



O PAPEL DA ANATEL

Guia sobre Bloqueio de Sites, Aplicativos e Conteúdos na Internet

Guia Sobre Bloqueio de Sites, Aplicativos e Conteúdos na Internet

Agência Nacional de Telecomunicações
SAUS Quadra 06, Blocos C, E, F e H
CEP 70.070-940 - Brasília/DF
Tel.: (61) 2312-2000 – www.gov.br/anatel

Presidente

Carlos Manuel Baigorri

Conselho Diretor

Alexandre Reis Siqueira Freire
Octavio Penna Pieranti
Edson Holanda
Nilo Pasquali

Superintendente de Fiscalização (SFI)

Gesiléia Fonseca Teles



SUMÁRIO

1. INTRODUÇÃO	4
1.1 Premissas e Fundamentos Legais	5
2. CONCEITOS BÁSICOS DA INTERNET	6
2.1 O que é Endereço IP	7
2.2 O que é um domínio?	8
2.3 O que é DNS?	8
2.4 O que é URL?	9
2.5 Relação entre os elementos	10
3. O PAPEL DA ANATEL: COMPETÊNCIAS, LIMITES E PROCEDIMENTOS	11
3.1 O que a Anatel não faz em relação aos bloqueios	11
3.2 Quem executa tecnicamente os bloqueios	12
3.3 O papel concreto da Anatel diante de ordens judiciais	12
3.4 Procedimento para apoio técnico	13
4. POR QUE AS OPERADORAS NÃO CONSEGUEM BLOQUEAR VÍDEOS, PERFIS OU POSTAGENS ESPECÍFICAS - E O QUE FAZER NO LUGAR?	14
5. COMO O BLOQUEIO TÉCNICO É IMPLEMENTADO (DNS E ROTEAMENTO)	15
6. CONTORNOS: DNS PÚBLICOS E VPN	16
7. DOMÍNIOS “.BR” E O PAPEL DO NIC.BR	18
8. DOMÍNIOS ALTERNATIVOS E ORDENS DINÂMICAS	19
9. POR QUE NÃO SE RECOMENDA BLOQUEAR ENDEREÇOS IP?	20
10. INTELIGÊNCIA ARTIFICIAL, DEEPFAKES E NOVOS DESAFIOS REGULATÓRIOS E JUDICIAIS	21
11. DESTINATÁRIOS RECOMENDADOS DA DECISÃO JUDICIAL	24
12. FORMATO DAS LISTAS DE DOMÍNIO	24
13. REMOÇÃO DE APLICATIVOS	25

14. O QUE CONTEMPLAR NA DECISÃO (MODELO OPERACIONAL)	25
14.1 Bloqueio de endereço IP em caráter excepcional e quando demonstrada a inexistência de alternativa menos gravosa	26
14.2 Bloqueio de domínio	26
14.3 Remoção ou indisponibilização de URL específica pela plataforma	27
14.4 Remoção de conteúdo interno da plataforma	28
15. PAPEL DOS ÓRGÃOS EXECUTORES	30
16. EXEMPLOS PRÁTICOS	30
16.1 O vídeo que se espalhou em poucas horas (difamação)	30
16.2 O site que só existia para praticar ilícitos	31
16.3 O <i>deepfake</i> que parecia real demais	32
16.4 O aplicativo que gerava e distribuía conteúdo ilícito	32
16.5 O site de <i>phishing</i> que imitava um banco	33
17. CHECK-LIST PARA AUTORIDADES JUDICIAIS (OPERACIONAL)	34
18. REFERÊNCIA RÁPIDA – PERGUNTAS E RESPOSTAS	35
19. CONSIDERAÇÕES FINAIS	37

1. INTRODUÇÃO

Este Guia tem por objeto tratar das solicitações de bloqueio de acesso, oriundas de ordens judiciais, de sites, aplicativos e conteúdos na Internet, bem como delimitar, com maior precisão, o papel técnico, regulatório e operacional da Agência Nacional de Telecomunicações (Anatel) no encaminhamento, acompanhamento e apoio ao cumprimento dessas decisões.

O documento foi concebido não apenas como um roteiro procedimental, mas como um instrumento de alinhamento conceitual entre os entes envolvidos na execução das ordens de bloqueio, a saber: as autoridades judiciais, órgãos executores de decisões, plataformas digitais e prestadoras de serviços de telecomunicações.

Na prática, muitas dificuldades enfrentadas no cumprimento de ordens judiciais não decorrem de má-fé ou resistência deliberada, mas de expectativas técnicas incompatíveis com a arquitetura real da Internet e com as competências legais dos diferentes atores envolvidos.

O que se busca nesse Guia é fornecer a magistrados, membros do Ministério Público, integrantes das polícias judiciárias (federal e civis) e demais órgãos responsáveis pela execução de decisões judiciais uma compreensão integrada sobre 3 (três) dimensões essenciais para o tratamento de ilícitos na Internet:

- 1.** a dimensão técnica, que envolve compreender como a Internet funciona em aspectos relevantes para bloqueios e remoções, incluindo DNS (*Domain Name System* – Sistema de Nomes de Domínio), URLs (*Uniform Resource Locator*), domínios, criptografia e arquitetura de redes, conceitos que serão explorados a seguir;

2. a dimensão institucional, que exige distinguir com clareza o que compete às plataformas digitais e o que compete às prestadoras de acesso à Internet, evitando imputações equivocadas de responsabilidade; e

3. a dimensão decisória, que diz respeito à forma de estruturar ordens judiciais de modo a maximizar sua efetividade prática, minimizando riscos de contorno, atrasos ou efeitos colaterais desproporcionais.

Parte-se da premissa de que a eficácia de uma ordem judicial de bloqueio de acesso depende simultaneamente de 3 (três) pilares interdependentes: fundamentação jurídica adequada, viabilidade técnica e clareza operacional.

1.1 Premissas e Fundamentos Legais

A Lei nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet, constitui o principal referencial normativo para questões envolvendo bloqueio de acesso e remoção de conteúdo no Brasil. Todavia, sua aplicação deve observar os parâmetros definidos pelo Supremo Tribunal Federal - STF no julgamento do RE 1037396 (Tema 987) e do RE 1057258 (Tema 533).

O art. 9º, §3º, da citada lei, ao prever que é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, impõe limites claros sobre o que as operadoras de telecomunicações podem fazer tecnicamente.

Por sua vez, a Lei nº 9.472, de 16 de julho de 1997 - Lei Geral de Telecomunicações - LGT, define o papel regulatório da Anatel e disciplina os serviços que viabilizam o acesso à Internet no país, notadamente:

- **Serviço Móvel Pessoal (SMP)**, que inclui acesso à Internet móvel via redes celulares;

