Modelo de Políticas para Intermediários da Internet e Conteúdo

Janeiro de 2025

Internet Society

Resumo executivo

Sem as funções intermediárias que transportam o tráfego da Internet de e para os endpoints (incluindo indivíduos, servidores, provedores de serviços e muitos outros), e sem os diversos outros tipos de funções intermediárias que facilitam esse tráfego, a Internet não existiria.

As funções intermediárias são essenciais para a existência da Internet. Este documento apresenta uma estrutura para compreender tais funções e desenvolver políticas relacionadas à responsabilidade pelo conteúdo online, sem prejudicar a capacidade dos indivíduos de utilizar a Internet para criar conteúdo e se comunicar-se uns com os outros.

Nosso foco está nas funções desempenhadas pelos intermediários da Internet para facilitar a comunicação online, como transmissão, roteamento, armazenamento, cache, hospedagem, segurança, curadoria e moderação de conteúdo. Esse foco reconhece que muitos intermediários desempenham múltiplas funções que levantam diferentes questões políticas e que vários tipos de intermediários oferecem funções essencialmente equivalentes, mesmo que seus serviços possam parecer bastante distintos.

Nosso objetivo neste documento é ajudar os formuladores de políticas a compreender essas funções e desenvolver políticas relacionadas a elas. Quando bem planejadas, estas políticas podem aprimorar a disponibilidade, a diversidade, a segurança e a privacidade da participação individual online. No entanto, políticas mal concebidas podem enfraquecer a segurança da Internet, prejudicar a concorrência, restringir a comunicação online, ampliar a exclusão digital e fragmentar a Internet.

Nosso objetivo não é isentar os intermediários de responsabilidade, mas sim enfatizar o papel crucial das proteções de responsabilidade na viabilização da participação individual na Internet. Políticas mal planejadas focadas nos intermediários podem ter efeitos prejudiciais para a Internet e a comunicação. Alternativas melhores, como as já existentes leis de privacidade, proteção do consumidor e combate à discriminação, estão muitas vezes disponíveis.

Neste documento, discutimos o **desenvolvimento das proteções de responsabilidade dos intermediários** e a motivação por trás delas, começando pela Seção 230 dos EUA, o Marco Civil da Internet do Brasil

e a Diretiva de Comércio Eletrônico e a Lei de Serviços Digitais da UE. Explicamos por que essas e outras leis semelhantes têm sido cruciais para o crescimento da Internet e para a capacidade dos indivíduos de participar online.

Também destacamos **algumas tendências de formulação de políticas voltadas para intermediários,** como regimes de notificação e retirada, moderação de uploads e requisitos específicos por faixa etária. Observamos que essas abordagens apresentam um risco de prejudicar a Internet ao comprometer suas operações técnicas e confiabilidade, enfraquecer a segurança e a privacidade, reduzir a concorrência, bloquear excessivamente conteúdos legais e excluir usuários da participação na Internet.

Este documento oferece os seguintes princípios para a formulação de políticas:

1. **Realizar uma avaliação de impacto na Internet** para entender se uma política proposta, relacionada às funções intermediárias ou de forma mais ampla, pode ter algum efeito adverso na Internet e suas operações.
2. **Delimitar cuidadosamente qualquer política proposta** à função intermediária específica que está causando o problema, estar atento a possíveis danos colaterais e; evitar afetar um conjunto excessivamente amplo de funções e entidades.
3. **Proteger as funções intermediárias de responsabilidade pelo conteúdo criado por terceiros,** incluindo "conteúdo gerado por usuários". As entidades que desempenham funções intermediárias devem ser protegidas de responsabilidade pelo conteúdo criado por terceiros que elas transmitem, recebem, hospedam, exibem, filtram ou, de outra forma, manipulam. Isso garante que os usuários possam continuar a se expressar e compartilhar conteúdo online.
4. **Proteger as funções intermediárias de curadoria e moderação de conteúdo gerado por usuários**. As entidades que hospedam conteúdo gerado por usuários têm o direito legítimo de estabelecer as "regras de conduta" para seus serviços e devem ser protegidas de responsabilidade por aplicar suas próprias regras e remover conteúdo inadequado.

5. **Para abordar preocupações relacionadas ao conteúdo online, formuladores de políticas podem utilizar leis existentes ou novas** que se concentram em: privacidade e segurança, não discriminação, acessibilidade, direitos humanos, concorrência, escolha e controle do usuário, transparência e abertura, entre outros.

Incluímos diversos **"Destaques"** sobre considerações de políticas para setores específicos online, incluindo redes sociais, redes federadas, jogos online, realidade aumentada/realidade virtual, publicidade, bem como modelos de negócios baseados em pagamento por conteúdo, gestão de discursos protegidos, direitos autorais e inteligência artificial (IA).

O **Anexo** ao final deste documento examina a ampla variedade de **funções intermediárias** que permitem ou facilitam as comunicações na Internet. Ele fornece uma listagem **detalhada** e descrição das funções intermediárias, além de incluir considerações técnicas e práticas para a formulação de políticas, bem como recomendações de políticas para cada função.

Sumário

Internet Society

1 Introdução

Este documento oferece um modelo para entender as funções intermediárias da Internet e desenvolver políticas relacionadas à responsabilidade por conteúdo online. As funções intermediárias da Internet facilitam a entrega e a exibição de conteúdo ou as comunicações pela Internet. Provedores de Serviços de Internet (ISPs, na sigla em inglês), sites de mídias sociais, provedores de hospedagem na web, serviços de streaming e serviços de e-mail são todos exemplos de entidades que fornecem funções intermediárias. Nosso objetivo é incentivar formuladores de políticas a elaborar políticas que preservem o que consideramos as características mais importantes da Internet: ser aberta, globalmente conectada, segura e confiável.

Neste documento, fornecemos uma visão geral da Internet e de algumas funções intermediárias significativas para auxiliar os formuladores de políticas que atuam na área de conteúdo online. Discutimos como as políticas que se concentram na Internet podem afetar as funções intermediárias e as interações dos usuários e, em alguns casos, prejudicar a segurança, confiabilidade e outras características essenciais desejáveis da Internet. Por fim, fornecemos recomendações específicas para os formuladores de políticas que buscam abordar objetivos sociais e políticos por meio de políticas que afetam as funções intermediárias da Internet e as entidades que as fornecem.[1]

O Que São Políticas e Como Elas São Implementadas?

As políticas que afetam a Internet podem assumir várias formas e incluir: obrigações legais, proteções legais, regulamentações administrativas, acordos internacionais, incentivos fiscais, reembolsos, esquemas de certificação, requisitos de aquisição e até mesmo decisões de **não** legislar ou regular.

1 Sob os regimes de proteção contra responsabilidade para intermediários aplicáveis à Internet, o foco está nas funções intermediárias que apoiam a criação, descoberta, busca, curadoria, entrega ou exibição de conteúdo. Isso pode incluir e-mails, tweets e outras publicações de indivíduos, bem como textos, áudios ou vídeos que são hospedados e exibidos em sites e grandes plataformas online. Esses regimes de responsabilidade, geralmente, não cobrem outros tipos de entidades que fornecem um serviço de "intermediário", como a transferência de dinheiro de uma pessoa para outra, e este artigo não aborda esse tipo de serviço não focado em conteúdo.

1.1 Desafios de Políticas Relacionados Aos Intermediários

Conforme explicado abaixo na Seção 2, uma ampla variedade de funções intermediárias é necessária para o funcionamento da Internet. Consequentemente, as políticas que se aplicam às entidades intermediárias da Internet ou às funções que elas desempenham também podem afetar significativamente a capacidade dos indivíduos de criar conteúdo e se comunicar uns com os outros.

A influência de políticas nesse processo pode ser positiva e construtiva. Acreditamos que a maioria dos formuladores de políticas reconhece o valor da Internet em seu trabalho. As políticas podem melhorar a forma como os indivíduos e as comunidades experimentam a Internet, por exemplo, incentivando os serviços a garantir a segurança dos dados e a proteger a privacidade de seus usuários, e podem aproveitar o poder da Internet como uma força para o bem na sociedade.

Entretanto, também é possível que haja consequências negativas significativas provenientes da elaboração de políticas: enfraquecimento da segurança e privacidade da Internet, eliminação de concorrentes menores e desestímulo a novos entrantes, danos à capacidade dos usuários de se comunicarem online, ampliação da exclusão digital e fragmentação da Internet. Acreditamos que os formuladores de políticas querem evitar essas consequências negativas, e esse é um dos motivos pelos quais a Internet Society está publicando este documento.

Para os formuladores de políticas que consideram políticas que se aplicam à Internet, é essencial considerar os muitos e diversos tipos de funções intermediárias críticas para a comunicação na Internet. Além disso, é importante lembrar que as próprias entidades que fornecem as funções intermediárias são extremamente diversas, incluindo provedores rurais, pequenas e grandes empresas de hospedagem de sites, serviços de backbone da Internet e enormes sites de compartilhamento de vídeo e mídias sociais. Essa diversidade significa que é crucial que quaisquer obrigações propostas sejam direcionadas à função intermediária precisa da forma mais restrita possível.

Reconhecemos que nem todo conteúdo na Internet é legal e benéfico para a sociedade, bem como que os países estão em busca de formas eficazes de limitar a disseminação de desinformação, conteúdo prejudicial e atividades criminosas online. Nesse sentido, os intermediários podem

apresentar um alvo atrativo para políticas devido à sua extensa interação com o conteúdo gerado pelos usuários. Não estamos argumentando que as entidades que desempenham funções intermediárias "não podem" ou "não devem" estar sujeitas a políticas de alguma forma. Nosso objetivo é mostrar que as políticas que afetam as funções intermediárias podem ter consequências significativas e não intencionais, além de prejudicar a Internet ou a capacidade das pessoas de se comunicarem pela Internet e, portanto, devem ser evitadas. Também destacamos uma variedade de ferramentas relacionadas a políticas, como leis de privacidade robustas, que os governos possuem para abordar questões sociais online.

1.2 A Internet Transformou As Comunicações Com Fortes Impactos Sociais e Econômicos Positivos

A Internet transformou drasticamente a forma como as pessoas se comunicam. Antes da era da Internet, o telefone e o correio eram as principais ferramentas disponíveis para comunicação entre as pessoas. Os meios de comunicação de massa, como jornais, televisão e rádio, ofereciam aos indivíduos pouca capacidade de se expressar e participar.

A Internet, em forte contraste com os jornais, o rádio e a televisão, capacita os indivíduos a participar da conversa, em tempo real e ao redor do mundo. O espectro de opções habilitadas para a Internet inclui comunicações de um para um (*por exemplo*, aplicativos de

A Internet fortalece a participação

O objetivo da Internet Society ao redigir este documento é explicar por que as funções intermediárias pensadas para habilitar e facilitar a comunicação de conteúdo gerado por usuários devem ser protegidas da responsabilização. Também desejamos destacar que existem outras ferramentas relacionadas a políticas disponíveis para abordar de forma construtiva as preocupações sobre os serviços online e o conteúdo de seus usuários. Não é nossa intenção aconselhar os formuladores de políticas sobre como regular a Internet, mas sim sobre como criar políticas que permitam que o resultado mais importante da Internet, as comunicações individuais, continue a florescer.

