

# Informativo Proteção de Dados e Cybersecurity: Relatório da FTC aponta vigilância de usuários, recurso do Google sobre quebra de sigilo e mais notícias

08.10.2024 13 minutos de leitura

## Autores

Felipe Palhares  
Fernanda Villela

## Áreas relacionadas

Proteção de Dados e  
Cybersecurity

## Assuntos

Informativos | Proteção de Dados e  
Cybersecurity | ANPD | LGPD

## RELATÓRIO DA FTC APONTA VIGILÂNCIA MASSIVA DE USUÁRIOS

Recentemente, uma análise das práticas de tratamento de dados pessoais de nove empresas de tecnologia e serviços de streaming apontou uma extensiva vigilância de usuários sem garantir a sua devida segurança. Essa análise ocorreu a partir de um relatório divulgado pela Comissão Federal do Comércio dos Estados Unidos ("FTC"), que revelou abusos para promover a monetização em detrimento da proteção de usuários.

O relatório é resultado de intimações emitidas em 2020 a essas empresas com base na Seção 6(b) da lei de comércio federal americana (FTC Act). À época, a FTC buscou informações a respeito de como eram coletados, rastreados e utilizados dados pessoais e informações demográficas. A definição de anúncios e outros conteúdos que seriam direcionados aos consumidores, detalhes sobre a aplicação de algoritmos, inteligência artificial e das análises realizadas a partir dos dados coletados também foram abordados. A FTC focou, ainda, no impacto dessas práticas em crianças e adolescentes.

As conclusões da FTC apontam que o modelo de negócio dessas empresas incentiva a coleta massiva de dados pessoais, inclusive por intermédio de *data brokers*, para alavancar a monetização. O relatório destacou práticas de tratamento de dados de usuários inadequadas, como a retenção de informações por prazo indeterminado, a manutenção de dados mesmo quando recebidas solicitações de exclusão e a ingerência e falta de monitoramento de sistemas automatizados. Foram constatados, ainda, riscos na utilização de tecnologias de rastreamento invasivas, como pixels, para a obtenção de um direcionamento mais preciso de publicidade. Outro ponto elucidado foi a falta de proteção conferida às crianças e adolescentes, visto que, em muitos casos, não eram implementadas medidas adequadas, como a falta de restrições em contas utilizadas por adolescentes.

Dentre as recomendações apontadas pela FTC no relatório estão, entre outras, a revisão de procedimentos e políticas, inclusive para conferir mais clareza aos usuários, a limitação do tratamento somente aos dados necessários às finalidades da coleta, a reanálise das práticas de segmentação de anúncios, a necessidade de estabelecer padrões mais rigorosos de teste e monitoramento de sistemas automatizados e conferir maior proteção às

crianças e adolescentes.

**> Referências:**

<https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance>

<https://istoedinheiro.com.br/gigantes-das-redes-sociais-sao-acusados-nos-eua-de-vigiar-usuarios/>

[https://www.ftc.gov/system/files/ftc\\_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf)

## **RECURSO DO GOOGLE SOBRE QUEBRA DE SIGILO ESTÁ EM CALENDÁRIO DE JULGAMENTO NO STF**

Desde 2018, o Google está em um embate judicial com o Ministério Público do Rio de Janeiro (MP-RJ) a respeito da quebra de sigilo telemático no caso Marielle Franco. Até então, decisões do Tribunal de Justiça do Rio de Janeiro e do Superior Tribunal de Justiça (STJ) determinaram a quebra de sigilo e condenaram o Google a fornecer os endereços de IP e os IDs dos dispositivos de todos os usuários que pesquisaram determinadas palavras-chave relacionadas à Marielle Franco na semana anterior ao seu assassinato, em março de 2018.

Em sede de Recurso Extraordinário, interposto no Supremo Tribunal Federal (STF), o Google alega "preocupação com o risco à privacidade dos brasileiros decorrente de ordens de quebra de sigilo genéricas e não individualizadas, direcionadas a usuários que não são suspeitos ou mesmo investigados."

Foi reconhecida a repercussão geral do tema e o julgamento iniciado em setembro de 2023, mas posteriormente paralisado. À época, apenas a Ministra Rosa Weber havia votado. Na ocasião, Weber se posicionou a favor do Google, reconhecendo que não há dispositivo legal que legitime exigir o fornecimento dessa quantidade de dados pessoais de inúmeros usuários que pesquisaram determinadas combinações de palavras em provedores de aplicação. Em seu voto, a Ministra concluiu que a quebra de sigilo de forma genérica, sem delimitação dos pedidos, seria desproporcional e não estaria amparada pelo Marco Civil da Internet.