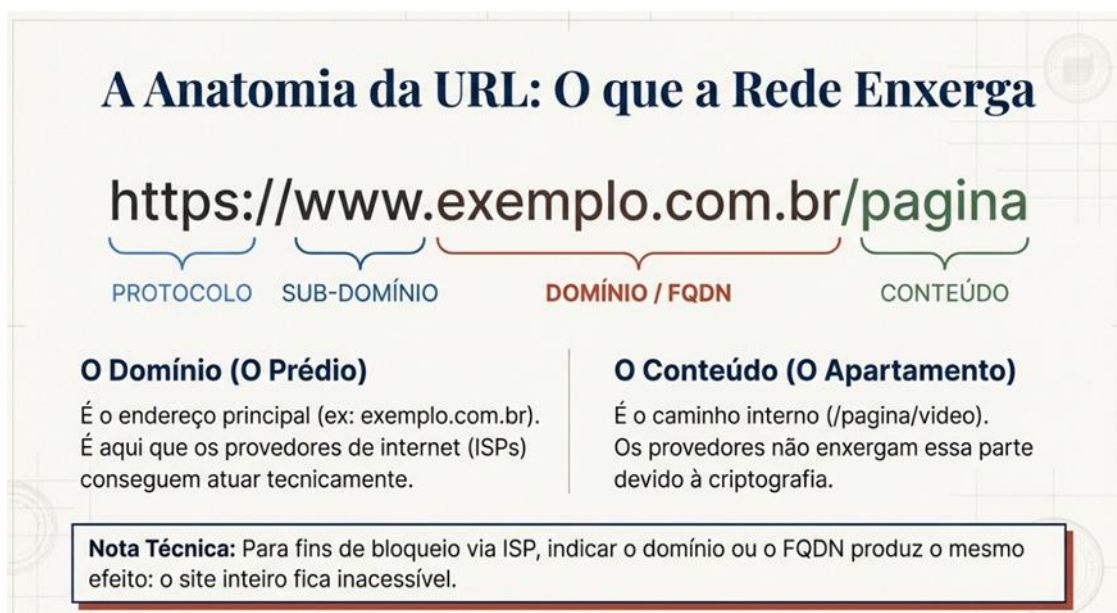
- **Serviço de Comunicação Multimídia (SCM)**, que abrange acesso à Internet fixa por meio de cabos, fibra óptica ou rádio; e
- **Serviço Limitado Privado (SLP)**, utilizado em algumas infraestruturas corporativas e institucionais.

São esses serviços que constituem a base técnica sobre a qual eventuais bloqueios de acesso à Internet podem ser implementados pelas prestadoras.

2. CONCEITOS BÁSICOS DA INTERNET

Para compreender corretamente como ocorre o acesso a conteúdos na Internet, e, conseqüentemente, como funcionam medidas judiciais de bloqueio ou remoção, é útil conhecer alguns elementos básicos da estrutura da rede. Esses elementos aparecem com frequência em decisões judiciais e em comunicações com provedores de Internet.

A explicação a seguir apresenta esses conceitos na mesma ordem em que participam do funcionamento real da Internet, partindo do elemento mais fundamental até o endereço completo de uma página.



Quando uma pessoa acessa um site, diversos sistemas trabalham em conjunto para localizar o conteúdo desejado. Os principais elementos envolvidos são:

Endereço IP (número do servidor).

Domínio (nome principal do site);

DNS (sistema que traduz nomes em números); e

URL (endereço completo de um conteúdo).

2.1 O que é Endereço IP

O endereço IP (*Internet Protocol*) é o identificador numérico utilizado para localizar dispositivos conectados à Internet.

Cada servidor que hospeda um site, serviço ou aplicação possui um endereço IP, que funciona de maneira semelhante a um número único de identificação na rede. Esse número permite que os equipamentos da Internet saibam para onde enviar e de onde receber informações.

Um exemplo simplificado de endereço IP seria:

192.0.2.1

Quando um usuário acessa um site, o computador ou telefone precisa, em última análise, estabelecer comunicação com o endereço IP do servidor onde o conteúdo está hospedado.

Assim, do ponto de vista técnico, toda comunicação na Internet ocorre entre endereços IP.

2.2 O que é um domínio?

Como endereços IP são compostos apenas por números e são difíceis de memorizar, foi criado um sistema de nomes que permite identificar serviços de forma mais simples. Esses nomes são chamados de domínios.

Um domínio é o nome pelo qual um site ou serviço se torna conhecido e acessível ao público. Exemplos conhecidos incluem:

Google - google.com

Facebook - facebook.com

Wikipedia - wikipedia.org

Na prática, o domínio funciona como um nome associado a um ou mais endereços IP. Dessa forma, os usuários podem acessar serviços utilizando nomes fáceis de lembrar, em vez de números.

2.3 O que é DNS?

O DNS (*Domain Name System* – Sistema de Nomes de Domínio) é responsável por **traduzir domínios em endereços IP**. Funciona como uma agenda telefônica da Internet.

Quando alguém digita o endereço de um site, como **www.exemplo.com**, o computador não sabe trabalhar diretamente com esse “nome bonito”, só com números chamados endereços IP (algo como 192.0.2.15).

O DNS é o “serviço de tradução” que converte o nome do site nesse número técnico para que a conexão aconteça.

Uma analogia útil é pensar na lista telefônica ou na agenda de contatos do celular. O usuário procura “**Maria**” pelo nome, mas o telefone, por baixo, precisa do número para

completar a chamada; o DNS faz esse papel entre o nome do site e o número IP do servidor. Significa que sem o DNS, os usuários precisariam memorizar números para acessar qualquer site.

No dia a dia, essa tradução é feita de forma automática pelos servidores de DNS configurados na operadora de Internet (móvel ou fixa) ou no próprio dispositivo do usuário.

O usuário comum nunca vê esse processo, apenas digita o nome do site e a página aparece, mas tecnicamente sempre houve essa consulta ao DNS antes do carregamento.

2.4 O que é URL?

A URL (*Uniform Resource Locator*) é o endereço completo de um recurso específico na Internet.

Enquanto o domínio identifica um site de forma geral, a URL permite localizar uma página ou conteúdo específico dentro desse site.

Uma URL normalmente contém três elementos principais:

1. Protocolo de acesso, que indica como a comunicação será feita (por exemplo, http ou https);
2. Domínio, que identifica o servidor onde o site está hospedado;
3. Caminho interno, que indica a página ou recurso específico dentro do site.

Exemplo de URL:

`https://exemplo.com/noticias/decisao-judicial`

Nesse exemplo:

- a) https indica o protocolo de comunicação;

- b) exemplo.com é o domínio;
- c) /noticias/decisao-judicial identifica a página específica dentro do site.

Assim, enquanto o domínio aponta para o site como um todo, a URL identifica um conteúdo específico dentro desse site.

2.5 Relação entre os elementos

Em termos simplificados, o funcionamento do acesso a um conteúdo na Internet ocorre da seguinte forma:

- 1.** O usuário digita uma URL no navegador.
- 2.** O navegador identifica o domínio presente nesse endereço.
- 3.** O sistema DNS é consultado para descobrir qual endereço IP corresponde a esse domínio.
- 4.** O dispositivo então se conecta ao endereço IP do servidor, que envia o conteúdo solicitado.

Essa sequência explica por que diferentes tipos de medidas técnicas, como bloqueios por IP, por domínio ou por URL, podem produzir efeitos distintos na acessibilidade de um conteúdo na Internet.

E compreender essa diferença permite que medidas de bloqueio ou remoção sejam direcionadas ao nível técnico adequado, reduzindo impactos indevidos sobre outros conteúdos ou serviços legítimos.



Para fins de ordens judiciais de bloqueio de acesso, a distinção decisiva é entre o domínio e o caminho interno.

As prestadoras conseguem atuar tecnicamente sobre o domínio, mas não conseguem bloquear seletivamente apenas um conteúdo interno sem afetar o acesso ao site como um todo. Em termos práticos, é possível "fechar o prédio inteiro", mas não apenas um "apartamento".

3. O PAPEL DA ANATEL: COMPETÊNCIAS, LIMITES E PROCEDIMENTOS

3.1 O que a Anatel **não faz** em relação aos bloqueios

É recorrente que decisões judiciais atribuam à Anatel a execução direta de bloqueios de sites, remoção de conteúdos ou suspensão de contas em plataformas digitais. Essa compreensão não corresponde às competências legais nem às capacidades técnicas da Agência.