"Uma característica principal da Internet, uma que a distingue de todos os outros meios de comunicação, é que ela foi feita para ser aberta a todos. Os indivíduos podem falar, debater, criar, inventar e interagir com outros, estejam eles do outro lado da cidade ou ao redor do mundo." (Depoimento perante o Congresso de Andrew Sullivan, CEO da Internet Society, em 08 de março de 2023)

mensagens criptografadas), de um para muitos (*por exemplo,* publicação de um site) e de muitos para muitos (*por exemplo,* plataformas de mídias sociais). Em seus primórdios, a Internet apoiou comunicações por meio de quadros de avisos, listas de discussão, grupos de discussão, blogs e uma infinidade de outras formas de engajamento do usuário.

A capacidade dos indivíduos de usar a Internet para comunicações, enviando e recebendo informações de outras pessoas na própria cidade ou ao redor do mundo, também proporciona benefícios diretos, que introduzem vantagens para esses indivíduos, suas comunidades e seus países. As pessoas estão usando a Internet para criar novas oportunidades sociais e econômicas para si mesmas e para os outros. Empreendedores podem desenvolver produtos e serviços que atendam às necessidades de suas comunidades, enquanto governos podem interagir com seus cidadãos de forma muito mais robusta, rápida e com menor custo. As comunicações facilitadas pela Internet aprimoram o conhecimento global e as oportunidades econômicas. Além desses benefícios, a Internet claramente criou oportunidades econômicas para países, empresas, organizações e pessoas ao redor do mundo.[2]

1.3 A Internet Capacita Comunicações Ativas e Individuais

Com a Internet, os indivíduos não são mais meros receptores passivos de conteúdo criado principalmente por corporações ou sancionado por governos. As pessoas são participantes ativas na criação de conteúdo e na forma como esse conteúdo pode ser disponibilizado para outros ao redor do mundo. Neste documento, usamos o termo "**conteúdo gerado pelo usuário**" para nos referir a qualquer coisa publicada ou compartilhada online por um usuário, e não pelo proprietário de um site.

O conceito de **conteúdo gerado pelo usuário** frequentemente surge em casos legais e debates sobre políticas a respeito de quem deve ser legalmente responsável por esse conteúdo. O **conteúdo gerado pelo usuário** pode ser uma obra original criada pelo próprio usuário que a publicou na Internet ou pode ter sido criado por outra pessoa e publicado, com ou sem a permissão do criador original.

2 Como observado no relatório da OCDE de 2010 sobre O Papel Econômico e Social dos Intermediários da Internet, o crescimento das entidades que fornecem funções intermediárias na Internet contribuiu para os seguintes aspectos: crescimento econômico e produtividade, investimento em infraestrutura, aumento do emprego e empreendedorismo, inovação, capacitação dos usuários, escolha, confiança e privacidade. Consulte https://doi.org/10.1787/5kmh79zzs8vb-en

A principal característica que define o **conteúdo gerado pelo usuário** é que ele foi criado ou publicado em um site ou compartilhado online por alguém que não seja o proprietário do site ou do serviço. Ele se distingue do "**conteúdo original do site**", ou seja, conteúdo criado pelos funcionários, contratados e serviços de desenvolvimento de conteúdo do proprietário do site, pelo qual o proprietário do site tem responsabilidade legal clara.

O espectro de conteúdo gerado pelo usuário é amplo. Pode ser conteúdo publicado por indivíduos, mas também pode ser publicado por uma organização ou corporação. Há uma variedade ilimitada de tipos de **conteúdo gerado pelo usuário**: publicações em mídias sociais, e-mails, mensagens, vídeos curtos ou longos, avaliações de produtos, poesias, música ou dados de observação de cientistas cidadãos. O **conteúdo gerado pelo usuário** pode ser sério, bobo, artístico, factualmente correto, factualmente incorreto, inteligente, ofensivo, assediante, profundo, útil, inútil — qualquer coisa no vasto espectro de ideias e expressões humanas. Mas, é claro, alguns podem ser prejudiciais, difamatórios, enganosos, ameaçadores ou até mesmo ilegais.

Conteúdo Original do Site em Comparação Com Conteúdo Gerado Pelo Usuário

Se um fabricante de automóveis decidir criar um site básico para exibir os novos modelos de automóveis disponíveis para compra, o conteúdo desse site seria criado pelo fabricante e seus funcionários e contratados. Assim como o fabricante de automóveis é responsável pelo conteúdo de um folheto ou outro documento impresso, este também é igualmente responsável pelo conteúdo que publica online. Chamamos esse conteúdo de **conteúdo original do site**. Em geral, o fabricante teria uma responsabilidade clara e possível responsabilidade legal pelo conteúdo que criou e disponibilizou online.

Se o fabricante de automóveis optar por adicionar funcionalidades interativas ao site e permitir que visitantes individuais publiquem comentários sobre os modelos de automóveis, esses comentários seriam **conteúdo gerado pelo usuário**. O site teria uma mistura de conteúdo original do site e algum conteúdo gerado pelo usuário.

Em contraste, um site típico de mídia social para entusiastas de automóveis provavelmente conteria predominantemente **conteúdo gerado pelo usuário**: os visitantes do site publicam

conteúdo longo e curto e discutem com outros visitantes. Algum **conteúdo original do site** criado pelos proprietários do site pode estar presente, como informações de suporte e termos de uso.

A questão da responsabilidade e da responsabilidade civil pelas entidades que fornecem funções intermediárias que ajudam a facilitar a comunicação de **conteúdo gerado pelo usuário** é um tema central discutido neste documento.

1.4 O Papel das Funções Intermediárias na Viabilização da Comunicação na Internet

A Internet não existiria sem as entidades que fornecem funções intermediárias. Sua arquitetura descentralizada e distribuída fundamental, que é essencial para possibilitar os benefícios sociais e econômicos da Internet, depende das centenas de milhares de entidades que fornecem funções intermediárias.

As funções intermediárias da Internet incluem a entrega, segurança, hospedagem e facilitação das comunicações na Internet. Para entender melhor as funções intermediárias na Internet, pode ser útil realizar uma comparação com os serviços postais. Esses serviços utilizam muitos intermediários diferentes para entregar as correspondências: transportadores que coletam e entregam as correspondências, caminhões e aviões para transportar as correspondências, seguranças para proteger as correspondências, caixas de correio para armazená-las, agências para administrá-las, entre outros. Todas essas entidades são agentes do serviço postal.

A Internet possui entidades intermediárias que realizam serviços e funções análogas, mas com uma diferença essencial: as funções intermediárias da Internet são fornecidas por entidades independentes, e não há um escritório central de coordenação controlando a entrega das comunicações. Os serviços postais controlam como as correspondências são entregues a partir do ponto em que são recebidas; na Internet, não há uma única entidade controlando como o conteúdo é entregue ou quem é responsável por cada etapa do processo. Além disso, ao contrário dos serviços postais, o conteúdo na Internet é quase sempre dividido em partes que são transmitidas separadamente e podem passar por redes independentes diferentes. Adicionalmente, ao contrário dos serviços postais, muitas páginas de sites são compostas por componentes dinâmicos criados e hospedados por diferentes entidades.

Os protocolos técnicos abertos e interoperáveis da Internet são o que permitem que uma grande diversidade de comunicações, incluindo páginas da web compostas dinamicamente, sejam transmitidas sem um controlador central.

No entanto, em ambos os casos, tanto o serviço postal e seus agentes quanto os vários intermediários envolvidos nas comunicações na Internet, estão comunicando conteúdo gerado pelo usuário. Porém, as funções dos intermediários são diferentes.

Neste documento, optamos por focar nas "funções" intermediárias (como "fornecer acesso à Internet") em vez de tipos de entidades (como "provedor de serviço de Internet" ou "site de mídia social"). Acreditamos que essa abordagem fornece maior rigor e precisão ao definir políticas, pois muitas entidades realizam múltiplas funções intermediárias diferentes, e essas funções diferentes levantam questões sobre políticas distintas.

Por exemplo, um Provedor de Serviço de Internet (ISP), além de fornecer acesso à Internet para residências, pode realizar funções intermediárias adicionais, como telefonia VoIP, consulta de DNS, hospedagem de e-mail e filtragem de conteúdo ou de malware. Uma plataforma de mídia social, além de fornecer aos seus membros a capacidade de publicar e reagir ao conteúdo, pode realizar outras funções intermediárias, como mensagens individuais, hospedagem de sites e videoconferência ao vivo. Além disso, alguns serviços online podem incorporar as mesmas ou equivalentes funções intermediárias. A introdução de políticas ou regras, por exemplo, sobre o uso de conteúdo incorporado em sites de mídias sociais, pode inadvertidamente impactar o uso de conteúdo incorporado na Internet por todos.

Nosso foco está nas funções intermediárias da Internet que, de alguma forma, estão envolvidas na exibição, descoberta, curadoria ou entrega de *conteúdo criado* **por terceiros**, ou seja, conteúdo gerado pelo usuário.

1.5 Comparação Entre Responsabilidade Por Conteúdo Gerado Pelo Site e Conteúdo Gerado Pelo Usuário

Um ponto de partida para a comparação é que quem cria conteúdo online é responsável por ele, e não é considerado um intermediário para esse conteúdo. No entanto, se esse indivíduo transmitir, exibir, hospedar ou, de

outra forma, facilitar conteúdo criado *por terceiros*, ele seria considerado um intermediário e, geralmente, não seria legalmente responsável por esse conteúdo.

Para algumas entidades, *todo* o conteúdo em seus sites ou serviços é criado "por terceiros". Outros sites de entidades podem conter uma mistura de conteúdo criado "por terceiros" (e, portanto, merecendo proteções contra responsabilidade de intermediários) e conteúdo que elas mesmas criaram (e, portanto, não protegido contra responsabilidade). Três exemplos podem ajudar a ilustrar a distinção:

- Para um Provedor de Serviço de Internet residencial, todo o conteúdo transmitido para e a partir daquela residência é criado por uma entidade distinta do provedor. O provedor não cria conteúdo algum; ele é apenas responsável por transportá-lo. O provedor, normalmente, fornece funções intermediárias apenas para o conteúdo que ele manuseia entre o usuário final e o resto da Internet. Do ponto de vista da responsabilidade, o provedor não é responsável pelo conteúdo que transporta.
- Para um fabricante de automóveis com um site que descreve seus produtos, mas *também* permite que os usuários publiquem avaliações ou comentem sobre o conteúdo, a empresa é responsável pela maior parte do conteúdo no site e não é vista como fornecedora de uma função intermediária para aquele conteúdo específico. No entanto, a empresa ***está*** *fornecendo uma função intermediária* com relação aos comentários dos clientes publicados no site da empresa. Isso porque esses comentários foram criados por alguém diferente da empresa. O fabricante de automóveis é legalmente responsável pelo conteúdo que criou e publicou, mas o conteúdo publicado por terceiros exige uma abordagem diferente em relação à responsabilidade.
- Para a empresa independente de hospedagem de sites que opera os servidores e a infraestrutura usados pelo fabricante de automóveis, a função é puramente intermediária: *todo* o conteúdo no site (criado pela empresa de automóveis, juntamente com os comentários dos clientes) é conteúdo gerado pelo usuário. Assim como o ISP, a empresa de hospedagem de sites não deve ser responsabilizada pelo conteúdo publicado por terceiros nos sites que hospeda.

