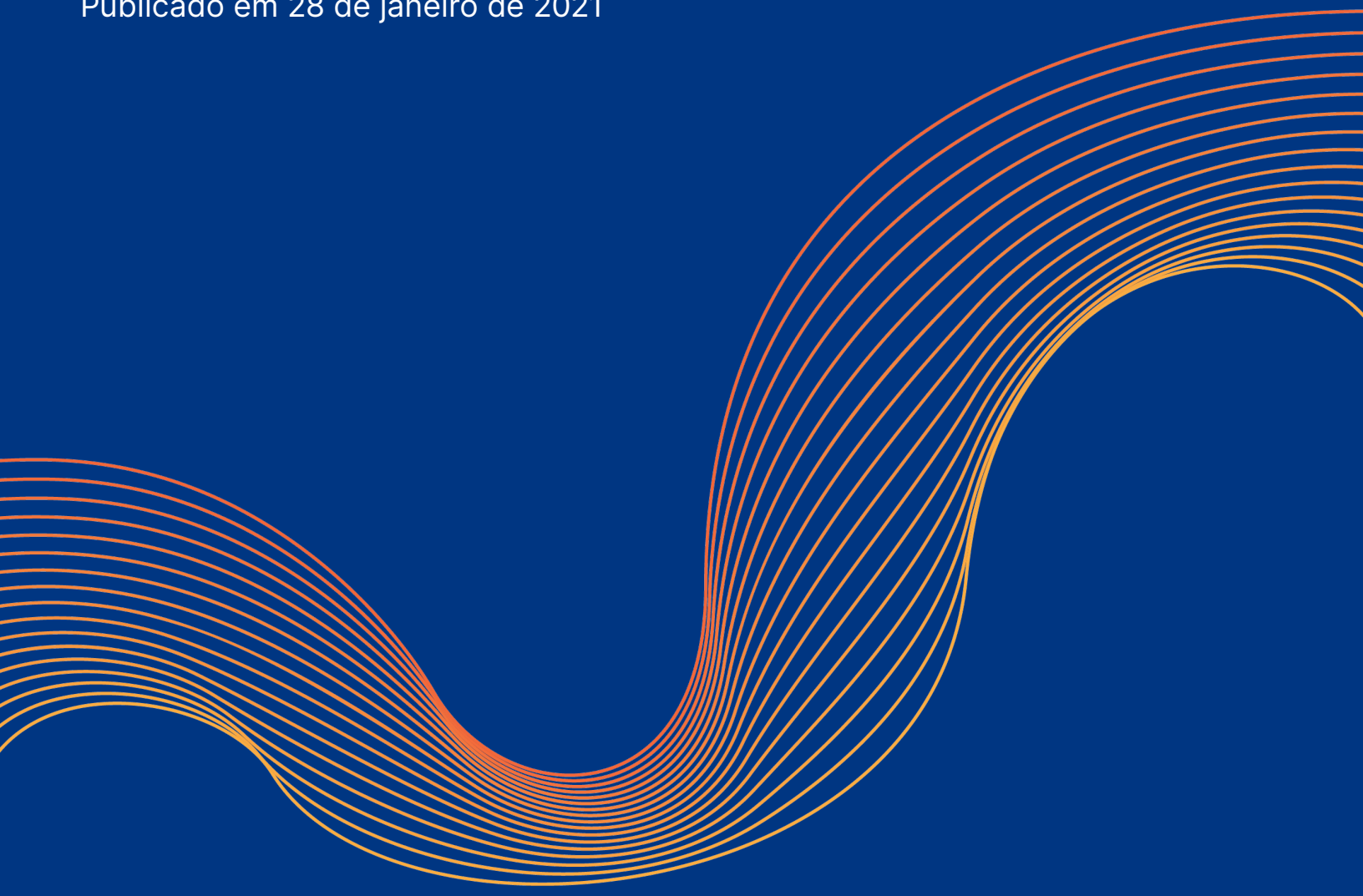
ARTIGO

CLOUDFLARE

Políticas da Cloudflare relativas à privacidade de dados e às solicitações legais

Publicado em 28 de janeiro de 2021



+55 11 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

Em última instância, a rede e os negócios da Cloudflare são todos baseados na confiança do cliente. Buscamos continuamente conquistar e manter essa confiança criando e implantando produtos que ajudam a melhorar a segurança do nosso sistema, a criptografar dados em repouso ou em trânsito e a permitir que nossos clientes determinem como o tráfego é inspecionado em diferentes locais ao redor do mundo.