A Anatel não opera redes de Internet, não gerencia servidores ou sistemas de DNS, não controla roteadores das operadoras e não possui ferramentas próprias para bloquear sites, remover vídeos ou suspender perfis.

A atuação da Agência é essencialmente regulatória e fiscalizatória, e não operacional.

3.2 Quem executa tecnicamente os bloqueios

Os bloqueios de acesso a sites (domínios) são executados exclusivamente pelas prestadoras de serviços de telecomunicações, que incluem operadoras de telefonia móvel (SMP), provedores de Internet fixa (SCM) e, em casos específicos, prestadores de infraestrutura corporativa (SLP).

São essas empresas que possuem controle sobre os equipamentos de rede, sistemas de DNS e políticas de tráfego que permitem ou impedem o acesso a domínios na Internet.

3.3 O papel concreto da Anatel diante de ordens judiciais

Diante de uma decisão judicial de bloqueio de acesso a sites (domínios), a atuação da Anatel normalmente pode envolver, a depender dos termos judiciais:

- recepção e análise técnica preliminar da decisão;
- encaminhamento formal da decisão às prestadoras responsáveis pela execução;
- esclarecimento de dúvidas técnicas sobre exequibilidade;
- acompanhamento do cumprimento e, quando necessário, solicitação de comprovações às operadoras; e
- realização de testes ou verificações técnicas para confirmar se o bloqueio foi implementado.

Em síntese, a Anatel coordena e fiscaliza, enquanto a execução material dos bloqueios cabe às prestadoras.



3.4 Procedimento para apoio técnico

Caso o órgão executor (ex. Ministério Público ou Polícia Judiciária) necessite de apoio técnico - por exemplo, para identificar domínios alternativos, avaliar possíveis rotas de contorno ou verificar a efetividade de um bloqueio - basta solicitar formalmente à Anatel por meio de ofício específico.

4. POR QUE AS OPERADORAS NÃO CONSEGUEM BLOQUEAR VÍDEOS, PERFIS OU POSTAGENS ESPECÍFICAS - E O QUE FAZER NO LUGAR?

Antes de analisar as limitações jurídicas e técnicas, é importante distinguir duas situações que frequentemente se confundem:

1. a remoção de um conteúdo específico; e
- 2 a interrupção de acesso a um site como um todo.

No primeiro caso, busca-se retirar um vídeo, postagem ou perfil determinado; no segundo, pretende-se impedir o acesso ao domínio inteiro.

Do ponto de vista jurídico, o art. 9º, §3º, do Marco Civil da Internet impede que prestadoras inspecionem o conteúdo das comunicações dos usuários.

Isso significa que elas não podem “ler” vídeos, postagens ou mensagens para decidir seletivamente o que bloquear, nem filtrar tráfego por tema ou assunto. Assim, ordens judiciais que exijam das operadoras o bloqueio de um vídeo ou perfil específico pressupõem uma inspeção de conteúdo que é vedada e, na prática, inviável.

Há também uma limitação técnica estrutural: as operadoras veem principalmente para qual domínio ou endereço IP o tráfego está sendo direcionado, mas não conseguem identificar, de forma utilizável, qual vídeo ou postagem específica está sendo acessada dentro de uma plataforma, especialmente porque a maior parte do tráfego moderno é criptografado por HTTPS.

Como consequência, quando o objetivo é remover um conteúdo específico, a medida tecnicamente adequada é dirigir a ordem diretamente à plataforma que o hospeda, pois ela controla os sistemas internos que identificam vídeos, perfis e postagens. A

plataforma pode localizar o material, removê-lo, restringir sua visualização e, quando necessário, adotar medidas para prevenir republicações.

Em paralelo, é recomendável que a decisão também determine a desindexação em mecanismos de busca, pois links podem continuar circulando mesmo após a remoção na plataforma.

O bloqueio de acesso de domínio pelas prestadoras deve ser visto como medida excepcional, adequada principalmente quando o site é estruturalmente voltado ao ilícito, quando há reiterado descumprimento por plataformas ou quando a gravidade e urgência do caso justificam uma intervenção ampla.

5. COMO O BLOQUEIO TÉCNICO É IMPLEMENTADO (DNS E ROTEAMENTO)

Na prática, a maior parte dos bloqueios realizados pelas prestadoras ocorre no nível do Sistema de Nomes de Domínio (DNS), que traduz nomes de sites em endereços IP. O que as operadoras fazem é impedir que a “agenda de contatos” (o DNS) devolva o número correto daquele domínio (IP). Assim, quando o usuário tenta acessar o site bloqueado, o navegador não consegue localizar o servidor, resultando em erro de acesso ou em uma página de bloqueio.



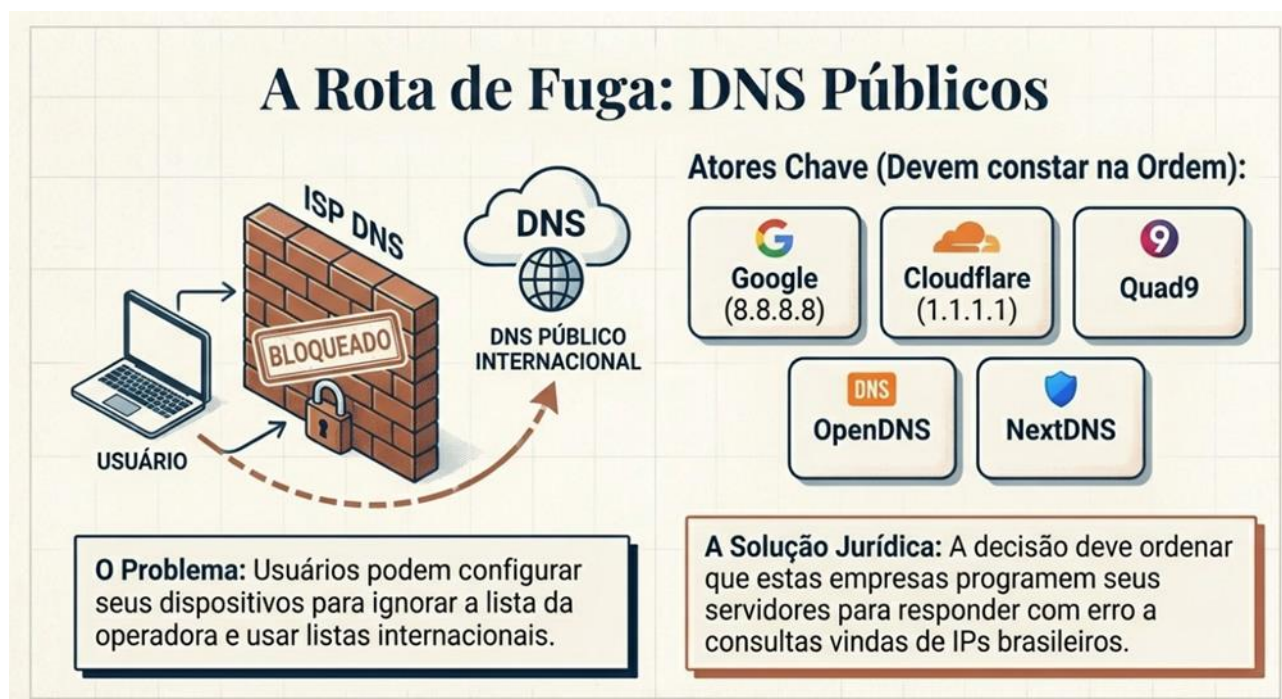
Esse mecanismo explica por que não é tecnicamente viável bloquear apenas um caminho interno de uma URL: o DNS opera no nível do domínio, não no nível do conteúdo específico.