Importância das Funções Intermediárias Para a Capacidade dos Indivíduos de Usar a Internet e Compartilhar Conteúdo

A nível de vizinhança, as pessoas dependem de intermediários — provedores e redes comunitárias — para se conectar à Internet.¬¬ Uma vez conectados, *toda* comunicação pela Internet exige a participação de várias entidades independentes que fornecem funções intermediárias para transportar, hospedar, proteger e entregar bilhões de comunicações todos os dias.

Todos usam a Internet para coisas diferentes, mas qualquer uso exige que as pessoas, muitas vezes sem saber, acessem e dependam de dezenas, centenas ou mais entidades fornecendo funções intermediárias a cada hora em que estão online. Essa dependência das funções intermediárias é fundamental para o funcionamento diário da Internet. Por esse motivo, as políticas que afetam as funções intermediárias devem ser elaboradas com muito cuidado, para não afetar negativamente o funcionamento da Internet.

2 A Internet e a Responsabilidade dos Intermediários

Esta seção faz uma breve revisão de alguns aspectos técnicos da Internet e introduz algumas características importantes, parte do que chamamos de "o modo como a Internet se conecta em rede". Também descrevemos o papel crítico que as funções intermediárias e as entidades que as fornecem desempenham em todas as comunicações pela Internet.

2.1 As Falhas Críticas do Modelo de Comunicação Com "Comutação de Circuitos" do Século XIX Que Antecederam a Internet

Antes da Internet, o principal sistema de comunicações entre pessoas era o sistema telefônico com "comutação de circuitos", no qual os comutadores eram usados para criar um circuito elétrico dedicado entre o originador de uma ligação telefônica e o destinatário. Sessenta anos atrás, para possibilitar uma ligação telefônica de Nova York a Joanesburgo, a empresa telefônica americana conectaria fiações locais para criar um circuito que se conectaria a um cabo submarino que, por sua vez, se conectaria à empresa telefônica sul-africana. A empresa telefônica sul-africana, então, montaria um circuito do outro lado para levar as vozes através do oceano. Após a ligação, o circuito seria desmontado e os recursos usados na chamada estariam disponíveis para realizar outra ligação telefônica. Durante a maior parte do século 20, a maioria das chamadas telefônicas dentro de um país era tratada por uma única empresa monopolista de telefonia que controlava a rede, cobrava pelas chamadas e era responsável pela manutenção e expansão da rede. Em alguns países, as empresas eram de propriedade ou operadas pelo governo.

A abordagem de comutação de circuitos da telefonia tradicional é extremamente ineficiente. A reserva de recursos necessária para uma

chamada telefônica significava que uma residência ou comunidade com uma única linha telefônica só poderia ter uma conversa por vez e talvez tivesse que esperar até que as linhas para o destinatário estivessem disponíveis. A rede precisaria ser superdimensionada para lidar com picos de carga, e os custos eram muito altos. Muitas vezes, havia capacidade insuficiente durante horários de pico, como épocas festivas como o Natal e a véspera de Ano Novo. O uso de um circuito dedicado para uma única chamada telefônica era ineficiente por si só, porque os fios podiam carregar mais conteúdo do que uma única chamada. A ineficiência técnica e econômica da telefonia tradicional foi um fator crítico no desenvolvimento das redes "comutadas por pacotes", a base para a Internet de hoje.

A telefonia com comutação de circuitos tinha outros riscos e custos. Uma rede com controle centralizado e estrutura hierárquica é vulnerável a interrupções causadas por falhas de centros de comando ou partes da rede[3]. A empresa nacional de telefonia monopolista, sem incentivo para introduzir novos produtos e serviços no mercado, tendia a sufocar a inovação em serviços para o consumidor com regulamentação onerosa ou custos inacessíveis. Pode ser que uma competição adicional na telefonia com comutação de circuitos tivesse levado a mais inovação, mas a centralização intrínseca da comutação de circuitos significava que, em algum momento, toda rede ficaria sob o controle exclusivo de uma entidade, que teria pouco incentivo econômico para investir em novos serviços.

Esses e outros inconvenientes levaram os pesquisadores nas décadas de 1960 e 1970 a desenvolver e aprimorar a "comutação por pacotes" e, por fim, a desenvolver o que se tornou a Internet.

2.2 Compreendendo o Modo Como a Internet se Conecta em Rede

Muitas vezes chamada de "rede de redes", a Internet é uma rede conectada formada por dezenas de milhares de redes que escolheram se conectar umas com as outras. Os primeiros projetistas da Internet reconheceram os benefícios de um design flexível para permitir o surgimento de novas tecnologias e para que novas redes se conectassem. Eles também perceberam que a melhor forma de implementar uma rede muito grande e distribuída era aproveitar as redes existentes, conectando-as com tecnologias simples, de baixo custo e amplamente disponíveis.

3 A Internet, em comparação, é altamente distribuída, o que melhora sua confiabilidade e robustez, além de sua capacidade de contornar problemas de rede.

Ao contrário da telefonia com comutação de circuitos, as comunicações pela Internet fluem sobre essa rede de redes utilizando a comutação por pacotes:[4] toda comunicação é dividida em pequenos "pacotes", e cada pacote viaja independentemente. Por exemplo, cada e-mail é dividido em vários pacotes menores, que podem, e frequentemente o fazem, tomar caminhos diferentes pela Internet para alcançar o destinatário pretendido. Ao chegarem ao destino, são reconstruídos de forma perfeita antes de serem entregues ao e-mail do usuário final. Esta foi uma grande inovação na forma como o conteúdo era comunicado através das redes.

A Internet é composta por quase 76 mil redes independentes que utilizam os mesmos protocolos técnicos e optam por operar em conjunto. Muitas dessas redes são de propriedade privada, mas algumas são de propriedade dos governos ou controladas por eles. Cada rede toma decisões independentes sobre como direcionar o tráfego para seus vizinhos com base em suas próprias necessidades, modelo de negócios e requisitos locais. Além disso, há centenas de milhares de outras entidades, como provedores de hospedagem de sites, serviços de e-mail, serviços de domínio, serviços de identidade e provedores de segurança, os quais oferecem serviços críticos para apoiar e facilitar a comunicação pela Internet. Não há controle ou coordenação centralizada das redes ou das entidades de apoio.[5]

Esse design distribuído e descentralizado é fundamental para o sucesso da Internet. A Internet se espalhou por todo o mundo e cresceu tanto devido a esse princípio essencial de design. À medida que surgem novas necessidades, áreas de operação ou invenções, novas redes se conectam facilmente e de forma barata à Internet. Em particular, esse design permitiu que redes pequenas ou remotas se conectassem à Internet a um custo relativamente baixo, geralmente sem mais negociações ou acordos além daqueles com os provedores de serviços locais.

A Internet é fundamentalmente diferente das redes de comunicação com comutação de circuitos do passado, e essas diferenças na operação distribuída e no design descentralizado são críticas para a saúde contínua e o crescimento da Internet.

4 Para uma descrição da comutação de pacotes, consulte https://www.internetsociety.org/blog/2022/04/common-internet-network-interconnection-and-charging-practices/; consulte também https://en.wikipedia.org/wiki/Packet_switching.

5 Um artigo da Internet Society, "The Internet Way of Networking: Defining the critical properties of the Internet" (O modo como a Internet se conecta em rede: definindo as propriedades críticas da Internet), Internet Society, 09 de setembro de 2020, https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/, identifica as propriedades críticas que tornam a Internet "A Internet" e sustentam o crescimento e a adaptabilidade da Internet. Este documento faz parte de um esforço maior chamado "The Internet Way of Networking" (O modo como a Internet se conecta em rede), com recursos adicionais em https://www.internetsociety.org/action-plan/internet-way-of-networking/.

2.3 O Papel das Funções Intermediárias

As entidades que fornecem funções intermediárias desempenham um papel essencial não apenas no fornecimento de conectividade global e compartilhamento de conteúdo, mas também de segurança, privacidade e acessibilidade. A Internet depende de uma série de funções intermediárias para funcionar.

Uma ampla diversidade de funções intermediárias oferece suporte à Internet moderna. Algumas podem ser familiares aos usuários e formuladores de políticas, como as fornecidas por ISPs, "provedores de tráfego" que conectam outras redes entre si, serviços de hospedagem que suportam conteúdo de sites e e-mails, motores de busca e redes sociais. Outros tipos de funções intermediárias podem ser menos conhecidos, como cache de conteúdo, defesa de redes e cibersegurança, resolução do "sistema de nomes de domínio" (DNS) e registro de domínios.[6] Até mesmo alguns tipos de software, como navegadores de Internet, fornecem funções intermediárias ao receber conteúdo da Internet e exibi-lo para o usuário final (frequentemente com bloqueio de sites maliciosos para fins de segurança).

Sem funções intermediárias para transportar o tráfego da Internet de e para *endpoints* (incluindo indivíduos, servidores, provedores de serviços e muitos outros), e sem os muitos outros tipos de funções intermediárias que facilitam esse tráfego, não haveria uma Internet.

Os usuários podem escolher interagir diretamente com alguns provedores de funções intermediárias, como seu Provedor de Serviços de Internet para acessar a Internet, sua ferramenta de busca preferida e seu navegador para exibir e, às vezes, filtrar conteúdo. Ter uma variedade de opções disponíveis também permite uma maior escolha e controle para o usuário. Por exemplo, os usuários podem escolher usar funções intermediárias focadas na proteção de privacidade ou que ofereçam experiências online "fáceis e simples para a família".

No entanto, a maioria dos usuários não sabe nem compreende a enorme gama de funções intermediárias que facilitam sua comunicação. Por exemplo, os usuários podem não saber sobre a busca de DNS ou quem está fornecendo a função de busca de DNS para suas pesquisas na web, ou quem e o que facilita o tráfego de seus pacotes depois que saem de seu provedor de serviços de Internet doméstico. Além disso,

6 O Anexo deste artigo fornece uma lista mais longa de intermediários, cobrindo dezenas de tipos, juntamente com recomendações específicas para formuladores de políticas, com orientações sobre armadilhas a serem observadas em relação a cada tipo de intermediário.

muitas das entidades que fornecem as funções intermediárias podem não ter relação (legal ou de qualquer outra forma) com o usuário que iniciou a comunicação ou o destinatário, nem entre si. Embora muitas entidades sejam comerciais, algumas funções intermediárias da Internet são fornecidas por comunidades sem fins lucrativos ou voluntárias. As entidades podem estar em diferentes jurisdições tanto do remetente quanto do destinatário. Essa abordagem descentralizada e distribuída é "uma característica, não um defeito". Seria impossível ter relações diretas ponto a ponto para todas as funções intermediárias em uma escala tão grande quanto a da Internet. A abordagem distribuída da Internet oferece flexibilidade, resiliência e a possibilidade de aumentar e diminuir a capacidade conforme necessário.