Porém, nem todos os desafios podem ser solucionados com engenharia. Por esse motivo, também temos políticas e procedimentos que orientam a maneira como gerenciamos dados de clientes e de usuários finais nos nossos sistemas e como tratamos as solicitações legais e governamentais em relação aos dados.

Este artigo descreve essas políticas e fornece links para informações mais detalhadas sobre as várias facetas da nossa abordagem em relação a privacidade de dados e conformidade. Ele abrange especificamente:

- Nossa visão sobre o panorama de privacidade de dados em constante mudança
- Nossas políticas relativas à privacidade e solicitação de dados

O panorama de privacidade de dados em constante mudança

A explosão dos serviços em nuvem — e o fato de que os dados podem ser armazenados fora dos países onde residem aqueles que os geraram — tem sido um desafio para os governos que realizam investigações policiais. Provedores de serviços on-line de todos os tipos costumam servir como um ponto de acesso para esses registros eletrônicos.

Para provedores de serviços como a Cloudflare, solicitações de dados vindas do governo podem ser problemáticas. O trabalho da polícia e de outras autoridades governamentais é importante. Ao mesmo tempo, os dados solicitados pela polícia e outras autoridades governamentais não nos pertencem. Ao usarem nossos serviços, nossos clientes nos atribuem um encargo de confiança no que se refere a esses dados. Manter essa confiança é fundamental para a nossa empresa e os nossos valores.

Essas tensões são agravadas pelo fato de que diferentes governos têm diferentes padrões quando se trata da proteção de dados pessoais. Os Estados Unidos, por exemplo, proíbem que as empresas divulguem o conteúdo de suas comunicações — inclusive com governos de outros países — em todas as circunstâncias, com poucas exceções definidas legalmente. A União Europeia, que há muito tempo considera a privacidade um direito humano fundamental, protege todos os dados pessoais da UE por meio do Regulamento Geral de Proteção de Dados (GDPR). Embora essas proteções se sobreponham em determinados aspectos, ambas diferem quanto ao seu escopo e às pessoas que são protegidas.

As diferenças entre as estruturas jurídicas são importantes, especialmente quando se trata de determinar se as solicitações judiciais de informação por parte de governos estrangeiros precisam ser consistentes com os requisitos de privacidade. Nos últimos anos, por exemplo, o Tribunal de Justiça da União Europeia (TJUE) concluiu, em várias ocasiões, que as restrições legais dos EUA à coleta de dados, juntamente com certos compromissos voluntários como o Escudo de Privacidade (ou seu antecessor, a proteção U.S.-EU Safe Harbor) não se adequavam à conformidade com os requisitos de privacidade da UE, em grande parte devido às leis dos EUA que permitem que as autoridades legais coletem informações sobre cidadãos não americanos para fins de inteligência estrangeira. Com efeito, o Comitê Europeu para a Proteção de Dados (CEPD) assumiu a posição de que uma solicitação de dados ao abrigo do direito penal dos EUA — fora de um processo jurídico no qual os países da UE mantenham algum grau de controle sobre as informações sendo produzidas — não constitui uma base legítima para a transferência de dados pessoais sujeitos ao GDPR.

Essencialmente, trata-se de disputas sobre quando é apropriado que um governo use ordens judiciais ou outros processos legais para acessar dados referentes a cidadãos de outro país. E tais disputas não acontecem apenas na Europa. Embora as respostas de suas políticas não sejam consistentes, um número crescente de países agora encara o acesso aos dados de seus cidadãos como uma preocupação de segurança nacional.