Além disso, as redes de telecomunicações são interconectadas nacionalmente e não respeitam limites administrativos internos, razão pela qual bloqueios em regra, são implementados com alcance nacional pelas prestadoras destinatárias da ordem.

6. CONTORNOS: DNS PÚBLICOS E VPN

Além dos servidores de DNS das próprias operadoras, existem provedores de DNS públicos acessíveis a qualquer pessoa, como Cloudflare, Quad9, Google, OpenDNS, Comodo e NextDNS.

Usuários com conhecimento técnico podem configurar seus dispositivos para utilizar esses servidores, contornando parcialmente bloqueios aplicados apenas por operadoras brasileiras.

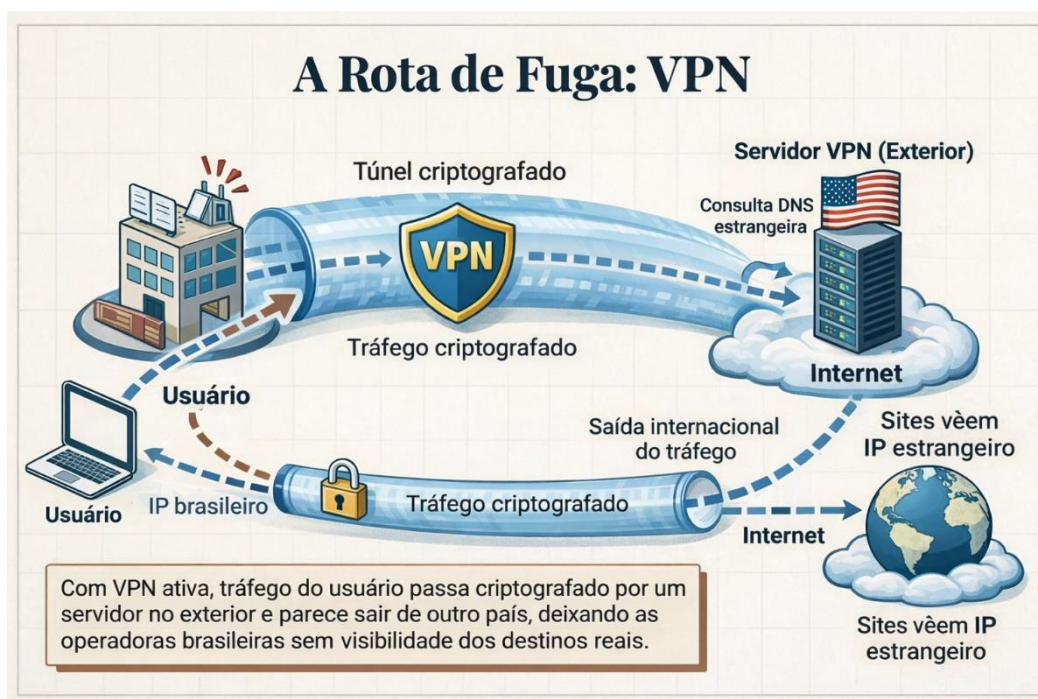


Embora tecnicamente possível, essa prática não é comum entre o usuário médio e, quando ocorre, geralmente indica intenção deliberada de afastar os efeitos de uma decisão judicial.

Quando houver risco relevante de evasão, recomenda-se que a decisão alcance também os provedores de DNS públicos, determinando que seus servidores que atendem usuários no Brasil respondam com erro às consultas referentes aos domínios bloqueados.

O uso de uma Rede Privada Virtual (*Virtual Private Network* – VPN) também pode permitir que o tráfego saia por servidores localizados fora do país.

Quando a VPN é ativada, o dispositivo do usuário estabelece um túnel criptografado com um servidor remoto, que pode estar localizado em outro país, fazendo com que todo o tráfego de dados passe primeiro por esse servidor antes de alcançar o destino final na Internet.



Nesse momento, a operadora deixa de visualizar diretamente os domínios acessados ou os endereços IP de destino, enxergando apenas uma conexão criptografada entre o usuário e o servidor VPN. Além disso, as consultas de DNS normalmente passam a ser realizadas pelo próprio provedor da VPN ou são encaminhadas dentro do túnel seguro, impedindo que o DNS da operadora nacional participe da resolução dos nomes de domínio.

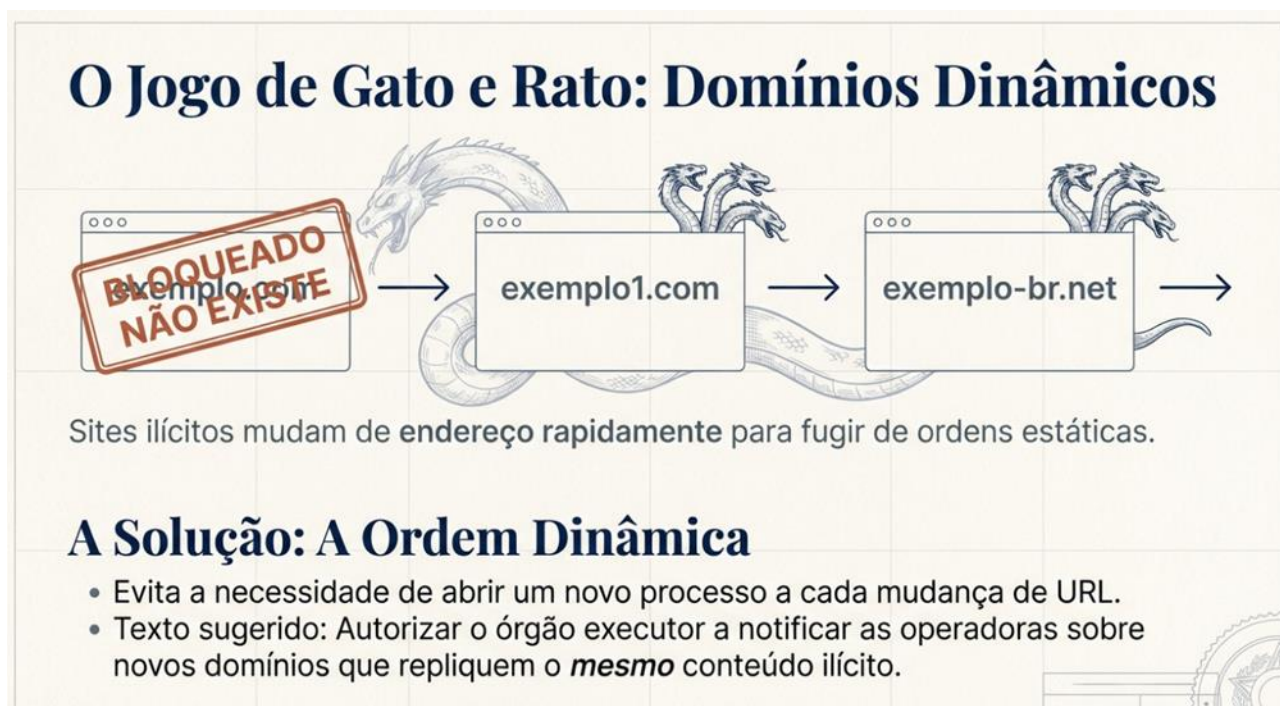
Como consequência, o ponto de saída do tráfego deixa de ser a infraestrutura da operadora brasileira e passa a ser o servidor VPN no exterior.