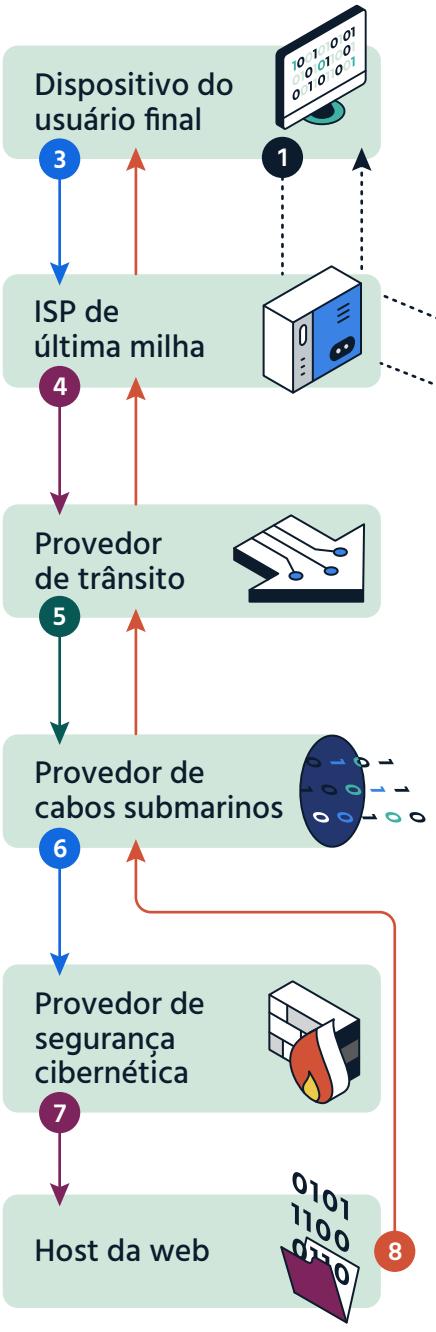
As entidades que fazem a Internet funcionar e ajudam os usuários a acessá-la (frequentemente chamadas de "intermediários de infraestrutura") geralmente não estão cientes do conteúdo específico que está sendo comunicado[7]. Em contraste, as entidades que ajudam os usuários a interagir com o conteúdo na Internet (por exemplo, uma plataforma de compartilhamento de vídeos ou uma rede social), normalmente, estão diretamente envolvidas na forma como o conteúdo é exibido, selecionado, compartilhado etc. No entanto, nem sempre existe uma linha clara entre essas entidades, e nem todas as "plataformas" estão cientes do conteúdo entregue aos usuários.[8]

7 Os intermediários de infraestrutura não apenas não se importam com o conteúdo específico sendo comunicado, mas também não conseguem ver o conteúdo devido ao uso crescente de criptografia de ponta a ponta em toda a Internet.

8 Por exemplo, a maioria dos serviços de mensagens online de indivíduo para indivíduo, como o WhatsApp e o Signal, emprega criptografia de ponta a ponta entre os usuários finais, tornando o conteúdo real transmitido opaco e desconhecido.

Provedores de funções intermediárias

Visão muito simplificada de alguns dos **provedores de funções intermediárias** envolvidos quando um usuário solicita uma página da web.



1. O computador do usuário solicita o endereço IP de uma página da web do provedor de DNS preferencial do usuário por meio do **provedor de última milha** do usuário.
2. O **provedor de DNS** retorna o endereço IP do website para o computador do usuário.
3. O computador do usuário solicita a página da web desejada do host da web localizado em outro país.
4. O ISP de última milha passa a solicitação para um **provedor de trânsito** para encaminhar ao host da web.
5. O provedor de trânsito transmite a solicitação para um **provedor de cabos submarinos**.
6. O provedor de cabos submarinos passa a solicitação por meio de outros provedores de trânsito para o **provedor de segurança cibernética** do host da web.
7. O provedor de segurança cibernética garante que a solicitação não faça parte de um ataque cibernético e a passa ao **host da web**.
8. O host da web recebe a solicitação do usuário e envia a página da web solicitada de volta ao usuário por meio de provedores de trânsito e interconexão semelhantes, mas geralmente diferentes.

3 Proteções de Responsabilidade Para Funções Intermediárias

Esta seção discute as proteções de responsabilidade, começando com uma breve história das origens e dos principais elementos da Seção 230 dos EUA. Também descrevemos o Marco Civil da Internet de 2014, do Brasil, e a Diretiva de Comércio Eletrônico de 2000 e o Ato de Serviços Digitais de 2022, da Europa. Em seguida, passamos a discutir outras abordagens nacionais ou regionais relacionadas.

Concluímos discutindo as tendências recentes em políticas relacionadas às funções intermediárias e identificamos alguns riscos específicos que essas abordagens podem apresentar para a Internet e os usuários da Internet.

3.1 O Desenvolvimento Inicial das Leis de Proteção aos Intermediários: Contextualização

A Internet inicial foi desenvolvida na década de 1970 com base em financiamento fornecido pelo Governo dos Estados Unidos (EUA). Inicialmente usada para colaboração e pesquisa por um pequeno conjunto de pesquisadores acadêmicos, governamentais e comerciais, ela começou como uma rede restrita aos EUA, mas rapidamente se expandiu para incluir conexões com a Europa, Ásia e Oceania. As proibições de tráfego pessoal e comercial foram gradualmente removidas na década de 1990. Em 1995, o Governo dos EUA transferiu formalmente a rede para o setor privado, o que deu início à inclusão da população civil à Internet.

À medida que mais e mais indivíduos passaram a poder se expressar publicamente na Internet, surgiram rapidamente questões sobre como

a responsabilidade por conteúdo prejudicial ou ilegal seria atribuída no contexto online. Nos EUA, processos foram movidos argumentando que as empresas que permitiam que as pessoas publicassem online deveriam ser legalmente responsáveis pelas palavras publicadas por tais pessoas. Na década de 1990, duas decisões judiciais emblemáticas dos EUA decidiram que aqueles que hospedam conteúdo online, os intermediários, **seriam** responsáveis pelas palavras publicadas por seus usuários, *se esses que hospedam o conteúdo tivessem tomado medidas para moderar o discurso online e remover conteúdos sexuais, ofensivos ou outros tipos de conteúdo.*[9]

Essas decisões judiciais criaram dois cenários impraticáveis e indesejáveis para a Internet emergente.

Por um lado, se as empresas tomassem ações para "moderar" o discurso online de seus usuários, elas seriam então responsáveis por esse conteúdo, mas essas entidades[10] não tinham o pessoal ou os recursos para analisar, bloquear ou remover qualquer conteúdo que pudesse gerar responsabilidade.[11]

Por outro lado, as empresas poderiam evitar a responsabilidade se *não* tomassem ações para remover conteúdos sexuais, ofensivos ou outros tipos de conteúdo que os usuários publicassem. Mas esse ambiente teria resultado em conversas e publicações inundadas de conteúdo questionável. Em vez de se tornar uma plataforma útil para interação social, cívica e de crescimento econômico, a Internet teria perdido sua utilidade como uma ferramenta para comunicação, expressão e comércio individual.

Essas decisões judiciais criaram uma incerteza significativa e uma responsabilidade potencialmente debilitante para o conteúdo gerado por usuários na Internet em desenvolvimento.

9 *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), decidiu que um provedor de serviços online não seria responsabilizado pelo discurso de um participante em um fórum online, mas *apenas* porque o provedor não moderava nenhum conteúdo. Já *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 24 de maio de 1995), responsabilizou um provedor de serviços online pelo discurso dos participantes porque o provedor se envolveu em algum tipo de monitoramento e regulamentação de conteúdo.

10 Embora os grandes sites de redes sociais de hoje sejam um exemplo óbvio, a Internet dos anos 1990 tinha menos "megassites" e, muitas vezes, não havia um intermediário claro que tivesse o direito ou a responsabilidade de moderar o conteúdo. Quando um moderador era identificado, com frequência, poderia ser um indivíduo privado que se voluntariava, e não uma empresa privada.

11 Mesmo em um ambiente com recursos abundantes, alguns tipos de moderação, como a de conteúdo difamatório, são problemáticos, pois a questão de saber se o conteúdo é ou não difamatório, muitas vezes, é impossível de ser determinada por um moderador individual.

3.2 As Primeiras Leis de Responsabilidade de Intermediários da Internet: Seção 230 dos EUA

Diante desse desafio para o potencial da Internet e a capacidade dos indivíduos de se engajarem online, entre 1995 e 1996, o Congresso dos Estados Unidos decidiu enfrentar a realidade de que os regimes de responsabilidade existentes não funcionavam para a Internet:

- A responsabilidade baseada em publicadores, que se aplicava a jornais offline, levaria a uma responsabilidade potencial e massiva que prejudicaria a liberdade de expressão individual na Internet ou a uma Internet na qual os sites não poderiam impor regras de comportamento e cortesia.
- O regime de transporte comum aplicável ao serviço telefônico básico não poderia ser aplicado nem às redes de acesso à Internet, que possuíam alguns aspectos de provedores de comunicação, mas não o suficiente para se encaixar nesse modelo, nem aos hosts de conteúdo, que operam de maneira completamente diferente dos provedores comuns.
- O regime de responsabilidade que se aplicava ao rádio, à televisão e ao vídeo a cabo, que é baseado em acordos contratuais individualmente negociados entre as redes e as corporações que fornecem conteúdo, não poderia de forma alguma se aplicar a um mundo com milhões e, por fim, bilhões de usuários online.

Precisávamos de uma nova abordagem quanto à responsabilidade.

Foi nesse cenário que o Congresso dos EUA considerou e promulgou o "Internet Freedom and Family Empowerment Act", que se tornou a Seção 230 do Código 47 dos Estados Unidos (USC) (frequentemente chamada simplesmente de "Seção 230").[12] Um dos objetivos explícitos do Congresso com a Seção 230 era "promover o desenvolvimento contínuo da Interne

12 O texto que se tornou a Seção 230 originalmente veio de uma proposta legislativa da Câmara dos Representantes, chamado Internet Freedom and Family Empowerment Act (Lei de Liberdade na Internet e Fortalecimento Familiar). Durante a conferência entre a Câmara e o Senado para reconciliar a legislação da Telecommunications Act (Lei das Telecomunicações), o texto da Seção 230 foi colocado imediatamente após e na mesma seção estatutária do projeto de lei do Senado, conhecido como Communications Decency Act (Lei de Decência nas Comunicações). O contexto adicional sobre a nova Telecommunications Act (Lei das Telecomunicações) está disponível em "What's in a Name", (https://www.lawfaremedia.org/article/whats-name-quite-bit-if-youre-talking-about-section-230), "Section 230: An Overview" (pelo Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R46751), entre outros. O texto final pode ser encontrado em https://www.congress.gov/bill/104th-congress/senate-bill/652.

e outros serviços interativos de computador e outros meios interativos."[13] O Congresso reconheceu que os serviços interativos de computador em geral, e a Internet em particular, mesmo em seu estágio inicial quando a Seção 230 foi promulgada, ofereciam uma plataforma profundamente diferente para a comunicação interativa entre indivíduos.

O Congresso dos EUA observou na legislação que a "Internet e outros serviços interativos de computador oferecem um fórum para uma verdadeira diversidade de discursos políticos, oportunidades únicas para o desenvolvimento cultural e inúmeras avenidas para a atividade intelectual."[14] O Congresso concluiu que essas comunicações interativas, que fomentam o discurso público, deveriam ser incentivadas. A Internet, diferentemente das formas anteriores de comunicação em massa "publicadas", transforma o indivíduo de um receptor passivo de produtos principalmente criados por corporações em um participante ativo na formação da comunicação e do conteúdo. O Congresso reconheceu que essa "interatividade" movida pelo indivíduo era um atributo essencial da Internet emergente que justificava proteção.