Políticas da Cloudflare relativas à privacidade de dados e solicitações de dados

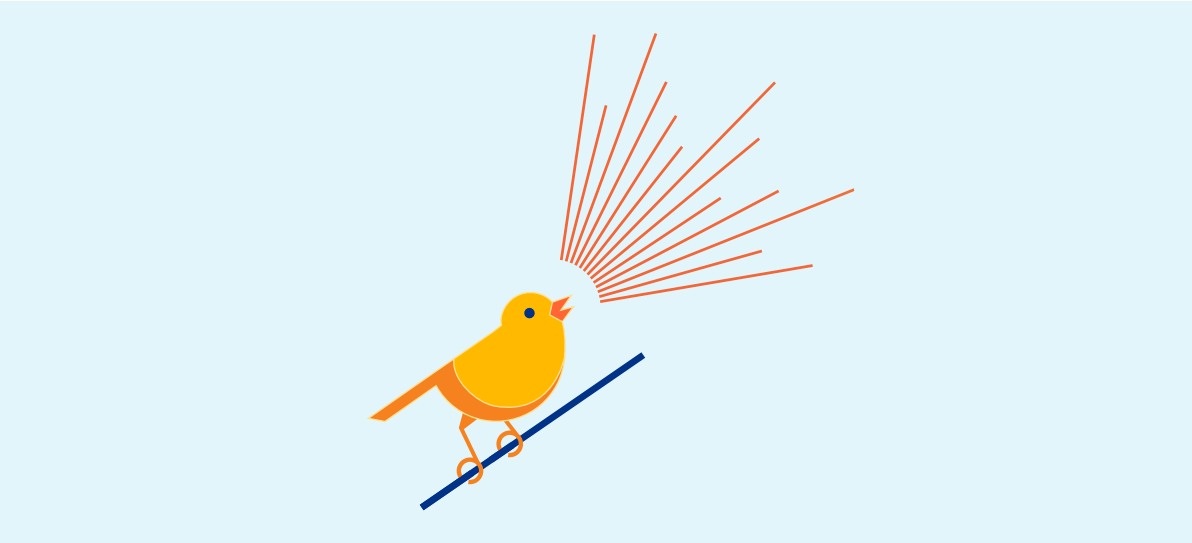
A Cloudflare vem mantendo há muito tempo políticas sobre como abordar preocupações referentes ao acesso a dados pessoais.
Fazemos isso tanto devido ao fato de que é a coisa certa a fazer quanto à certeza de que esses conflitos legais que observamos hoje pareciam inevitáveis. Essas políticas abrangem o seguinte:

- Compromissos assumidos publicamente no que se refere à forma como tratamos dados privados e como lidamos com as solicitações desses dados enviadas pela polícia
- Nossa maneira de informar nossos clientes quanto à existência de tais solicitações de dados

De modo geral, quando existe um conflito entre dois ordenamentos jurídicos diferentes, optamos por aquele que adota a maior proteção de privacidade. E sempre exigimos que haja um processo legal. Isso se deve ao fato de que, uma vez que a porteira dos dados seja aberta, poderá ser difícil fechá-la novamente.

Nossos compromissos públicos referentes a dados privados e solicitações das autoridades policiais

Começando pelo nosso primeiro relatório de transparência em 2013, detalhando as solicitações de dados enviadas por autoridades policiais, assumimos publicamente um compromisso relativo à forma como abordamos solicitações de dados e declarações públicas sobre coisas que nunca fizemos. Chamamos essas declarações públicas sobre coisas que nunca fizemos "canários" de garantia, refletindo a ideia de que cumprem uma função de alerta dirigido ao mundo exterior.



Esses "canários" cumprem duas funções. Em primeiro lugar, trata-se de uma declaração pública de que não tomaremos tais providências voluntariamente. Em segundo, podem constituir um mecanismo para transmitir informações — por meio da remoção da declaração do site — que, de qualquer outra forma, teríamos restrições para divulgar.