7. DOMÍNIOS “.BR” E O PAPEL DO NIC.BR

Quando o domínio objeto de bloqueio terminar em “.br”, a ordem judicial de bloqueio deve ser encaminhada ao NIC.br (Registro.br), responsável pela administração desses registros no Brasil. Nesses casos, é recomendável determinar a “suspensão da delegação do domínio” ou “suspensão do registro”, conforme o caso, medida que dificulta significativamente a continuidade do serviço no território nacional.

8. DOMÍNIOS ALTERNATIVOS E ORDENS DINÂMICAS

Os responsáveis por sites bloqueados frequentemente criam domínios para contornar decisões judiciais.



Para mitigar esse comportamento, recomenda-se que a decisão judicial preveja uma ordem dinâmica de bloqueio, autorizando o Ministério Público ou a Polícia Judiciária a identificar e solicitar o bloqueio de novos domínios que reproduzam substancialmente o mesmo conteúdo ilícito, sem necessidade de nova decisão judicial para cada endereço.

9. POR QUE NÃO SE RECOMENDA BLOQUEAR ENDEREÇOS IP?

O bloqueio direto de endereços IP (*Internet Protocol*) é tecnicamente arriscado porque um mesmo IP pode hospedar centenas de sites diferentes, o que poderia resultar no bloqueio indevido de conteúdos lícitos.

Além disso, a associação entre domínio e IP pode ser alterada rapidamente pelo responsável pelo conteúdo, exigindo monitoramento contínuo e tornando a medida pouco eficaz.

Por que **NÃO** bloquear Endereços IP?

O Risco do Dano Colateral (Hospedagem Compartilhada)

- Um único endereço numérico (IP) pode hospedar centenas de sites legítimos. Bloquear o IP derruba todos eles.
- **Realidade Técnica:** Criminosos trocam de IP facilmente. O bloqueio é ineficaz e perigoso.
- **Veredito:** Foque no DOMÍNIO (FQDN), evite o IP.

Por essas razões, o bloqueio por IP não é recomendável como regra geral.

Para mitigar esse comportamento, recomenda-se que a decisão preveja uma ordem dinâmica de bloqueio, autorizando o Ministério Público ou a Polícia Judiciária a identificar e solicitar o bloqueio de novos domínios que reproduzam substancialmente

o mesmo conteúdo ilícito, sem necessidade de nova decisão judicial para cada endereço.

10. INTELIGÊNCIA ARTIFICIAL, DEEPFAKES E NOVOS DESAFIOS REGULATÓRIOS E JUDICIAIS

A difusão de ferramentas de inteligência artificial generativa alterou significativamente a dinâmica de produção, circulação e replicação de conteúdos na Internet, criando desafios para o Poder Judiciário, para as plataformas digitais e para o setor de telecomunicações.

Diferentemente de períodos anteriores, em que a maior parte do conteúdo era produzida manualmente por pessoas identificáveis, hoje é possível gerar textos, imagens, áudios e vídeos em larga escala, com alta qualidade técnica e em tempo extremamente reduzido.

Esse cenário produz 3 (três) efeitos jurídicos e operacionais relevantes.

Primeiro, a velocidade de propagação de conteúdos ilícitos aumentou de forma exponencial, pois ferramentas automatizadas permitem criar múltiplas versões de um mesmo material quase instantaneamente.

Segundo a identificação do autor ou responsável tornou-se mais complexa, uma vez que conteúdos podem ser gerados, editados e repostados por diferentes agentes, em diferentes jurisdições, sem rastro claro de origem.

Terceiro, a fronteira entre verdadeiro e falso tornou-se mais tênue, especialmente no caso de *deepfakes*.

Os *deepfakes* - conteúdos audiovisuais manipulados por Inteligência Artificial - IA para simular falas, gestos ou aparências de pessoas reais - representam um dos desafios

mais sensíveis. Eles podem ser utilizados para difamação, fraude, manipulação política, extorsão ou desinformação em larga escala.

Diferentemente de um vídeo comum, um *deepfake* bem elaborado é difícil de distinguir do material autêntico para o usuário médio, o que potencializa o dano reputacional e social.

Do ponto de vista técnico, as plataformas passaram a adotar ferramentas de detecção automatizada de conteúdo manipulado, baseadas em análise de padrões de compressão, inconsistências visuais e rastros digitais.

Contudo, essas ferramentas ainda não são infalíveis e exigem constante atualização, pois os próprios modelos de IA evoluem rapidamente.

Para fins de decisões judiciais, isso implica algumas cautelas e possibilidades específicas.

Em casos envolvendo *deepfakes* ou conteúdos gerados por IA, a simples remoção de um único arquivo frequentemente é insuficiente, pois cópias idênticas ou levemente modificadas tendem a reaparecer em outras contas ou plataformas. Por isso, pode ser necessário determinar medidas estruturais, como:

- a remoção do conteúdo original e de suas duplicatas identificáveis;
- a utilização, pelas plataformas, de mecanismos automatizados de detecção e bloqueio de *reuploads*, entendidos como novas publicações de conteúdos já removidos anteriormente por violarem regras;
- a preservação de registros técnicos para eventual identificação de responsáveis;
- a desindexação do material em mecanismos de busca; e
- quando houver um site próprio dedicado à difusão desse conteúdo, o bloqueio do domínio associado.

Quando o ilícito estiver vinculado a um aplicativo que utiliza IA para gerar ou disseminar conteúdo ilícito, como, por exemplo, um aplicativo que cria *deepfakes* sob demanda,

pode ser necessário determinar sua retirada das lojas digitais (Google Play e Apple App Store), além de exigir relatórios técnicos sobre medidas preventivas adotadas pela empresa responsável.

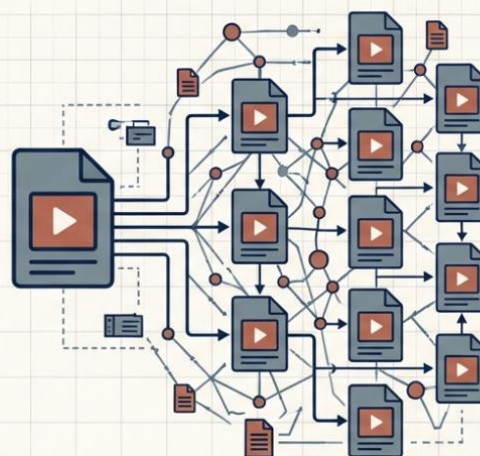
Também se torna relevante, nesses casos, a cooperação entre diferentes plataformas, uma vez que o mesmo conteúdo pode circular simultaneamente em redes sociais, serviços de vídeo, aplicativos de mensagens e sites independentes. Decisões judiciais mais eficazes tendem a contemplar esse caráter multiplataforma do problema, em vez de se restringirem a um único provedor.

Por fim, é importante reconhecer que a inteligência artificial não é apenas um risco: ela também pode ser uma ferramenta auxiliar para a execução de decisões judiciais, permitindo monitoramento automatizado de novos domínios, identificação de conteúdo similar e análise de padrões de evasão.

Novos Desafios: Inteligência Artificial e Deepfakes

A Ameaça: Replicação em massa e deepfakes. O link morre, mas o arquivo sobrevive.

- ✓ **Remoção na Origem (App Stores):** Ordem para Google Play e Apple App Store removerem aplicativos disseminadores.
- ✓ **Detecção Automatizada:** Exigir das plataformas (YouTube, Meta) filtros de 'hash' para bloquear re-uploads do mesmo arquivo.
- ✓ **Foco no Arquivo:** A ordem deve visar o conteúdo do vídeo/áudio, independente da URL onde ele reapareça.