Texto-chave da Seção 230:

§ 230(c)(1): **Tratamento de editor ou orador**. Nenhum provedor ou usuário de um serviço interativo de computador será tratado como editor ou orador de qualquer informação fornecida por outro provedor de conteúdo de informação.

§ 230(c)(2): **Responsabilidade civil**. Nenhum provedor ou usuário de um serviço interativo de computador será responsabilizado por causa de:

> (A) qualquer ação voluntária tomada de boa-fé para restringir o acesso ou disponibilidade de material que o provedor ou usuário considera como obsceno, indecente, lascivo, sujo, excessivamente violento, ofensivo ou censurável, mesmo que esse material seja constitucionalmente protegido; ou
>
> (B) qualquer ação tomada para permitir ou disponibilizar aos provedores de conteúdo de informação ou outros meios técnicos para restringir o acesso ao material descrito no parágrafo ([A]).

13 47 USC § 230(b)(1), disponível em https://www.congress.gov/104/statute/STATUTE-110/STATUTE-110-Pg56.pdf.

14 47 USC § 230(a)(3).

§ 230(f): **Definições**.

(2) **Serviço interativo de computador**

O termo "serviço interativo de computador" significa qualquer serviço de informação, sistema ou provedor de software de acesso que fornece ou permite acesso por computador por múltiplos usuários a um servidor de computador, incluindo especificamente um serviço ou sistema que fornece acesso à Internet e tais sistemas operados ou serviços oferecidos por bibliotecas ou instituições educacionais.

(3) **Provedor de conteúdo de informação**

O termo "provedor de conteúdo de informação" significa qualquer pessoa ou entidade que seja responsável, no todo ou em parte, pela criação ou pelo desenvolvimento de informações fornecidas através da Internet ou qualquer outro serviço interativo de computador.

(4) **Provedor de software de acesso**

O termo "provedor de software de acesso" significa um provedor de software (incluindo software cliente ou servidor), ou ferramentas que permitem fazer uma ou mais das seguintes ações:

(A) filtrar, selecionar, permitir ou bloquear conteúdo;

(B) selecionar, escolher, analisar ou sintetizar conteúdo; ou

(C) transmitir, receber, exibir, encaminhar, armazenar em cache, pesquisar, subdividir, organizar, reorganizar ou traduzir conteúdo.

A Seção 230 dos **Estados Unidos** contém três elementos críticos:

1. Os serviços interativos de computador (um termo estatutário usado na Seção 230 que se refere essencialmente a entidades que fornecem funções intermediárias) na Internet não são legalmente responsáveis pelo conteúdo que outras entidades — indivíduos, corporações e outros provedores de conteúdo — publicam na Internet. Em vez disso, a responsabilidade legal pelo conteúdo permanece com a pessoa ou entidade que o criou ou publicou. Esse elemento permite que provedores de acesso à Internet, serviços de hospedagem na web e muitos outros transmitam ou hospedem conteúdo sem o temor de uma responsabilidade potencialmente massiva.

2. Os serviços interativos de computador não são responsáveis se decidirem bloquear ou remover conteúdo indesejado em suas plataformas. Esse elemento garante que os hosts e as plataformas online estejam protegidos caso removam conteúdo odioso, ofensivo ou de outra forma questionável de seus sites. Por exemplo, se um indivíduo publicar conteúdo sexualmente explícito em uma plataforma online, ele não poderá processar a plataforma caso o conteúdo seja removido ou bloqueado. Assim, os intermediários estão protegidos por suas decisões de moderação.
3. As empresas que desenvolvem ferramentas tecnológicas para permitir que os usuários filtrem e bloqueiem conteúdo indesejado na Internet não podem ser responsabilizadas por criar essa capacidade de bloqueio. Por exemplo, se um site com conteúdo odioso e malicioso for bloqueado por um software instalado por um responsável em um computador doméstico, o site não poderá processar o fabricante do software por bloquear seu conteúdo. Esse elemento incentiva o desenvolvimento de ferramentas que permitam aos *usuários* escolher limitar os tipos de conteúdo legal que eles (e suas famílias) podem acessar.

Todas as proteções mencionadas se estendem de forma muito ampla a qualquer serviço interativo de computador envolvido na transmissão, transporte, hospedagem, seleção, exibição ou, de outra forma, facilitação da transmissão ou exibição de conteúdo criado por terceiros, e não apenas ao serviço onde o conteúdo foi publicado ou compartilhado.

A Seção 230 não utiliza os termos "intermediário" ou "função de intermediário". Em vez disso, a lei define amplamente o termo "serviços interativos de computador" para se referir às funções básicas de acesso à Internet, tráfego, hospedagem, busca e serviços relacionados. Em seguida, a Seção 230 aplica as proteções de responsabilidade acima a qualquer "provedor ou usuário de um serviço interativo de computador."

Vale destacar que até mesmo usuários individuais estão protegidos pela Seção 230 em circunstâncias em que, por exemplo, encaminham uma publicação online para outro destinatário.

A Seção 230 é considerada uma razão crítica para que a liberdade de expressão individual tenha prosperado na Internet nos Estados Unidos.[15] Ao mesmo tempo, o Congresso dos EUA também buscava proteger e incentivar o potencial econômico da Internet. E os benefícios econômicos

15 Jeff Kosseff, um acadêmico jurídico dos EUA, chegou a escrever um livro inteiro, "The Twenty-Six Words that Created the Internet", fazendo referência à Seção 230 como sendo singularmente responsável por grande parte da indústria da Internet dos EUA. Consulte também https://www.propublica.org/article/nsu-section-230 para obter contexto adicional.

e sociais combinados que os Estados Unidos experimentaram com a Internet levaram outros grandes governos a adotar regras semelhantes.

Os Estados Unidos foram a primeira nação a adotar proteções legais de responsabilidade para intermediários da Internet. Outras nações e regiões adotaram proteções semelhantes, mas com algumas diferenças importantes.

3.3 Proteções Iniciais a Intermediários na Europa

Em 2000, a **União Europeia** (UE) adotou a Diretiva de Comércio Eletrônico (2000/31/EC),[16] para abordar as proteções a intermediários. Na prática, a Diretiva de Comércio Eletrônico adotou uma abordagem muito semelhante à Seção 230, mas com três distinções significativas:

- A diretiva da UE dividiu os intermediários em três categorias básicas: (a) meros condutos, (b) provedores de armazenamento em cache e (c) provedores de hospedagem.
- A diretiva não definiu os tipos de entidades abrangidas, mas abordou tipos específicos de "atividades" que receberiam proteção de responsabilidade (da mesma forma que este documento se concentra em "funções" de intermediários em vez de categorias de intermediários).
- Mais importante, a diretiva da UE exige que intermediários que obtenham conhecimento de conteúdo supostamente ilegal tomem medidas para removê-lo de forma razoavelmente rápida.[17]

A Diretiva de Comércio Eletrônico regulou questões de proteção de intermediários na União Europeia por mais de 20 anos, até ser modificada e complementada pela Lei de Serviços Digitais e outras medidas discutidas a seguir.

3.4 O Marco Civil da Internet no Brasil

A partir de 2009, um amplo conjunto de partes interessadas no **Brasil**, incluindo governo, academia, sociedade civil e indústria, empreendeu um esforço colaborativo para desenvolver um conjunto de leis que

16 Consulte https://eur-lex.europa.eu/eli/dir/2000/31/oj; https://en.wikipedia.org/wiki/Electronic_Commerce_Directive_2000.

17 O regime de "aviso e retirada" criado pela Diretiva de Comércio Eletrônico é contrastado com a abordagem nos Estados Unidos, onde a Primeira Emenda da Constituição dos EUA geralmente (fora do contexto de direitos autorais) proíbe mandatos legais para remover conteúdo sem uma determinação judicial específica de que o conteúdo é ilegal.

regulamentassem a Internet. Por meio de um engajamento multissetorial, o processo recebeu extensos comentários e contribuições, resultando em esboços que foram desenvolvidos e refinados. A legislação resultante foi promulgada em 2014 como o Marco Civil da Internet, Lei Federal Brasileira nº 12.965/2014.[18] O governo brasileiro declara que o Marco Civil "estabelece os princípios, as garantias, os direitos e os deveres para o uso da Internet no Brasil."[19]

A Seção III do Marco Civil apresenta uma declaração direta e clara sobre a proteção de responsabilidade de intermediários, com disposições adicionais que permitem a remoção de conteúdo por ordem judicial e proteção da privacidade mediante notificação. As principais disposições das provisões sobre intermediários incluem:

> **Artigo 18**. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
>
> **Artigo 19**. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
>
> ...
>
> **Artigo 20**. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o Artigo 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.
>
> ...

18 Consulte https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6, ou a versão oficial em inglês da lei em https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180 e https://www.daniel-ip.com/en/articles/the-brazilian-internet-bill-of-rights-and-online-infringement-of-ip-rights/.

19 Versão em inglês do Marco Civil, disponível em http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_%20internet.pdf.

> **Artigo 21**. O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

A abordagem brasileira é considerada na região como um modelo para proteger funções de intermediários, ao mesmo tempo em que padroniza uma via judicial para tratar das preocupações governamentais e da sociedade em relação a conteúdos ilegais ou prejudiciais.

3.5 Atualizações Nas Proteções a Intermediários na Europa

Em 2022, a **União Europeia (UE)**, motivada por preocupações relacionadas à segurança online, à disseminação de desinformação e discurso de ódio, e outras condutas ilícitas ou prejudiciais em grandes plataformas e serviços amplamente utilizados, adotou uma atualização significativa e uma expansão da Diretiva de Comércio Eletrônico de 2000. A nova abordagem continuou a focar nos serviços (muitos dos quais englobam "funções de intermediários" discutidas aqui), em vez de empresas. Isso reflete o reconhecimento de que algumas entidades podem desempenhar diferentes funções de intermediários, sendo, portanto, elegíveis a diferentes tipos de proteção ou sujeitas a diferentes obrigações, dependendo da função específica executada.

O objetivo global do *Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, sobre um Mercado Único para Serviços Digitais e que altera a Diretiva 2000/31/EC* (Lei de Serviços Digitais)[20] é criar um mercado único para serviços online na UE. A Lei de Serviços Digitais inclui proteções de responsabilidade para conteúdos gerados por usuários (exceto quando o provedor de serviços tem conhecimento de que o conteúdo é ilegal), mas as combina com requisitos de "devida diligência". Essas obrigações tornam os provedores

20 Consulte https://eur-lex.europa.eu/eli/reg/2022/2065/oj, bem como as Perguntas Frequentes fornecidas pela Comissão Europeia em https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 e informações resumidas em https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

mais responsáveis pelo que ocorre em seus serviços. Em vez de impor responsabilidades civis, a Lei de Serviços Digitais utiliza multas para desencorajar e punir a não conformidade com essas obrigações.