O julgamento no STF continua, e a decisão final terá implicações significativas na definição dos limites às solicitações de quebra de sigilo do histórico de buscas em plataformas durante investigações criminais. Em sendo um tema de repercussão geral, o desfecho da decisão servirá de referência para casos semelhantes.

**> Referências:**

<https://oglobo.globo.com/rio/noticia/2024/09/18/caso-marielle-stf-pode-julgar-caso-sobre-entrega-de-dados-do-google.ghtml>

<https://www.cnnbrasil.com.br/politica/stf-retoma-julgamento-sobre-se-google-deve-fornecer-lista-de-quem-pesquisou-sobre-marielle/>

<https://www.noticiasaoiminuto.com.br/politica/2205112/stf-deve-retomar-julgamento-sobre-pedido-de-dados-ao-google-do-caso-marielle>

<https://www.cartacapital.com.br/justica/stf-retoma-julgamento-sobre-acesso-a-dados-de-usuarios-do-google-no-caso-marielle-franco/>

## **PROJETO DE LEI PREVÊ A ADOÇÃO DE MEDIDAS DE SEGURANÇA ADEQUADAS POR ÓRGÃOS PÚBLICOS**

Está em tramitação na Câmara dos Deputados o Projeto de Lei nº 2987/2023 (PL), que altera a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) para assegurar a imutabilidade, a auditabilidade e a segurança de informações.

Para tanto, o PL estipula que órgãos e entidades públicas devem adotar medidas de segurança para garantir adequada proteção aos dados que tratam contra incidentes de segurança da informação, sejam estes acidentais ou causados por ciberataques.

O PL não define quais seriam as medidas de segurança adequadas, mas dispõe sobre a possibilidade daqueles sujeitos ao regime da LAI apresentarem planos estratégicos para a sua implantação.

Parcerias com entidades públicas ou privadas para garantir a adoção das tecnologias apropriadas, bem como a utilização da tecnologia blockchain são meios abordados pelo PL como medidas para viabilizar um nível de proteção efetivo.

A justificativa para a apresentação do PL tem como base os diversos incidentes cibernéticos sofridos por órgãos e entidades públicas, como os que afetaram o STJ em 2020 e o Ministério da Saúde em 2021.

### **> Referências:**

<https://www.camara.leg.br/noticias/1083854-projeto-visa-aumentar-protecao-de-dados-publicos-contrataques-ciberneticos/>

[https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=2286029&filename=PL%202987/2023](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2286029&filename=PL%202987/2023)

## **STJ RECONHECE QUE PROVEDORES DE APLICAÇÃO NÃO SÃO OBRIGADOS A EXCLUIR ANÚNCIOS DENUNCIADOS POR VIOLAÇÃO DE SEUS TERMOS DE USO**

A Terceira Turma do STJ, no julgamento do Recurso Especial nº 2088236/PR, decidiu que plataformas de intermediação de comércio eletrônico, salvo exceções previstas em lei, não são obrigadas a excluir publicações de terceiros que violem seus termos de uso.

No caso em discussão, um anunciante de colchões notificou extrajudicialmente a plataforma na qual anunciava seus produtos para solicitar a exclusão de publicações de concorrentes. O anunciante alegou que publicações ofertando colchões sem a certificação do Inmetro representariam violação aos termos de uso da plataforma.

Em seu voto, a Ministra Nancy Andrighi, ao destacar julgados anteriores do STJ, elucidou que não é possível impor a plataformas de intermediação a responsabilidade de realizar a prévia fiscalização sobre a origem de todos os produtos, por não se tratar de atividade intrínseca ao serviço prestado.

Isso porque plataformas de intermediação de comércio eletrônico seriam classificadas como provedores de aplicação e o Marco Civil da Internet apenas condiciona a responsabilidade dos provedores de aplicação face ao não cumprimento de ordem judicial.

De acordo com Andrighi, as práticas a serem adotadas por plataformas de comércio eletrônico em virtude do descumprimento dos termos de uso não são regulamentadas, devendo, assim, serem considerados os dispositivos do Marco Civil da Internet que tratam da matéria.

Dessa forma, concluiu a Ministra que, salvo exceções previstas em lei, como em casos de violação de direitos autorais ou divulgação de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais publicadas sem autorização de seus participantes, provedores de aplicação tem responsabilidade subjetiva face ao conteúdo gerado por terceiros. Logo, não são obrigados a excluir publicações de usuários que violem seus termos de uso, ainda que mediante requisição ou notificação extrajudicial.