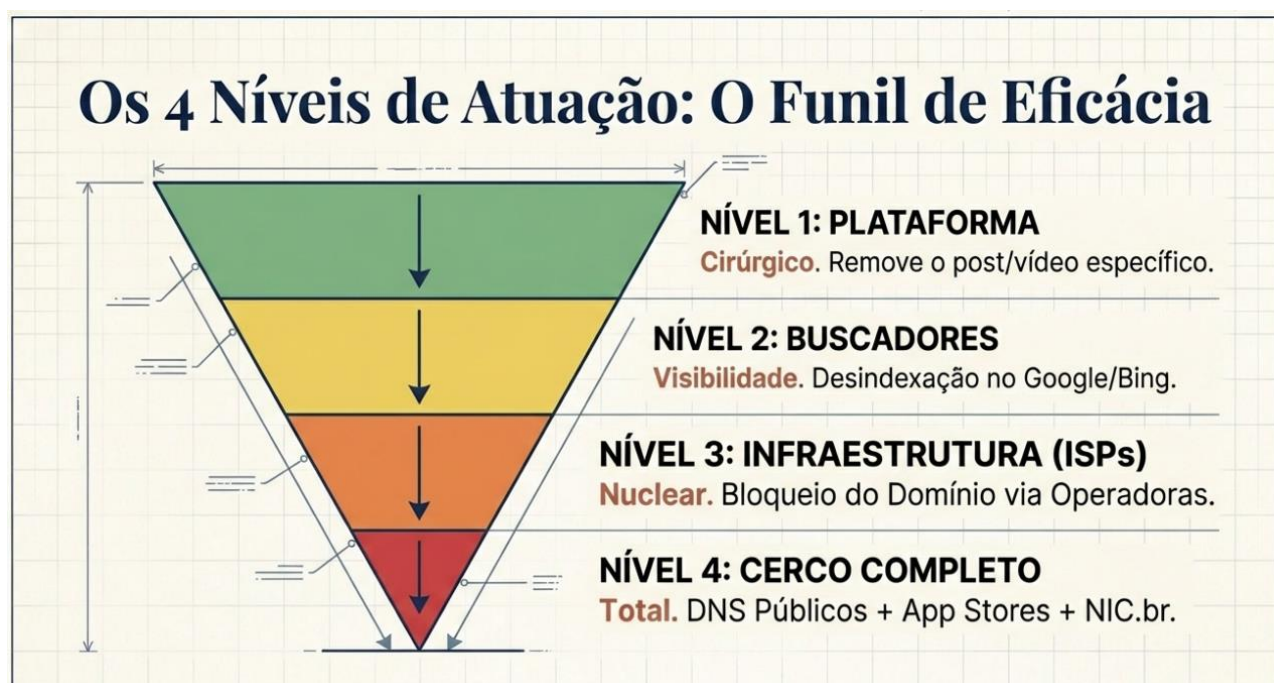


Nesse sentido, o desafio contemporâneo não é apenas reprimir o uso indevido da IA, mas também integrá-la de forma responsável às estratégias de cumprimento e fiscalização.

11. DESTINATÁRIOS RECOMENDADOS DA DECISÃO JUDICIAL

Conforme o caso concreto, a decisão pode precisar alcançar diferentes atores:

- i. as plataformas que hospedam o conteúdo;
- ii. as prestadoras de acesso à Internet;
- iii. provedores de DNS públicos;
- iv. o NIC.br (quando o domínio for “.br”); e
- v. lojas de aplicativos, quando houver app envolvido.



A definição clara desses destinatários aumenta a efetividade prática da ordem.

12. FORMATO DAS LISTAS DE DOMÍNIO

Para facilitar a execução técnica, recomenda-se que listas de domínios ou FQDN sejam apresentadas em PDF e arquivos digitais simples, como TXT, CSV, ODS ou XLSX,

evitando o formato de imagem, que dificulta a implementação da decisão pelas prestadoras de serviços de telecomunicações.

13. REMOÇÃO DE APLICATIVOS

Sempre que houver aplicativo relacionado ao conteúdo ilícito, a ordem judicial deve prever sua retirada de todas as lojas pertinentes, evitando que o material continue acessível por essa via. Nesse caso, a citada ordem deve ser encaminhada à empresa responsável pela loja de aplicativos.

14. O QUE CONTEMPLAR NA DECISÃO (MODELO OPERACIONAL)

A compreensão da diferença entre endereços IP, domínios, DNS e URLs permite que decisões judiciais relacionadas à Internet sejam formuladas de forma tecnicamente adequada e proporcional, direcionando a ordem ao agente capaz de cumpri-la e evitando impactos desnecessários sobre outros serviços.

Decisões mais eficazes costumam atuar em quatro níveis complementares:

- primeiro, determinam a remoção do conteúdo específico pelas plataformas;
- segundo, ordenam a desindexação em mecanismos de busca;
- terceiro, indicam claramente os domínios a serem bloqueados pelas prestadoras de acesso, quando necessário; e, por fim,
- incluem provedores de DNS públicos quando houver risco de contorno.

A seguir são apresentados exemplos práticos e modelos simplificados de redação judicial, ilustrando situações comuns.

14.1 Bloqueio de endereço IP em caráter excepcional e quando demonstrada a inexistência de alternativa menos gravosa

O bloqueio de endereço IP é uma medida técnica mais ampla, que pode afetar todos os serviços hospedados naquele servidor.

Isso ocorre porque um único endereço IP pode hospedar diversos domínios ou aplicações distintas.

Exemplo prático

Um servidor localizado no exterior hospeda diversas páginas, entre elas um site utilizado para comercialização de produtos ilícitos.

Caso seja determinado o bloqueio do endereço IP do servidor, todos os sites hospedados naquele mesmo servidor poderão se tornar inacessíveis, ainda que não tenham relação com a atividade investigada.

Por essa razão, esse tipo de medida costuma ser adotado apenas quando outras formas de bloqueio não são eficazes ou não estão disponíveis.

Exemplo de redação judicial

Modelo de decisão

Determino que os provedores de conexão à Internet adotem as medidas técnicas necessárias para bloquear o acesso ao endereço IP indicado nos autos, utilizado para a disponibilização do serviço objeto da presente decisão.

A medida deverá ser implementada no prazo de ____ horas, devendo os provedores informar nos autos o cumprimento da determinação.

14.2 Bloqueio de domínio

O bloqueio de domínio impede o acesso a todo o site identificado por aquele nome.

Trata-se de uma medida comum quando o site inteiro é utilizado para atividades ilícitas.

Exemplo prático

Um site hospedado no domínio:

exemplo-ilegal.com

é dedicado integralmente à prática de fraude ou à comercialização de produtos ilícitos.

Nesse caso, pode ser tecnicamente adequado determinar o bloqueio do domínio, impedindo o acesso ao site como um todo.

Exemplo de redação judicial

Modelo de decisão

Determino que os provedores de conexão à Internet adotem as medidas técnicas necessárias para impedir o acesso ao domínio indicado nos autos, utilizado para a disponibilização do conteúdo objeto da presente decisão.

O bloqueio deverá ser implementado por meio dos mecanismos técnicos adequados, inclusive mediante restrição de resolução de nomes de domínio.

14.3 Remoção ou indisponibilização de URL específica pela plataforma

A indisponibilização de URL pela plataforma é medida mais específica e proporcional, utilizada quando o conteúdo ilícito está localizado em uma página específica dentro de um site legítimo.

Exemplo prático

Um conteúdo ilícito foi publicado em uma página específica dentro de uma plataforma amplamente utilizada, como um vídeo ou postagem.

Exemplo de endereço:

<https://exemplo.com/pagina/conteudo-ilicito>

Nessa hipótese, a decisão deve ser dirigida à plataforma responsável pelo serviço, e não às prestadoras de telecomunicações, pois são as plataformas que conseguem localizar e indisponibilizar aquela página, vídeo, postagem ou recurso específico sem afetar todo o domínio.