Com base na Diretiva de Comércio Eletrônico, essa Lei aplica-se a um subconjunto de "serviços da sociedade da informação," definidos como três categorias de um "serviço de intermediário":[21]

1. Um serviço de "mero conduto" consiste na transmissão, em uma rede de comunicações, de informações fornecidas por um destinatário do serviço ou no fornecimento de acesso a uma rede de comunicações.
2. Um serviço de "armazenamento em cache" consiste na transmissão, em uma rede de comunicações, de informações fornecidas por um destinatário do serviço, envolvendo o armazenamento automático, intermediário e temporário dessas informações, realizado exclusivamente com o único objetivo de tornar mais eficiente a transmissão subsequente dessas informações a outros destinatários, mediante solicitação.
3. Um serviço de "hospedagem" consiste no armazenamento de informações fornecidas por, e a pedido de, um destinatário do serviço.

Além disso, a Lei impõe obrigações específicas a duas categorias de serviços: provedores designados de grandes motores de busca online (VLOSES) e plataformas online de muito grande dimensão (VLOPS), definidos como serviços com mais de 45 milhões de usuários mensais na UE. Essas obrigações incluem:

- Um ponto de contato para autoridades e usuários da UE.
- Termos e condições acessíveis e amigáveis ao usuário.
- Transparência quanto à publicidade, sistemas de recomendação e decisões de moderação de conteúdo.
- Uma avaliação baseada em riscos de seus serviço e medidas de mitigação apropriadas.
- Auditorias independentes.
- Compartilhamento de dados com autoridades para fins de conformidade e com pesquisadores autorizados para compreender riscos sistêmicos.
- Obrigação de oferecer uma opção de sistema de recomendação que não seja baseada em perfis de usuários.[22]

21 Ibid., Artigo 3, "Definições" da Lei de Serviços Digitais.

22 Consulte a orientação da Comissão Europeia em https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.

3.6 Proteções a Intermediários em Outros Contextos Nacionais e Internacionais

No início dos anos 2000, vários países também adotaram legislações nacionais focadas na Internet, implementando diferentes níveis de proteção para funções de intermediários.

Por exemplo, em 2000, a **Índia** aprovou a Lei de Tecnologia da Informação de 2000, que estipulava que intermediários não seriam responsabilizados por conteúdos de terceiros disponíveis se pudessem provar que a infração ou contravenção foi cometida sem seu conhecimento ou que haviam exercido toda a devida diligência para prevenir a ocorrência de tal infração ou contravenção.[23] A Lei também permite que o governo emita diretrizes para a remoção de certos conteúdos online.

Na **Nigéria**, em 2003, as Diretrizes para a Prestação de Serviços de Internet, publicadas pela Comissão de Comunicações da Nigéria, estabeleceram que provedores de serviços de Internet atuando como meros condutos (*ou seja*, hospedagem ou armazenamento em cache) não seriam responsabilizados por conteúdo e comunicações gerados por usuários, desde que cumprissem certas condições: eles deviam agir sem demora para remover ou desabilitar o acesso às informações ao receber uma notificação de remoção ou ao tomarem conhecimento de que as informações na origem inicial da transmissão foram removidas ou desabilitadas.[24]

A **África do Sul**, em sua Lei de Transações e Comunicações Eletrônicas de 2002, adotou abordagem semelhante, mas condicionou as limitações de responsabilidade ao provedor de serviços ser membro de um órgão representativo e estar vinculado ao código de conduta desse órgão, reconhecido pelo Ministro, além de exigir um processo de notificação e remoção.[25]

A **Lei de Comunicações Digitais Prejudiciais de 2015 da Nova Zelândia** protege "prestadores de serviços de hospedagem de conteúdo online" de responsabilidade, desde que sigam o processo estatutário de reclamações. A Lei inclui o requisito de que o prestador de serviços de hospedagem de

23 Consulte o Artigo 79 da Lei de Tecnologia da Informação de 2000 (Índia), disponível em https://www.meity.gov.in/writereaddata/files/itbill2000.pdf.

24 Diretrizes para a Prestação de Serviços de Internet publicadas pela Comissão de Comunicações da Nigéria em 2003, conforme o Artigo 70(2) da Lei de Comunicações da Nigéria de 2003, disponível em https://ncc.gov.ng/accessible/documents/62-guidelines-for-the-provision-of-internet-service/file.

25 Electronic Communications and Transactions Act 2002 (South Africa) available at https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.

conteúdo online notifique a pessoa que fez a reclamação e pode envolver a exigência de remover ou desabilitar o conteúdo.[26]

A **Austrália** está avançando ativamente em 2024 para adotar um regime de proteção de responsabilidade de intermediários focado em reivindicações legais por difamação.[27] As Disposições Modelo para Emenda à Lei de Difamação (Intermediários Digitais) de 2023 propõem alterações às leis "uniformes" de difamação da Austrália, as quais estão em vigor desde 2006, para harmonizar essas leis em relação a conteúdos digitais difamatórios em toda a Austrália. As novas disposições pretendem esclarecer a posição legal dos intermediários em relação a conteúdos digitais difamatórios. Elas preveem isenções de responsabilidade por difamação para intermediários digitais que fornecem serviços de armazenamento em cache, condutos, armazenamento e busca.[28] No entanto, essas isenções não estarão disponíveis se o intermediário digital, entre outras coisas, selecionou qualquer um dos destinatários ou promoveu o conteúdo difamatório. Não está claro se isso incluiria a promoção de conteúdo para usuários por meio de algoritmos de recomendação. A isenção para mecanismos de busca não se aplicaria a "resultados de busca patrocinados", ou seja, "os resultados [que] são promovidos ou priorizados pelo provedor de mecanismos de busca devido a um pagamento ou outro benefício concedido ao provedor em nome ou por meio de terceiros".

Além das leis obrigatórias adotadas pelos governos, várias organizações multilaterais ou multissetoriais emitiram declarações de apoio às proteções de responsabilidade para intermediários. Esses acordos internacionais e declarações refletem um consenso crescente sobre o valor dessas proteções. Fornecemos um resumo de algumas dessas declarações na tabela abaixo.

26 Harmful Digital Communications Act 2015 (New Zealand) available at https://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM6512504.

27 See https://pcc.gov.au/uniform/2023/pcc-584-d05b.pdf or https://www.parliament.nsw.gov.au/bill/files/18503/Passed%20by%20both%20Houses.pdf (New South Wales version).

28 Schedule 1, Sections 10C and 10D of the Model Defamation Amendment (Digital Intermediaries) Provisions 2023 available at https://pcc.gov.au/uniform/2023/pcc-584-d40.pdf.

Declarações Multilaterais e Multissetoriais Sobre Proteções de Responsabilidade Para intermediários

2011

O Relator Especial das Nações Unidas (ONU) sobre Liberdade de Opinião e Expressão, o Representante da Organização para a Segurança e Cooperação na Europa (OSCE) para a Liberdade de Imprensa, o Relator Especial sobre Liberdade de Expressão da Organização dos Estados Americanos (OEA) e o Relator Especial sobre Liberdade de Expressão e Acesso à Informação[29] da Comissão Africana dos Direitos Humanos e dos Povos (CADHP) emitiram uma declaração conjunta pedindo proteção aos intermediários "meros condutos" e a outras funções de intermediários. Eles expressaram o entendimento de que esses intermediários não devem ser obrigados a monitorar conteúdo gerado por usuários nem estar sujeitos a regras extrajudiciais de remoção de conteúdo que não ofereçam proteção suficiente à liberdade de expressão.

2013

No Fórum Africano de Governança da Internet, uma iniciativa pan-africana para promover padrões de direitos humanos e princípios de abertura na formulação e implementação de políticas da Internet na África, foi publicada a Declaração Africana sobre Direitos e Liberdades na Internet,[30] Essa declaração incluía o princípio básico de proteção de intermediários: "Ninguém deve ser responsabilizado por conteúdo na Internet do qual não seja o autor."[31]

2014

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) divulgou orientações amplas sobre a limitação da responsabilidade de intermediários:[32]

> **Limitar a responsabilidade de intermediários da Internet**. Limitações apropriadas à responsabilidade de intermediários da Internet desempenham um papel

29 https://www.osce.org/representative-on-freedom-of-media/78309.

30 https://africaninternetrights.org/en.

31 https://africaninternetrights.org/sites/default/files/African-Declaration-English-FINAL.pdf.

32 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0387.

> fundamental na promoção da inovação e criatividade, do fluxo livre de informações, de incentivos à cooperação entre as partes interessadas e do crescimento econômico. Os intermediários da Internet, como outras partes interessadas, também desempenham um papel importante no combate a atividades ilegais, fraudes e práticas enganosas e injustas realizadas por meio de suas redes e serviços. A proporcionalidade e a conformidade às proteções de todos os direitos fundamentais relevantes são essenciais nesse contexto.

Embora os princípios não sejam juridicamente vinculantes, essa orientação da OCDE reflete o reconhecimento amplo de muitos governos de que as proteções de responsabilidade para intermediários desempenham um papel importante na facilitação da expressão online e do engajamento criativo.

2018

Em 2018, o Conselho da Europa adotou a Recomendação do Comitê de Ministros aos Estados-Membros sobre os papéis e as responsabilidades dos intermediários da Internet (CM/Rec(2018)2)[33], aplicando uma abordagem baseada em direitos humanos às responsabilidades dos Estados e dos intermediários da Internet, deixando de lado questões de responsabilidade jurídica.

3.7 Tendências Recentes na Responsabilidade de Intermediários e Riscos Para a Internet

As proteções para intermediários são consideradas instrumentais para o crescimento da Internet e para o florescimento da liberdade de expressão individual na rede. Alguns países, reconhecendo os benefícios das salvaguardas para intermediários, codificaram a proteção de responsabilidade em lei. Em outros países, a ausência de leis que protejam os intermediários pode levar a proteções judiciais criadas ou a um tratamento mais problemático das funções intermediárias.

Nesta seção, identificamos algumas abordagens recentemente propostas

33 https://rm.coe.int/1680790e14.

para a formulação de políticas para funções de intermediários da Internet. Dependendo da implementação exata, essas abordagens podem criar riscos significativos para a Internet e os usuários da Internet, incluindo:

- Comprometer as operações técnicas e a confiabilidade da Internet.
- Enfraquecer a segurança e a privacidade na Internet.
- Reduzir a concorrência na Internet em um país devido às cargas ou responsabilidades impostas ao ISP.
- Limitar a capacidade dos indivíduos de compartilhar opiniões e outras formas de expressão na Internet.
- Bloqueio excessivo de conteúdo lícito.
- Exclusão inadequada de segmentos da população da participação na Internet.

Recomendamos uma cuidadosa ponderação dos riscos listados acima e outros impactos potenciais na Internet ao considerar essas abordagens para a formulação de políticas para funções intermediárias. Em seções posteriores deste documento, fornecemos orientações gerais e específicas aos formuladores de políticas sobre como evitar esses e outros riscos.