As entidades reguladoras começaram a reconhecer o valor dos compromissos de privacidade, em particular quando podem ser aplicados por contrato. De fato, os compromissos que temos incluído nos nossos relatórios de transparência ao longo dos anos são exatamente o tipo de compromisso que a Comissão Europeia recomendou que fosse incluído no seu esboço de Cláusulas Contratuais Padrão para cumprimento do GDPR.

Alguns exemplos importantes desses compromissos na data de publicação deste artigo incluem:

- **Nunca instalamos software ou equipamentos de autoridades policiais em nossa rede nem fornecemos um feed de conteúdo transitando em nossa rede:** como uma empresa de segurança na internet, sabemos que manter o controle sobre o acesso a nossas redes é absolutamente imperativo. Por essa razão, nossa equipe de segurança vem se concentrando em controles de acesso, criação de registros e monitoramento e se submete a diversas avaliações executadas por terceiros a cada ano. Queremos nos certificar de que nossos clientes entendam que não há nenhuma exceção desses controles destinada a beneficiar autoridades policiais ou agentes governamentais.
  Por isso afirmamos que a Cloudflare nunca instalou software ou equipamentos de autoridades policiais em nenhum local na nossa rede e que nunca fornecemos a nenhuma organização governamental um feed de conteúdo de nossos clientes transitando em nossa rede.
- **Nunca compartilhamos chaves de criptografia ou autenticação:** a Cloudflare acredita que uma criptografia forte — tanto para o conteúdo quanto para metadados — é necessária para a privacidade on-line. Se um país busca impedir que um outro governo acesse as informações pessoais de seus cidadãos, o primeiro passo deve ser a criptografia dessas informações pessoais. No entanto, é preciso que os clientes e reguladores também estejam confiantes de que a criptografia propriamente dita é confiável. Portanto, assumimos um compromisso no sentido de que nunca entregamos a ninguém nossas chaves de criptografia ou autenticação — ou chaves de criptografia ou autenticação de nossos clientes — e nunca nos permitimos enfraquecer, comprometer ou subverter nossa criptografia a pedido de autoridades policiais ou de qualquer outro terceiro.
- **Nunca modificamos o conteúdo de clientes ou solicitações de DNS:** não acreditamos que nossos sistemas devam ser explorados para conduzir as pessoas a sites que não pretendiam visitar ou alterar o conteúdo obtido on-line. Portanto, declaramos publicamente que nunca modificamos o conteúdo do cliente nem modificamos o destino pretendido das respostas de DNS a pedido de autoridades policiais ou de qualquer outro terceiro.
- **Transparência em torno de possíveis violações de compromissos assumidos:** nos comprometemos a contestar qualquer ordem judicial no sentido de nos obrigar a violar esses compromissos, nos tribunais de justiça, se necessário. Nosso objetivo é traçar nossos limites com muita clareza — não apenas junto a nossos clientes, mas também junto aos governos do mundo inteiro.

Embora nossa filosofia de proteção de dados tenha de modo geral se mantido inalterada desde a nossa fundação, ocasionalmente adaptamos nossos compromissos de modo a refletir as mudanças mais recentes em nossos produtos e no panorama de políticas. Uma lista completa e atualizada desses compromissos está disponível na nossa página de Relatórios de Transparência.

Notificar nossos clientes no caso de solicitações governamentais

A Cloudflare acredita há muito tempo que nossos clientes merecem ser notificados quando qualquer pessoa — inclusive uma autoridade policial ou outros agentes governamentais — utiliza processos judiciais para solicitar seus dados. Essas notificações permitem que nossos clientes contestem tais solicitações caso estejam preocupados.