Exemplo de redação judicial

Modelo de decisão

Determino que a plataforma responsável pelo serviço indicado nos autos promova, no prazo de ____ horas, a remoção ou indisponibilização do conteúdo acessível por meio da URL específica indicada na presente decisão, limitando a medida ao recurso identificado, sem prejuízo dos demais conteúdos lícitos hospedados no mesmo domínio.

Após o cumprimento da medida, a plataforma deverá informar nos autos as providências adotadas.

14.4 Remoção de conteúdo interno da plataforma

Muitas vezes o objeto da decisão judicial não é o site ou a página em si, mas o conteúdo específico ali publicado, como:

uma postagem

um vídeo

uma imagem

um comentário

Nesses casos, a medida adequada é a remoção do conteúdo pela própria plataforma que o hospeda.

Plataformas amplamente utilizadas, como Google, Meta Platforms (responsável por serviços como Facebook e Instagram) ou X Corp. (responsável pela rede social X), possuem controle direto sobre os conteúdos publicados em suas plataformas.

Assim, apenas essas empresas conseguem remover ou moderar o conteúdo específico.

Use esta seção quando o conteúdo ilícito não estiver suficientemente identificado apenas por uma URL, ou quando a plataforma utilize identificadores internos próprios, como ID de vídeo, ID de postagem, ID de perfil, hash de arquivo, nome de usuário, código de publicação ou outro elemento técnico equivalente.

Diferentemente da URL, que é o endereço público de acesso, o identificador interno é o dado usado pela própria plataforma para localizar o conteúdo em seus sistemas. Ele

pode ser mais estável e preciso do que a URL, especialmente quando o mesmo conteúdo aparece em diferentes links, é republicado, incorporado em outras páginas ou acessado por aplicativos.

Nessa hipótese, a decisão deve fornecer à plataforma os elementos mínimos que permitam a localização inequívoca do material, preferencialmente combinando URL, identificador interno, data de publicação, nome do perfil, captura de tela e descrição objetiva do conteúdo.

Exemplo de redação judicial

Modelo de decisão

Determino que a plataforma responsável pelo serviço indicado nos autos localize e remova, no prazo de ____ horas, o conteúdo identificado por seu ID interno, perfil, publicação ou outro identificador técnico equivalente constante dos autos, adotando as providências necessárias para impedir sua continuidade de exibição, compartilhamento ou acesso público, sem afetar conteúdos diversos não abrangidos pela presente decisão.

Após o cumprimento da medida, a plataforma deverá informar nos autos as providências adotadas.

Modelos de Decisão (Parte 1): O Básico Essencial

Modelos de Decisão (Parte 2): Cenários Complexos

MODELO C: Ordem Dinâmica (Anti-Evasão)

Autoriza-se o órgão executor a determinar o bloqueio de novos domínios que reproduzam o mesmo conteúdo, mediante comunicação simples às prestadoras.

MODELO D: Remoção de App

Determino que Google Play e Apple App Store removam o aplicativo [Nome] e que eventuais domínios associados sejam bloqueados.

CRUCIAL: Exigir listas de domínios em formato digital editável (.txt, .csv, .xlsx), nunca apenas em PDF ou Imagem.

15. PAPEL DOS ÓRGÃOS EXECUTORES

Normalmente, os órgãos executores (Ministério Público e Polícia Judiciária) acompanham o cumprimento das decisões, monitoram o surgimento de novos domínios ou plataformas com o mesmo conteúdo e solicitam bloqueios adicionais, quando necessário.

A Anatel pode prestar apoio técnico mediante solicitação formal.

16. EXEMPLOS PRÁTICOS

16.1 O vídeo que se espalhou em poucas horas (difamação)

Em uma manhã de segunda-feira, uma profissional conhecida em sua cidade acordou e descobriu que um vídeo com acusações falsas contra ela estava circulando em uma grande rede social. Em poucas horas, o material já havia sido compartilhado centenas

de vezes, aparecendo em grupos de WhatsApp, perfis de terceiros e até em resultados de busca no Google.

Seu advogado ingressou com uma medida judicial pedindo a retirada imediata do vídeo.

O juiz, ao analisar o caso, determinou que a própria plataforma removesse o conteúdo específico, fornecendo a URL exata e o identificador do vídeo.

Paralelamente, ordenou que os mecanismos de busca desindexassem os links relacionados, para reduzir a visibilidade do material.

Algumas pessoas sugeriram que as operadoras de Internet “**bloqueassem o vídeo**”, mas o magistrado deixou claro na decisão que isso não era tecnicamente possível nem juridicamente adequado, pois as prestadoras não conseguem atuar de forma seletiva sobre conteúdos internos de plataformas.

O resultado foi que o vídeo foi removido na origem, os principais links deixaram de aparecer nas buscas e, com o tempo, o alcance do material diminuiu drasticamente.

16.2 O site que só existia para praticar ilícitos

Um determinado site passou a ser investigado após inúmeras denúncias de usuários. Não se tratava de um portal legítimo com conteúdo variado, mas de uma página estruturada exclusivamente para a venda de produtos falsificados e a divulgação de golpes financeiros.

Após diligências, ficou claro que praticamente todo o conteúdo do domínio era ilícito. Diante disso, o juiz determinou o bloqueio do domínio principal junto às prestadoras de acesso no Brasil e incluiu também provedores de DNS públicos, para evitar contorno fácil da medida.

Como o domínio era registrado sob “.br”, o NIC.br foi notificado e suspendeu a delegação do endereço. Além disso, a decisão previu uma ordem dinâmica: caso os responsáveis

criassem novos domínios com o mesmo conteúdo, o órgão executor (Ministério Público ou Polícia Judiciária) poderia solicitar o bloqueio sem necessidade de nova decisão para cada endereço.

Algumas semanas depois, surgiu um site quase idêntico, com nome ligeiramente diferente. Graças à ordem judicial dinâmica, o bloqueio foi rapidamente estendido, evitando que o esquema ilegal continuasse operando.

16.3 O *deepfake* que parecia real demais

Durante um período eleitoral, começou a circular um vídeo em que um candidato aparecia fazendo declarações ofensivas e ilegais. A princípio, muitos acreditaram ser autêntico, mas especialistas confirmaram tratar-se de um *deepfake* altamente sofisticado, gerado por inteligência artificial.

A decisão judicial determinou a remoção imediata do vídeo original e de suas duplicatas identificáveis em todas as plataformas conhecidas. Também exigiu que a rede social utilizasse ferramentas automatizadas para impedir *reuploads* do mesmo material ou de versões ligeiramente modificadas.

Descobriu-se posteriormente que havia um site específico dedicado à disseminação desse e de outros *deepfakes*. O magistrado, então, ordenou o bloqueio desse domínio junto às prestadoras e aos provedores de DNS públicos, reconhecendo que o site era estruturalmente voltado à produção e difusão de conteúdo manipulado.

Combinando remoção, prevenção e bloqueio do ponto de origem, o impacto do *deepfake* foi significativamente reduzido.

16.4 O aplicativo que gerava e distribuía conteúdo ilícito

Uma empresa lançou um aplicativo que, sob o pretexto de “entretenimento”, permitia aos usuários criar e compartilhar imagens manipuladas com conteúdo ofensivo e ilegal.

Em pouco tempo, o app tornou-se popular entre grupos que o utilizavam para difamação e assédio.