Aviso e retirada: nem todos os regimes regulatórios adotaram a mesma abordagem em relação à responsabilidade dos intermediários. Em uma variante comum, os intermediários podem ser considerados responsáveis e até mesmo responsabilizados pelo conteúdo de seus usuários se não tomarem determinadas medidas. Por exemplo, algumas jurisdições possuem uma abordagem de "aviso e retirada", que exige que um intermediário remova o conteúdo após o recebimento de uma notificação legal de um tribunal ou agência governamental autorizada. Significativamente, não há obrigação geral dos intermediários de monitorar o conteúdo.[34]

Conhecimento: terceiros exigiram que os intermediários removessem conteúdo ilegal ou prejudicial quando tomaram conhecimento dele, com níveis variados de "conhecimento" exigidos, sendo o mais estrito o "conhecimento efetivo."[35]

34 No entanto, as emendas à Lei de Procedimento Criminal e Provas de 2021, na Lei de Proteção Cibernética e de Dados do Zimbábue, estabelecem que um provedor de hospedagem deve, se "obter conhecimento ou tomar ciência de qualquer informação ilegal armazenada, informar prontamente a autoridade apropriada para que possa avaliar a natureza da informação e, se necessário, emitir uma ordem para sua remoção". Texto disponível em https://www.law.co.zw/download/cyber-and-data-protection-act-chapter-1207/.

35 Consulte, por exemplo, Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE) (Espanha), disponível em https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13758.

Essas modificações (aviso e retirada, e conhecimento) à abordagem geral operam após o conteúdo ter sido carregado ou compartilhado por um usuário.

Moderação de upload: cada vez mais, há um crescente interesse em responsabilizar os intermediários, especialmente os intermediários de hospedagem de conteúdo, pela filtragem de certos tipos de conteúdo antes de serem compartilhados, como material de abuso sexual infantil (MASI). Às vezes, isso é referido como "moderação de upload" e, em algumas propostas, existe o desejo de impor essa obrigação até mesmo em aplicativos de mensagens criptografadas de ponta a ponta.[36]

Esses tipos de responsabilidades de conteúdo pré-publicação estão começando a ser denominados responsabilidades de "devida diligência" ou "dever de cuidar". Às vezes, eles também são abordagens de "responsabilidade condicional", em que um intermediário não será responsabilizado **desde que** faça ou impeça algo.

Requisitos específicos para idade: alguns países pressionaram para impor maiores responsabilidades às entidades intermediárias para excluir determinados grupos etários de seus serviços ou para modificar os serviços ou o conteúdo que exibem para esses usuários. A falha em tomar essas medidas pode fazer com que o serviço intermediário seja banido, bloqueado ou pode tornar a entidade intermediária responsável, dependendo de como a política é implementada.

Por exemplo, os intermediários podem ser protegidos da responsabilidade pelo conteúdo gerado pelo usuário na Indonésia se garantirem que seus sistemas não contenham ou facilitem a disseminação de conteúdo proibido. Eles também devem ter uma estrutura de governança para conteúdo gerado pelo usuário que inclua direitos, obrigações, relatórios, reclamações, responsabilidade e fornecer informações sobre usuários que fazem uploads proibidos e respondem a "avisos de retirada."[37]

Essa abordagem política está impulsionando o interesse em mecanismos técnicos para verificar a idade e identidade dos usuários antes que eles possam usar serviços ou acessar conteúdo. No entanto, os mecanismos disponíveis atualmente levantam sérias preocupações sobre eficácia,

36 Obviamente, se um intermediário que fornece mensagens criptografadas de ponta a ponta for obrigado a moderar o conteúdo enviado entre os usuários, então a mensagem não pode mais ser chamada de criptografada de ponta a ponta.

37 Regulamento do Ministro das Comunicações e Informação, da República da Indonésia, Número 5 de 2020 sobre Operadores de Sistemas Eletrônicos Privados, veja o artigo 11, disponível em https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020.

privacidade, segurança e prevenção do acesso a conteúdo online lícito.[38]

Requisitos de rastreamento: outra abordagem que surgiu é exigir que os intermediários sejam capazes de identificar quem publicou o conteúdo, até mesmo quando uma comunicação é criptografada de ponta a ponta. Como exemplo, na Índia, grandes intermediários de mensagens de mídias sociais devem ser capazes de identificar o primeiro originador de uma mensagem quando exigido por ordem judicial.[39]

Remoção das proteções de responsabilidade dos intermediários: as reações à experiência inicial com políticas específicas da Internet inspiraram algumas propostas amplas. Por exemplo, nos Estados Unidos, preocupações com as maiores plataformas resultaram em propostas excessivamente amplas para remover *todas* as proteções dos intermediários de *todas* as entidades protegidas pela Lei relevante, a Seção 230. Da mesma forma, no Brasil, foram levantadas questões sobre a validade contínua da abordagem adotada no Marco Civil da Internet em relação à responsabilidade dos intermediários. Essas propostas para alterar ou revogar as proteções de intermediários, mesmo na fase de proposta, têm o impacto direto de ameaçar a existência das operações da Internet, criando incerteza e a ameaça de responsabilidade irrestrita pelo conteúdo produzido por terceiros.

Códigos setoriais obrigatórios: algumas jurisdições estão exigindo códigos ou padrões setoriais aplicáveis[40] para criar novas obrigações legais (como segurança por projeto, avaliações de risco e aplicação dos termos de serviço) para categorias de intermediários, por exemplo, mídias sociais, mecanismos de busca, especialmente no contexto da segurança online.

Observamos que as políticas em todas as jurisdições são frequentemente elaboradas de maneira muito ampla. Às vezes, isso é intencional, uma

38 Consulte o artigo da Internet Society, "Texas' Mandatory Age Verification Law Will Weaken Privacy and Security on the Internet" (A Lei de Verificação de Idade Obrigatória do Texas Irá Enfraquecer a Privacidade e a Segurança na Internet), 23 de setembro de 2024, disponível em https://www.internetsociety.org/blog/2024/09/texas-mandatory-age-verification-law-will-weaken-privacy-and-security-on-the-internet/.

39 Disponível no site da MeitY em https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf. No momento deste documento, a constitucionalidade dessas regras está sujeita a vários processos legais.

40 Consulte, por exemplo, o registro de códigos e normas da indústria de segurança online da Austrália, disponível em https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards.

forma de acompanhar as mudanças tecnológicas e os usos da Internet. No entanto, essas políticas amplas geralmente têm um profundo efeito adverso na Internet e na capacidade dos indivíduos de se expressar online.

3.8 Uma Diversidade Global de Países

Este documento busca fornecer orientações úteis sobre políticas públicas para países ao redor do mundo, desde aqueles com altos níveis de penetração da Internet e setores da Internet bem desenvolvidos até aqueles que ainda estão expandindo o acesso e suas economias digitais.

Reconhecemos a existência de vastas diferenças em leis, culturas, economias, políticas, valores e até mesmo objetivos de políticas em relação ao conteúdo na Internet. Acreditamos que nossas recomendações a respeito de políticas serão úteis para qualquer formulador de políticas que esteja considerando regulamentações aplicáveis a intermediários. O documento começa com um foco na abordagem da política em proteger intermediários de responsabilidade e explica por que essa abordagem tem sido importante para permitir que indivíduos participem online. Também apresentamos algumas recomendações construtivas de políticas para abordar uma ampla variedade de preocupações.

Observamos que os sistemas jurídicos diferem em como abordam o conteúdo problemático online: alguns se concentram principalmente na pessoa que publica o conteúdo, enquanto outros focam nos intermediários que hospedam ou transmitem esse conteúdo. Além disso, embora a maioria dos países tenha litígios públicos e privados para tratar de conteúdo problemático online, alguns deles contam com litígios mais privados do que outros. Essas diferenças podem ter levado os países a se concentrarem em diferentes graus na questão das proteções dos intermediários contra responsabilidades. Em todas as situações, entretanto, uma recomendação fundamental é evitar atribuir responsabilidade — seja civil ou criminal — aos intermediários devido ao conteúdo publicado por um usuário ou terceiro. Caso tal responsabilidade seja imposta, isso prejudicaria a capacidade dos usuários da Internet de se expressarem e publicarem conteúdo online. No entanto, como mencionado na Seção 4, existem muitas maneiras pelas quais os governos podem abordar de forma construtiva as preocupações sobre políticas relacionadas aos provedores de serviços online.

Também é importante, ao formular políticas, compreender que as entidades que desempenham funções intermediárias variam em tamanho, receita, margens de lucro e modelo de negócios. Algumas delas são sem

fins lucrativos, e outras, dependendo do país e do ambiente de negócios, podem também ser operadas por governos. Algumas oferecem apenas uma função específica, enquanto outras estão fortemente integradas em diversos negócios relacionados. Isso resulta em interesses muito diversificados e, às vezes, opostos dentro da mesma indústria, além de diferenças significativas na capacidade de contribuir efetivamente para a formulação de políticas nessa área.

A jurisdição sobre provedores de serviços online também pode variar de país para país. Dependendo de onde uma entidade que desempenha funções intermediárias está localizada, questões jurisdicionais podem ser complexas. Pode ser mais fácil para os países exercerem jurisdição quando a entidade possui escritórios comerciais ou infraestrutura nesse país. Quando o conteúdo está hospedado fora do país, a jurisdição pode ser mais desafiadora, especialmente quando os países chegam a conclusões divergentes sobre a legalidade do mesmo conteúdo.

As questões jurisdicionais são importantes porque leis incompatíveis e reivindicações de jurisdição extraterritorial tornam caro e, talvez, até impossível para as entidades fornecerem funções intermediárias globalmente. Solicitamos veementemente que os formuladores de políticas evitem criar leis com efeitos extraterritoriais e considerem os riscos para a Internet em escala global.

4 Princípios da Formulação de Políticas Para Funções Intermediárias da Internet

Esta seção apresenta três conjuntos de princípios que a Internet Society acredita serem úteis para formuladores de políticas ao considerar aquelas que afetam os serviços de Internet:

1. Princípios gerais aplicáveis a qualquer formulação de políticas relacionadas à Internet ou seu uso.
2. Princípios que se concentram especificamente na proteção de intermediários contra responsabilidades.
3. Exemplos mais amplos de princípios legais e de políticas que podem ser aplicados às funções de intermediários sem comprometer as proteções destes contra responsabilidades.

O Anexo deste documento vai além desses princípios e fornece recomendações detalhadas de políticas sobre uma ampla variedade de funções de **intermediários da Internet**. No Anexo, também discutimos considerações técnicas e práticas para cada uma das funções intermediárias. As informações no Anexo estão agrupadas por tipo de função intermediária, abrangendo desde funções intermediárias geralmente reconhecidas, como hospedagem de conteúdo e entrega de conteúdo, até funções cruciais que permitem a comunicação de dados, a localização de conteúdos e a segurança das comunicações na Internet.

4.1 Princípios Gerais Para a Formulação Prudente de Políticas Relacionadas à Internet

Os seguintes princípios devem orientar amplamente qualquer ação de formulação de políticas relacionadas à Internet em geral, e às funções intermediárias em particular:

A. **Inclusão de partes interessadas no desenvolvimento de políticas**: as políticas serão mais eficazes e terão maior probabilidade de implementação se os formuladores de políticas incluírem outras partes interessadas ao longo do processo de desenvolvimento das políticas. O estreito envolvimento destes atores garantirá que conhecimentos e perspectivas relevantes sejam considerados. Recomendamos fortemente que os governos assegurem a participação mais ampla possível de todas as partes interessadas relevantes ao desenvolver políticas que impactem a Internet.

