes (clientes) em domínios de topo, sejam eles genéricos (gTLDs) ou de código de páis (ccTLDs). https://www.icann.org/en/icann-acronyms-and-terms?nav-letter=r&page=1.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Essas importantes considerações técnicas, jurídicas e operacionais buscam aprimorar a eficiência técnica e a adequação da ordem ao objetivo almejado, dado que podem produzir riscos significativos de danos colaterais. Deve-se considerar, ainda, a necessidade de reavaliações periódicas, de forma a garantir que bloqueios não permaneçam em vigor além do estritamente necessário.

3. Medidas proporcionais, subsidiárias e transparentes (recomendação das medidas progressivas)

A adoção de medidas de bloqueio de conteúdos, aplicações ou serviços no âmbito do ECA Digital deve observar rigorosamente o princípio da proporcionalidade e da subsidiariedade, além dos efeitos colaterais e ineficiências, fundamentais para assegurar que qualquer ordem judicial seja tecnicamente adequada, juridicamente plausível e socialmente responsável. Medidas que geram menos impactos ao ecossistema da Internet e sejam mais eficazes em relação ao que se almeja são capazes de alcançar o objetivo legítimo de cumprimento do ECA Digital, evitando-se excessos e impactos desnecessários.

A proporcionalidade entre o objetivo almejado, a medida de bloqueio pretendida e seus efeitos colaterais exige que tal medida seja dotada de fundamento técnico suficiente para atingir o fim proposto, incluindo reconhecer que certas modalidades de bloqueio podem não ser efetivas para impedir acesso a conteúdos ou funcionalidades específicas. Além disso, deve ser adequada de forma que os resultados esperados justifiquem a ordem após feita uma análise de custo benefício considerando eventuais impactos negativos sociais, tecnológicos e econômicos associados ao bloqueio. Também se exige que a medida seja limitada ao menor escopo técnico possível, evitando qualquer forma de intervenção mais ampla do que o necessário e prevenindo sobrebloqueios que afetem aplicações ou serviços não relacionados ao objeto da ordem.

A subsidiariedade, por sua vez, determina que medidas de maior impacto, como os bloqueios de aplicação, suspensão de domínios ou quaisquer restrições que afetem serviços, somente sejam admitidas após esgotadas todas as demais alternativas menos invasivas. Isso implica adotar uma escala progressiva de atuação, que inicia com a adoção de medidas sobre o conteúdo na sua origem e aplicações de penalidades, e somente ao final, se todas as anteriores forem esgotadas, adotar mecanismos de bloqueio. Essa lógica progressiva deve incluir ainda a demonstração explícita de que a intervenção técnica não apenas é necessária, mas também temporária, sujeita a revisão periódica e capaz de ser revertida prontamente caso cause impactos indevidos ou deixe de ser justificável.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Assim, antes de qualquer medida de bloqueio de aplicações através da incidência técnica na infraestrutura da Internet, é recomendado realizar avaliação dos riscos trazidos pelo bloqueio e dos seus efeitos (danos) colaterais, com uma análise técnica que esclareça o grau de eficácia e os impactos da medida pretendida. Essa avaliação deve ser formalizada, incluir análise de cenários de falha, delimitar mecanismos de mitigação e prever indicadores de monitoramento contínuo para detecção de efeitos adversos. A ausência dessa avaliação cria incerteza e pode resultar em medidas desproporcionais, ineficazes ou excessivamente prejudiciais.

Somente com a ciência do grau de efetividade e dos impactos da medida e, ainda, restando comprovado que outras medidas menos invasivas sobre a infraestrutura da Internet foram tentadas e restaram-se infrutíferas, é que se pode cogitar (com a devida cautela) medidas de bloqueios de aplicações. Além disso, deve-se garantir que qualquer medida adotada tenha prazo claramente delimitado, evitando a permanência de bloqueios que já não produzem efeito útil ou que, por inércia, continuem causando danos colaterais.

Além disso, destacamos um ponto relevante sobre a transparência na realização de bloqueios. Medidas de bloqueio, conforme mencionado, tem grande potencial de produzir efeitos que ultrapassam o caso concreto, atingindo usuários, empresas, serviços públicos e a própria estabilidade da Internet, razão pela qual devem observar padrões mínimos de transparência. A publicidade adequada de ordens de bloqueios e dos bloqueios em si permite que: operadores compreendam o escopo da ordem; que usuários sejam informados sobre os motivos de indisponibilidades de conteúdos, serviços ou produtos; e que a sociedade exerça controle democrático sobre medidas excepcionalmente restritivas, garantindo motivação clara, previsibilidade e a identificação prévia de riscos de sobrebloqueio ou falhas de implementação. Destaca-se que as autoridades responsáveis pela emissão das ordens de bloqueios devem produzir relatórios sistemáticos de externalidades indesejadas e não previstas geradas por tais medidas para garantir o controle social e o aprimoramento continuo dessas iniciativas. Nesse sentido, a documentação das ordens e as análises permanentes de efeitos esperados e externalidades negativas é condição para promover a transparência em medidas de bloqueio de aplicações e a confiança no ambiente digital.

Atualmente, ordens de bloqueios, sejam judiciais sejam administrativas, não costumam ser comunicadas aos usuários finais, tampouco publicizadas à sociedade. A ausência de transparência quanto à realização de bloqueios e aos motivos que os fundamentam aumenta a probabilidade de erros operacionais, gera inconsistências entre redes, favorece a manutenção de bloqueios além do necessário e, ainda, deixa os usuários sem justificativa alguma sobre indisponibilidades de acessos, ampliando, inclusive, impactos negativos sobre serviços legítimos. A divulgação da informação quanto à ordem que justificou o bloqueio pelos responsáveis pela sua execução contribui para que o bloqueio permaneça excepcional, temporário e sujeito a controle social, além de não deixar usuários sem informações.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

4. Recomendações

A análise apresentada evidencia que medidas de bloqueio de aplicações, serviços ou conteúdos no contexto do ECA Digital são complexas e que a implementação delas pode gerar altíssimo impacto ao ecossistema da Internet.