Após ação judicial, o magistrado determinou a retirada do aplicativo tanto da Google Play quanto da Apple App Store. Também ordenou o bloqueio do site oficial do app, que servia como ponto central de *download* e comunicação com os usuários.

Além disso, o órgão executor foi autorizado a monitorar o surgimento de versões clonadas do aplicativo, solicitando sua remoção sempre que identificadas.

16.5 O site de *phishing* que imitava um banco

Usuários começaram a receber mensagens com links para um site que imitava a página de login de uma instituição financeira. Ao inserir suas credenciais, as vítimas tinham seus dados capturados por terceiros, possibilitando fraudes e acessos indevidos a contas bancárias.

Assim que o esquema foi identificado, o juiz determinou que a empresa de hospedagem responsável pelo site fraudulento retirasse o conteúdo do ar imediatamente. Paralelamente, ordenou o bloqueio do domínio principal pelas prestadoras de acesso à internet e, quando necessário, por provedores de DNS públicos, a fim de reduzir o risco de contorno da medida.

Como o domínio utilizado era registrado sob “.br”, o NIC.br/Registro.br também foi comunicado para adoção das providências cabíveis quanto ao registro ou à delegação do domínio, conforme os termos da decisão judicial.

A decisão também determinou a desindexação dos links associados ao golpe em mecanismos de busca, bem como autorizou o órgão executor a monitorar e indicar novos domínios que reproduzissem substancialmente a mesma página fraudulenta, permitindo a extensão dinâmica das medidas de bloqueio.

Com a combinação de retirada na origem, bloqueio do domínio, atuação sobre o registro “.br”, desindexação e monitoramento de domínios espelho, o site fraudulento perdeu rapidamente sua capacidade de atingir novas vítimas.

17. CHECK-LIST PARA AUTORIDADES JUDICIAIS (OPERACIONAL)

Antes de decidir, recomenda-se verificar:

1. se a ordem visa remover conteúdo específico ou bloquear um site inteiro;
2. se, no caso de conteúdo específico, a decisão está dirigida à plataforma correta;
3. se os domínios ou FQDNs estão claramente indicados;
4. se há previsão de desindexação em mecanismos de busca;
5. se é necessário incluir provedores de DNS públicos;
6. se o domínio é “.br” e, nesse caso, se o NIC.br foi notificado;
7. se há risco de domínios alternativos que justifique ordem dinâmica;
8. se as listas de domínios serão fornecidas em formato digital adequado; e
9. se, em casos de IA/deepfake, há medidas para prevenir republicações.

Checklist do Magistrado: Antes de Assinar

- ☒ É **remoção pontual** ou **bloqueio total**?
Se pontual -> Plataforma;
Se total -> Operadora.
- ☒ O **domínio** foi indicado claramente (FQDN)?
- ☒ O domínio é **.br**? (Se sim, incluir notificação ao NIC.br).
- ☒ Há risco de **mudança de nome**? (Se sim, incluir previsão de Ordem Dinâmica).
- ☒ Incluiu os **DNS Públicos**? (Cloudflare, Google, etc.).
- ☒ A decisão contém uma **lista técnica** em formato **.txt** ou **Excel**?

18. REFERÊNCIA RÁPIDA – PERGUNTAS E RESPOSTAS

Pergunta 1: A Anatel pode bloquear sites por ordem judicial?

A Anatel não possui meios técnicos e legais para promover, por si só, a retirada de conteúdo ou bloqueio de acesso a sítio eletrônico. Essa medida se encontra no campo de atuação das prestadoras de serviços de telecomunicações, pois apenas elas detêm a gestão das suas redes de telecomunicações. No caso do acesso à Internet, tal operação se dá pelas empresas prestadoras do Serviço Móvel Pessoal - SMP (que provê o acesso à Internet móvel), do Serviço de Comunicação Multimídia - SCM (que provê o acesso à Internet fixa) e, em alguns casos, do Serviço Limitado Privado - SLP (utilizado na conexão de infraestruturas da rede).

Pergunta 2: Se a Anatel não pode bloquear sites por ordem judicial diretamente, qual o seu papel?

No intuito de apoiar o cumprimento de decisões judiciais que versam sobre bloqueio de sítios eletrônicos, a Anatel as encaminha para as prestadoras para que estas adotem todas as medidas necessárias ao seu integral cumprimento.

Pergunta 3: O que usuários e aplicativos costumam utilizar para contornar o bloqueio de sites por ordem judicial?

Existem 2 (duas) formas ou técnicas principais que usuários ou aplicativos podem usar para contornar o bloqueio de sites por ordem judicial:

1. A configuração de dispositivos, redes ou aplicativos para utilizar servidores DNS não alcançados pela ordem judicial (por exemplo, servidor DNS fora do país, servidor DNS próprio do usuário, ou provedor de DNS que não tenha sido objeto da decisão); e
2. A utilização de Redes Privadas Virtuais (Virtual Private Network - VPN) cujo ponto de saída - o servidor VPN - não seja alcançado pela ordem judicial (tipicamente, fora do país).

Essas técnicas são de fácil implantação para usuários mais versados em tecnologia. Entretanto, são passos adicionais que não são triviais para o usuário médio e, como são tomadas explicitamente, indicam, ainda que de forma não assertiva, que o usuário as implementou para efetivamente contornar o bloqueio, isto é, desrespeitar a decisão.

Pergunta 4: É possível bloquear determinada conta de usuário ou um vídeo específico em plataformas, por exemplo, de redes sociais?

Por razões técnicas e em alinhamento com o §3º do art. 9º da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), os prestadores de serviços de telecomunicações não podem analisar os pacotes de dados, e por isso não podem interromper, conteúdos específicos como, por exemplo, uma conta ou perfil de plataforma digital, um vídeo ou uma página específica. O que é possível, pelas prestadoras de serviços de telecomunicações, é a atuação em nível de rede para interromper todo o tráfego aos sítios eletrônicos em questão, se a determinação judicial tiver a abrangência dessa medida mais gravosa.

Para se bloquear uma conta de usuário, um vídeo ou uma página específica, deve-se determinar à plataforma do serviço que o faça, considerando ainda que o conteúdo em questão pode vir a ser divulgado em outras plataformas.

Pergunta 5: A quais entidades a decisão de bloqueio ou retirada de conteúdo devem ser direcionadas para maior eficiência?

Sequencialmente, ou de forma simultânea, se assim determinado, a decisão de retirar um conteúdo da Internet deve buscar:

(i) a plataforma que detém o conteúdo, tais como redes sociais, plataformas de vídeo e de mensagens; e

(ii) a infraestrutura de acesso ao conteúdo: prestadoras de serviços de telecomunicação, provedores de DNS de uso público, prestadoras de serviço de VPN público, registradoras de domínio (registro.br/NIC.br, para domínios registrados no país). A Anatel pode apoiar o cumprimento de decisões judiciais pelo seu encaminhamento para os habilitadores de acesso à Internet para que estes adotem todas as medidas necessárias ao seu integral cumprimento.

Devido à grande flexibilidade da Internet, sugere-se que as decisões judiciais prevejam que o órgão executor possa, dinamicamente, determinar novos bloqueios de recursos com conteúdo igual ou similar ao que se deseja bloquear.

19. CONSIDERAÇÕES FINAIS

Bloqueios de acesso a sites (domínios) são instrumentos úteis, porém limitados. A abordagem mais eficaz combina remoção direta nas plataformas, bloqueio de domínios quando necessário, monitoramento contínuo pelo órgão executor e apoio técnico da Anatel.

A Agência permanece à disposição para prestar suporte sempre que formalmente solicitada.

Guia sobre Bloqueio de Sites, Aplicativos e Conteúdos na Internet