Na verdade, já nos nossos primeiros dias como uma empresa adotávamos uma política de notificar nossos clientes nessas oportunidades. Em janeiro de 2013, quanto tínhamos menos de 30 funcionários, o FBI apareceu em nosso escritório com uma intimação na forma de uma Carta de Segurança Nacional solicitando informações sobre um cliente e nos proibindo de discutir o fato com qualquer pessoa além de nossos advogados. Naquela época, as Cartas de Segurança Nacional não tinham praticamente nenhuma supervisão, podendo ser emitidas e implementadas por um único poder do governo americano, além de forçosamente impedir indefinidamente seus destinatários de falarem sobre ela.

Reconhecemos que podem haver circunstâncias nas quais possa ser adequado que as autoridades policiais restrinjam temporariamente a divulgação para preservar a viabilidade de uma investigação. No entanto, também acreditamos que o governo deveria ser obrigado a justificar qualquer disposição de não divulgação e que qualquer disposição de não divulgação deveria ser explicitamente limitada ao tempo mínimo necessário para a finalidade em questão. Neste diapasão, trabalhamos junto à Fundação Fronteira Eletrônica para contestar a intimação judicialmente.

O processo judicial resultante demorou vários anos e ficamos impedidos de falar sobre isso até 2017. Porém, em última instância, o FBI cancelou a intimação.

Devido ao fato de os tribunais dos EUA terem sugerido que ordens de não divulgação por um tempo indefinido constituem um problema em termos constitucionais, o Departamento de Justiça dos EUA emitiu uma orientação em 2017 instruindo os promotores federais a limitarem as ordens de não divulgação ao prazo máximo de um ano, exceto em circunstâncias excepcionais. No entanto, isso não impediu todas as autoridades policiais dos EUA de emitirem ordens de não divulgação com prazo indefinido. Na data da publicação deste artigo, tínhamos recebido pelo menos 28 ordens de não divulgação que não incluíam uma data de expiração desde 2017. Trabalhando junto à União Americana pelas Liberdades Civis (ACLU), a Cloudflare ameaçou mover ações judiciais por ocasião do recebimento dessas ordens de não divulgação com prazo indefinido. Em cada caso, o governo subsequentemente adicionou limites de tempo aos requisitos de não divulgação das ordens em questão, o que nos permitiu notificar nossos clientes quanto a tais solicitações.

Nossa abordagem dos conflitos legais

Cumprir leis como o GDPR, particularmente quanto a ordens legais que possam pôr-nos na difícil posição de nos ser pedido que o violemos, exige que sejam envolvidos tribunais. Um provedor de serviços como a Cloudflare pode pedir a um tribunal que anule pedidos legais devido a conflitos de legislação, tendo-nos comprometido - tanto em declarações públicas como contratualmente, através da nosso Adendo de Processamento de Dados - a tomar essa medida quando necessário para evitar tais conflitos. A nossa posição é de que o conflito deve ser remetido de volta à esfera à qual pertente — entre dois governos que disputam quem deve ter direito a aceder à informação.

Conclusão

Este artigo constitui apenas uma apresentação dos nossos amplos e profundos compromissos com a privacidade de dados.
Para maiores informações sobre esses compromissos, confira:

- **Nossa política geral de privacidade:** abrange informações sobre quais dados coletamos, como os usamos, quais dados compartilhamos e outras dúvidas comuns relativas à privacidade.
- **Nossos relatórios de transparência:** informações atualizadas sobre as solicitações judiciais que recebemos no sentido de divulgar informações sobre nossos clientes.
- **Nossa página inicial de conformidade e privacidade de dados:** os mais recentes comunicados sobre como nossas políticas e produtos atendem às necessidades de privacidade e conformidade.

Em última instância, administrar uma rede global que protege os dados de clientes e de usuários finais — e cumpre as diferentes leis de privacidade do mundo inteiro — requer que voltemos aos valores que defendemos desde nossos primeiros dias como empresa: obedecer nossos princípios e manter a transparência, respeitar a privacidade, requerer os devidos procedimentos judiciais e notificar os clientes para que possam tomar suas próprias decisões referentes aos seus dados.