### **> Referências:**

<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/16092024-Mercado-Livre-nao-e-obrigado-a-excluir-anuncios-denunciados-por-violacao-dos-termos-de-uso-do-site.aspx>

<https://valor.globo.com/legislacao/noticia/2024/09/16/stj-mercado-livre-nao-e-obrigado-a-excluir-anuncios-denunciados.ghtml>

[https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento\\_tipo=integra&documento\\_sequencial=241989643&registro\\_numero=202302654234&peticao\\_numero=&publicacao\\_data=20240426&formato=PDF](https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=241989643&registro_numero=202302654234&peticao_numero=&publicacao_data=20240426&formato=PDF)

## IMPLANTAÇÃO DA POLÍTICA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DO SISTEMA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

Em dezembro de 2023, por meio da Resolução nº 281/2023, o Conselho Nacional do Ministério Público (CNMP) instituiu a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público.

As medidas têm como finalidade assegurar integral proteção a dados pessoais e defender o direito à autodeterminação informativa contra lesões de terceiros.

Para efetivar a implementação do Sistema Nacional de Proteção de Dados, a Unidade Especial de Proteção de Dados Pessoais (UEPDAP) do CNMP e a Autoridade Nacional de Proteção de Dados (ANPD) se reuniram, em setembro de 2024, e decidiram elaborar um termo de colaboração mútua. O objetivo primordial é promover a colaboração entre as entidades visando fomentar a tutela do direito à proteção de dados pessoais no país.

A colaboração entre a UEPDAP e a ANPD também inclui o desenvolvimento de processos para o compartilhamento de informações sobre incidentes de segurança, além da atuação conjunta na formulação de estratégias nacionais voltadas para a proteção de dados pessoais.

### > Referências:

<https://www.cnmp.mp.br/portal/todas-as-noticias/17855-cnmp-e-anpd-avancam-nas-tratativas-para-implementacao-do-sistema-nacional-de-protecao-de-dados-pessoais>;

<https://www.cnmp.mp.br/portal/todas-as-noticias/17212-cnmp-institui-a-politica-nacional-de-protecao-de-dados-pessoais-e-o-sistema-nacional-de-protecao-de-dados-pessoais-no-ministerio-publico#:~:text=J%C3%A1%20o%20Sistema%20Nacional%20de,e%20a%20observ%C3%A2ncia%2C%20pelas%20estruturas>

## STJ DECIDE SOBRE EXTENSÃO DA ORDEM DE RETIRADA DE CONTEÚDO A OUTROS PAÍSES

Em setembro, a Terceira Turma do STJ iniciou o julgamento do REsp nº 2147711/SP para analisar se plataformas de busca podem ser obrigadas a apagar também em outros países conteúdos ilícitos perante a legislação brasileira. O caso em tela envolve a veiculação de um vídeo em *streaming*, produzido a partir de conteúdos falsos, que foi alvo de ordem de retirada junto à plataforma de buscas.

A decisão de primeiro grau estabeleceu a obrigação de remover o conteúdo apenas em território nacional. No entanto, o Tribunal de Justiça de São Paulo (TJSP) determinou que a remoção do conteúdo deveria abarcar "toda a extensão da rede mundial de computadores, o que não implica em violação à soberania de outros países".

O TJSP entendeu que o conceito clássico de limite territorial não se aplicaria ao caso por se tratar de veiculação por meio da internet, que tem caráter global. A plataforma de buscas recorreu ao STJ ressaltando que a lei federal brasileira teria sido extrapolada e que questões de soberania deveriam ser consideradas para evitar eventuais violações.

O julgamento no STJ teve voto da Ministra Nancy Andrighi, que seguiu a posição afirmada pelo TJSP. Andrighi ressaltou o alcance transfronteiriço da internet e alegou que o artigo 11 do Marco Civil da Internet estendeu a jurisdição brasileira internacionalmente, sendo aplicável sempre que dados são coletados no Brasil. O Ministro Ricardo Villas Bôas Cueva interrompeu o julgamento e pediu vistas para análise.