Considerando que:

- o bloqueio de aplicações, serviços ou conteúdos é um instrumento legítimo para coibir violações graves e reiteradas aos direitos de crianças e adolescentes;
- a arquitetura da Internet é distribuída, descentralizada e resiliente, composta por múltiplos agentes, camadas técnicas e modelos operacionais heterogêneos, o que impõe limitações estruturais à eficácia e à previsibilidade de medidas de bloqueio, especialmente quando direcionadas à infraestrutura de rede, como provedores de conexão, sistemas de resolução de nomes, CDNs ou pontos de troca de tráfego;
- experiências nacionais e internacionais demonstram que bloqueios de aplicações, quando adotados sem adequada fundamentação técnica e avaliação prévia de impactos, tendem a produzir sobrebloqueios, degradação de serviços essenciais, incentivos à migração para ambientes menos seguros e resultados desproporcionais em relação ao objetivo de proteção pretendido;
- medidas de bloqueio podem gerar efeitos colaterais não previstos, como o estímulo ao uso indiscriminado e até ilícito de VPNs e resolvedores alternativos, e a exposição de crianças e adolescentes a ambientes digitais com menores salvaguardas de segurança, privacidade e proteção de dados;
- o bloqueio de aplicações constitui medida de elevado impacto econômico, técnico, social e jurídico, cuja implementação envolve riscos significativos de efeitos colaterais não intencionais, podendo afetar serviços legítimos, usuários alheios à conduta ilícita, direitos fundamentais de terceiros e a própria estabilidade da infraestrutura da Internet;

O CGI.br recomenda:

1. que o bloqueio de aplicações e serviços seja tratado como **medida excepcional, em decorrência de suas consequências e efeitos colaterais, temporária e condicionada, em observância aos princípios da proteção integral, da necessidade e da proporcionalidade;**

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

2. **a adoção prévia e progressiva de medidas menos invasivas em consonância com os princípios da subsidiariedade e da adequação técnica.** Nesse sentido, é essencial que eventual regulação afirme, de modo explícito, que bloqueios de aplicações ou serviços, somente podem ser adotados após esgotadas todas as alternativas menos gravosas;

3. **que medidas de bloqueio sejam dirigidas aos respectivos responsáveis e/ou provedores de serviços Internet adequados,** considerando a diversidade do ecossistema digital brasileiro, evitando direcionamento a atores que não possuem capacidade técnica para cumprir tais medidas;

4. **que medidas de bloqueio de aplicações e serviços tenham duração estritamente limitada,** sejam periodicamente reavaliadas e cessem tão logo a causa motivadora desapareça, evitando que permaneçam em vigor por tempo indeterminado;

5. **que medidas de bloqueio de aplicações e serviços sejam amparadas por análise técnica prévia e justificativa fundamentada, avaliação sobre eficácia e impactos, identificação do ponto da infraestrutura capaz de cumprir a ordem de forma eficaz e com menos impactos.** Essa análise deve ser formalizada, deve disponibilizar elementos verificáveis e incluir, sempre que possível, estimativas de riscos, cenários de falha e plano de monitoramento e reversão. Com isso, é possível aprimorar medidas de bloqueio para que sejam capazes de alcançar a finalidade específica da ordem judicial, sejam endereçadas para a execução por agentes que dispõem de capacidade técnica para tal, sempre orientados pelo princípio fundamental da minimização dos efeitos colaterais, e sejam acompanhadas por estudos técnicos que fundamentem sua implementação;

6. **que a aplicação de medidas de bloqueio no âmbito do ECA Digital observe padrões mínimos de transparência e publicidade, compatíveis com seu caráter excepcional e temporário.** As informações sobre os dados dos processos judiciais que emanaram as ordens de bloqueio, bem como os bloqueios efetivamente ordenados, devem ser devidamente publicizados, de modo a permitir que operadores compreendam o escopo da determinação, que usuários sejam informados sobre os motivos da indisponibilidade de conteúdos, serviços ou aplicações para que a sociedade possa exercer controle democrático sobre eventuais medidas restritivas de direitos;

7. **que as autoridades públicas responsáveis pela emissão das ordens de bloqueios produzam relatórios sistemáticos de externalidades negativas e não previstas geradas por tais medidas**, e que tais relatórios sejam publicizados para o acompanhamento público;

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

8. **que o Poder Judiciário, sempre que necessário, consulte previamente o CGI.br, de modo a receber orientação técnica sobre os mecanismos disponíveis e efetivos, seus limites e potenciais impactos para o ecossistema da Internet.** Essa cooperação técnica contribui para que ordens judiciais sejam eficazes, evitando efeitos colaterais indesejados e garantindo alinhamento às melhores práticas nacionais e internacionais de governança da Internet. Sugere-se também que essa consulta inclua avaliação de alternativas menos invasivas e que seja documentada no processo decisório.

O CGI.br, no âmbito de sua missão institucional, atua de forma colaborativa com o Poder Judiciário e demais autoridades competentes, a fim de orientar sobre as melhores práticas para a implementação de ordens judiciais, especialmente quando envolvem medidas excepcionais como o bloqueio de aplicações, de serviços ou de conteúdos. Ressalta-se que a efetiva proteção de crianças e adolescentes no ambiente digital deve ser garantida e promovida de modo a conciliar a tutela de direitos com a preservação da funcionalidade, segurança, estabilidade e integridade da Internet, evitando intervenções desproporcionais ou tecnicamente inadequadas.