#### **> Referências:**

<https://www.conjur.com.br/2022-dez-26/google-apagar-conteudo-difamatorio-brasil-exterior/>

<https://www.conjur.com.br/2024-set-11/stj-analisa-google-pode-ser-obrigado-a-a-pagar-video-em-outros-paises/>

## **STF ANALISA A CONSTITUCIONALIDADE DE DISPOSITIVOS DO MARCO CIVIL DA INTERNET**

Em nosso último Informativo, destacamos os temas do Marco Civil da Internet que estão em discussão no STF e serão analisados de maneira conjunta, em razão da proximidade da matéria. O Presidente do STF, Luís Roberto Barroso, comunicou que essas ações serão julgadas após as eleições, devido à dificuldade de construção de um consenso legislativo sobre o tema.

A respeito desses julgamentos, no início de setembro, a Advocacia-Geral da União (AGU) requereu o ingresso da União no julgamento para participar como *amicus curiae*. A União defende que o artigo 19 do Marco Civil da Internet deve ser interpretado conforme a Constituição Federal, ou seja, para evitar abusos e violações de direitos fundamentais.

Na interpretação da AGU, o artigo 19 trata-se de regra geral que não afasta a aplicação de normas específicas diferentes que também defendem a proteção de outros direitos fundamentais. Provedores de aplicação devem ser responsabilizados, ainda que sem ordem judicial prévia e, de acordo com a AGU, essa interpretação "deve considerar, para tanto, três situações específicas: i) casos de fraude; ii) veiculação de conteúdo publicitário ou impulsionado; e iii) aplicação de regras especiais previstas em legislação específica".

A Associação Brasileira de Provedores de Internet e Telecomunicações (Abrint), em contrapartida, ingressou com uma Ação Direta de Constitucionalidade (ADC 91) para reconhecer a constitucionalidade do artigo 10, §1º do Marco Civil da Internet. O dispositivo prevê que dados de registros de conexão e de aplicação de internet só devem ser disponibilizados por provedores mediante ordem judicial.

A Abrint alega confusão com a disposição constante no §3º, que prevê a disponibilização, sem necessidade de ordem judicial, de dados cadastrais às autoridades administrativas. Assim, alguns dados que não deveriam ser classificados como "cadastrais", como endereço de IP e data e hora de conexão, deveriam ser obtidos apenas mediante ordem judicial. A Abrint alega que o atendimento de solicitações requisitando a disponibilização de tais dados implicaria em quebra de sigilo de comunicações.

#### > Referências:

<https://valor.globo.com/brasil/noticia/2024/09/25/stf-julgara-acoes-sobre-marco-civil-da-internet-e-plataformas-digitais-apos-eleicoes.ghtml>

<https://convergenciadigital.com.br/governo/agu-redes-sociais-sao-responsaveis-por-conteudo-mesmo-sem-ordem-judicial/>

<https://noticias.stf.jus.br/postsnoticias/associacao-pede-que-stf-valide-necessidade-de-ordem-judicial-para-acessar-registros-de-usuarios-na-internet/>

<https://convergenciadigital.com.br/internet/abrint-vai-ao-stf-para-barrar-pedidos-de-identificacao-de-usuarios-sem-ordem-judicial/>

## **STF AUTORIZA MP E AUTORIDADES POLICIAIS A SOLICITAREM DADOS CADASTRAIS DE INVESTIGADOS A EMPRESAS DE TELEFONIA**

No dia 11 de setembro, o Plenário do STF julgou a Ação Direta de Inconstitucionalidade (ADI) nº 4906, movida pela Associação Brasileira de Concessionárias de Serviço Telefônico Fixo Comutado (Abrafix) na qual questiona a validade do artigo 17-B da Lei de Lavagem de Dinheiro.

O referido dispositivo permite que autoridades policiais e o Ministério Público (MP) tenham acesso aos dados cadastrais de pessoas investigadas por crimes de lavagem de dinheiro mantidos pela Justiça Eleitoral, instituições financeiras, empresas telefônicas, provedores de internet e administradoras de cartão de crédito sem a necessidade de autorização judicial prévia.

Inicialmente, os ministros afirmaram que a Abrafix tem legitimidade apenas para representar as empresas de telefonia, e não os demais setores afetados, como a Justiça Eleitoral e instituições financeiras. Por maioria dos votos, foi decidido que o dispositivo é constitucional, destacando que os dados em questão não estão protegidos por sigilo, vez que são fornecidos pelo próprio usuário ao contratar um serviço telefônico. Dessa forma, é permitido acesso às autoridades policiais e ao MP aos dados cadastrais dos investigados por lavagem de dinheiro, sem necessidade de ordem judicial.

No entanto, para evitar o acesso a dados protegidos por sigilo, os ministros restringiram a interpretação do dispositivo legal apenas aos "dados cadastrais" referentes à qualificação pessoal, filiação e endereço dos investigados.

## > Referências:

<https://valor.globo.com/politica/noticia/2024/09/11/stf-mp-e-policias-podem-pedir-as-operadoras-de-telefonias-dados-cadastrais-de-investigados-sem-ordem-judicial.ghtml>

<https://noticias.stf.jus.br/postsnoticias/norma-que-autoriza-mp-e-policia-a-requisitar-de-telefonias-dados-cadastrais-de-investigados-e-valida-decide-stf/>

<https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wp-allimport/uploads/2024/09/11200722/ADI-4906-acesso-a-dados-cadastrais-pelo-MP-e-policia-rev.-LC-FSP-18h52.pdf>

## **CASO X: X CUMPRE DECISÕES DO STF E SOLICITA O SEU DESBLOQUEIO EM MEIO À INVESTIGAÇÃO DE ACESSOS ILEGAIS À PLATAFORMA**

Após a suspensão do funcionamento do X no Brasil, decretada por Alexandre de Moraes no final de agosto em razão do não cumprimento de decisões do STF pela empresa, o caso teve significativos desdobramentos.

Na metade de setembro, a plataforma voltou a funcionar no país em razão da alteração dos registros de seus servidores. O X utilizou um software que mascara endereços de IP, criando obstáculos aos bloqueios de acesso à plataforma determinados por autoridades brasileiras. No entanto, a empresa parou de utilizar o software e retomou seus servidores próprios, assim que o relator do caso, o Ministro Alexandre de Moraes, multou o X e a Starlink pelo descumprimento da medida.

Nesse cenário, a Procuradoria-Geral da República (PGR) solicitou ao STF o início de investigação pela Polícia Federal (PF) para apurar os usuários que acessaram o X de maneira irregular. Os acessos foram realizados após o bloqueio da plataforma, por meio de ferramentas que mascaram endereços de IP, como VPNs. A PF concluiu o levantamento e enviou à Suprema Corte um relatório apontando os usuários que descumpriram a decisão do Ministro Alexandre de Moraes, mas a lista está sob sigilo.

Apesar desse impasse, o X começou a cumprir as decisões impostas pelo STF. Dentre as medidas acatadas, a plataforma bloqueou contas de usuários que foram alvo de decisões judiciais, bem como quitou as multas avaliadas em R\$18 milhões, ao transferir os valores bloqueados do X e da Starlink para a União. Os documentos exigidos por Moraes referentes à indicação de um representante no país também foram apresentados.

Tendo em vista a adoção dessas medidas, o X requereu o restabelecimento da plataforma no Brasil. O pedido no âmbito do processo ainda está sob análise do STF.



## > Referências:

<https://oglobo.globo.com/politica/noticia/2024/09/19/moraes-multa-x-e-starlink-e-m-r-5-milhoes-por-dia-por-descumprimento-de-bloqueio-da-rede.ghhtml>;

<https://oglobo.globo.com/politica/noticia/2024/09/19/x-volta-a-rodar-com-servidores-proprios-e-abandona-escudo-da-cloudflare.ghhtml>

<https://valor.globo.com/empresas/noticia/2024/09/19/a-pedido-da-pgr-pf-vai-investigar-quem-acessou-o-x-de-forma-irregular.ghhtml>;

<https://oglobo.globo.com/politica/noticia/2024/09/24/multas-por-uso-do-x-deve-m-atingir-usuarios-que-espalharem-discurso-de-odio-e-fake-news-define-pgr.ghhtml>

<https://valor.globo.com/politica/noticia/2024/09/25/pf-envia-ao-stf-relao-dos-usuarios-que-acessaram-o-x.ghhtml>

<https://www.dw.com/pt-br/rede-x-come%C3%A7a-a-cumprir-decis%C3%B5es-do-stf/a-70275639>

<https://valor.globo.com/empresas/noticia/2024/09/27/moraes-vai-analisar-pedido-da-rede-x-para-voltar-a-operar.ghhtml>

<https://www1.folha.uol.com.br/colunas/monicabergamo/2024/09/x-comeca-a-cumprir-ordens-do-stf-e-alexandre-de-moraes-diz-que-e-preciso-paciencia.shtml>

<https://www1.folha.uol.com.br/colunas/monicabergamo/2024/09/x-apresenta-dos-dokumentos-exigidos-por-alexandre-de-moraes-e-volta-a-pedir-desbloqueio-no-brasil.shtml>

## Profissionais que aliam visão jurídica e visão de mercado



**Felipe Palhares**



**Fernanda Villela**