B. **Realizar uma avaliação de impacto na Internet**: a arquitetura técnica e as operações da Internet podem ser direta e, muitas vezes, involuntariamente afetadas por políticas, regulamentações ou leis aplicadas ao conteúdo na Internet ou às funções intermediárias que permitem a comunicação na Internet. Recomendamos fortemente que os formuladores de políticas realizem uma Avaliação de Impacto na Internet para qualquer nova proposta de política, mesmo que pareça estreitamente direcionada, a fim de entender se pode haver impactos negativos na Internet e em suas operações. A Internet Society analisou as propriedades e habilitadores críticos que são essenciais para a existência e prosperidade da Internet e desenvolveu um Kit de Ferramentas de Avaliação de Impacto da Internet para auxiliar os formuladores de políticas nesse processo.[41]

C. **Delimitar cuidadosamente qualquer regulamentação ou lei** proposta às funções intermediárias específicas que causam o problema: há o risco de abranger um conjunto excessivamente amplo de funções intermediárias, especialmente quando uma preocupação social está associada a um grupo restrito de empresas ou funções. Por exemplo, se houver uma preocupação

41 *Consulte* o artigo da Internet Society, The Internet Way of Networking: Defining the Critical Properties of the Internet (O modo como a Internet se conecta em rede: definindo as propriedades críticas da Internet), 09 de setembro de 2020, disponível em https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/; Internet Society, Internet Impact Assessment Toolkit (Kit de ferramentas para avaliação de impacto da Internet), 08 de novembro de 2021, disponível em https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/introduction/.

a respeito de tipos específicos de conteúdo hospedado por um grupo de sites, a proposta de formulação de políticas deve ser direcionada a esse tipo de conteúdo e a esse grupo específico de sites. Como as funções intermediárias são essenciais para as operações básicas da Internet e para a capacidade de expressão online dos indivíduos, qualquer formulação de políticas deve ser cuidadosamente ajustada para evitar afetar um conjunto excessivamente amplo de funções intermediárias e entidades.

D. **Não usar proteções de intermediários como ameaça ou moeda de troca**: as proteções para funções intermediárias são tão fundamentais para a operação da Internet que não devem ser usadas como incentivo em debates de políticas públicas ou como penalidade em regulamentações ou leis. Uma legislatura não deve, por exemplo, aprovar um projeto de lei que estabeleça que, se um conjunto de empresas não cumprir um determinado requisito, elas perderiam suas proteções de intermediárias. A capacidade dos indivíduos de se expressarem online não deve ser refém de outros objetivos de formulação de políticas. Os formuladores de políticas devem regular ou legislar diretamente para alcançar seus objetivos, sem ameaçar as proteções para as funções intermediárias ou comprometer o funcionamento da Internet.

E. **A política deve promover a abertura**: o acesso à Internet, serviços, aplicações, sites e conteúdos facilita a participação individual. O acesso aberto aprimora a experiência do usuário e o potencial da Internet de impulsionar a inovação, a criatividade e o desenvolvimento econômico. Os formuladores de políticas devem evitar limitar ou bloquear a disponibilidade de funções intermediárias que fornecem acesso à Internet, suas aplicações e serviços.

F. **Intervenções políticas devem ser o mais próximas possível do dano**: há menor probabilidade de causar danos colaterais a outros usuários da Internet e à própria Internet se as intervenções políticas se concentrarem no conteúdo problemático e em sua origem. Por exemplo, em vez de tentar bloquear o acesso ao conteúdo por meio de bloqueio de endereço IP ou DNS — o que também poderia impedir o acesso a conteúdo legítimo e interromper o tráfego da Internet — a pessoa que publicou o conteúdo poderia ser obrigada a removê-lo.

4.2 Princípios Específicos Sobre a Proteção de Intermediários Contra a Responsabilidade

Os quatro princípios a seguir concentram-se em diferentes aspectos das operações e do trabalho das entidades que fornecem funções intermediárias, e a necessidade de oferecer proteções para esse trabalho:

G. **Proteger as funções intermediárias que possibilitam a comunicação na Internet de responsabilidades por "conteúdo gerado pelo usuário", ou seja, conteúdo criado por terceiros**: sem proteções de responsabilidade, a infraestrutura da Internet, bem como as ferramentas básicas que as pessoas usam para acessar e interagir com o conteúdo, seriam paralisadas por ações legais ilimitadas. Sem proteções para essas funções intermediárias, a Internet não poderia operar de forma prática. Recomendamos fortemente que as entidades que fornecem essas funções intermediárias da Internet sejam protegidas de responsabilidades por conteúdo criado por terceiros, que elas transmitem, recebem, armazenam em cache, filtram ou, de outra forma, manipulam.

H. **Proteger as funções intermediárias que hospedam, facilitam e otimizam a entrega de "conteúdo original do site" (ou seja, conteúdo criado pelo proprietário do site)**: Eas entidades que hospedam os mais de 1 bilhão de sites da Internet devem ser protegidas de responsabilidades pelo conteúdo que seus clientes publicam online. Se as empresas de hospedagem fossem responsabilizadas pelo conteúdo que seus clientes colocam online, a maioria não conseguiria continuar oferecendo esse serviço. Isso afetaria especialmente os pequenos e médios provedores de hospedagem na web, aumentando os custos, sufocando a concorrência e reduzindo a disponibilidade e a diversidade de conteúdo online. Os proprietários dos sites devem permanecer responsáveis e potencialmente sujeitos a responsabilidades pelo conteúdo em seus sites, enquanto as entidades que fornecem funções intermediárias, como hospedagem na web, motores de busca e armazenamento em cache, não devem ser responsabilizadas.

I. **Proteger as funções intermediárias que hospedam e exibem conteúdo gerado por usuários**: as entidades que fornecem funções intermediárias para hospedar conteúdo gerado por usuários devem ser protegidas de responsabilidades por esse conteúdo. Sem essa proteção, esses intermediários não seriam

capazes de continuar a carregar o conteúdo. Isso influenciaria de maneira dramática e negativa a capacidade de indivíduos de publicar conteúdo e participar de conversas e debates com outros usuários da Internet. As funções intermediárias são um requisito fundamental para que os indivíduos possam comunicar suas palavras, opiniões, criações artísticas e conversas com outras pessoas. Proteções para intermediários devem ser disponibilizadas às entidades que hospedam conteúdo gerado por usuários para garantir que os usuários possam continuar a se expressar e compartilhar conteúdo online.

J. **Proteger as funções intermediárias de seleção e moderação de conteúdo gerado por usuários**: uma entidade que hospeda conteúdo gerado por usuários *deve* ser capaz de estabelecer "regras de convivência" para os tipos de discussões, obras criativas ou outros conteúdos que deseja hospedar. Por exemplo, se uma entidade que hospeda conteúdo gerado por usuários optar por não hospedar conteúdo "adulto" ou escolher estabelecer regras de comportamento para os usuários, ela deve ter liberdade para fazê-lo. Essas entidades, que desempenham funções intermediárias de hospedagem de conteúdo do usuário, também devem ser protegidas de responsabilidades por remover conteúdo irrelevante ou questionável. Dado o vasto volume de conteúdo gerado por usuários carregado e compartilhado a cada minuto, a curadoria é muitas vezes crucial para ajudar os usuários a encontrar um conteúdo específico ou tipo de conteúdo. A curadoria geralmente envolve o uso de um ou mais algoritmos, desde um algoritmo simples que apresenta o conteúdo na ordem em que é recebido até algoritmos mais sofisticados que apresentam o conteúdo com base no perfil do usuário e em suas interações com o serviço. A filtragem e as "regras de convivência" permitem que os serviços de conteúdo hospedado e seus usuários evitem serem sobrecarregados com material irrelevante, inconveniente e malicioso, que obscurece o conteúdo legítimo e afasta a participação individual na Internet. Regimes de proteção de intermediários devem proteger as entidades contra responsabilidade legal por fazer cumprir suas próprias regras de convivência ou remover conteúdo questionável.

4.3 Princípios Jurídicos e de Políticas Específicos Que Podem Ser Aplicados às Funções Intermediárias Sem Prejudicar as Comunicações na Internet

As funções intermediárias são essenciais para qualquer conteúdo transmitido, hospedado ou gerenciado de outra forma, e essas funções precisam de proteção contra responsabilidade pelo gerenciamento desse conteúdo. No entanto, isso *não* significa que as entidades que fornecem essas funções não possam ser reguladas. Existe uma ampla variedade de políticas, regulamentações e leis que já se aplicam, ou podem se aplicar, às entidades que fornecem funções de intermediação, incluindo, por exemplo, leis de concorrência e proteção ao consumidor. Abaixo estão alguns princípios de política que podem ajudar a abordar algumas das preocupações políticas que surgiram em relação às funções de intermediação na Internet:

Privacidade e segurança do usuário

- A privacidade e a segurança são essenciais para proteger a confidencialidade, integridade e privacidade das comunicações dos indivíduos.
- As políticas devem aplicar regras rigorosas para proteger a privacidade e aumentar a segurança das comunicações na Internet.
- As entidades que fornecem funções intermediárias devem adotar práticas como “segurança desde o design” e “privacidade desde o design”, implementando as melhores práticas do setor e inovando para melhorar os recursos de privacidade e segurança.

Controle e escolha do usuário

- Proporcionar aos usuários a capacidade de escolher e controlar o conteúdo que consomem permite que eles se protejam filtrando conteúdo e fontes irrelevantes ou indesejadas.
- As políticas devem buscar ampliar as escolhas e o controle dos usuários sobre os serviços online que utilizam e o conteúdo que decidem visualizar.

Acessibilidade do usuário

- A Internet deve estar disponível para todos.

- Políticas que promovem acessibilidade robusta podem orientar o design e a implementação de funções intermediárias, permitindo que os indivíduos com diferentes necessidades de acessibilidade participem da comunicação online.[42]
- Entidades que oferecem funções intermediárias na Internet devem buscar fornecer conteúdos e controles online que interajam de forma previsível e eficaz com tecnologias assistivas.

Direitos do usuário

- A Internet permite que os usuários exerçam seus direitos humanos online. Funções intermediárias desempenham um papel essencial na facilitação de direitos como liberdade de expressão, associação e acesso à informação online. A interferência por parte de governos nas operações de funções intermediárias pode impedir ou dificultar o exercício desses direitos pelos indivíduos.
- Os formuladores de políticas devem avaliar, evitar ou minimizar o impacto potencial de quaisquer políticas propostas sobre o exercício dos direitos humanos.

Habilidades digitais do usuário

- Habilidades digitais (também conhecidas como alfabetização digital) capacitam os usuários a serem mais seletivos no conteúdo que consomem, a reconhecer desinformação, a gerenciar configurações de privacidade e segurança e a relatar conteúdos indesejados.
- As políticas devem promover habilidades digitais para usuários de todas as faixas etárias e necessidades, por meio de educação digital em escolas, bibliotecas públicas, programas governamentais e iniciativas comunitárias.

Não discriminação do usuário

- Os indivíduos têm o direito de serem tratados de forma igualitária, independentemente de categorias como raça, cor, sexo, nacionalidade, idioma, religião ou etnia, origem nacional ou social.[43]

42 Consulte as Diretrizes de Acessibilidade para Conteúdo Web 2.2 do W3C, Documentos de Compreensão em https://www.w3.org/WAI/WCAG22/Understanding/intro.

43 A lista de classes e características protegidas pode variar dependendo do país e/ou jurisdição legal. As listadas aqui são retiradas do Artigo 1 da Convenção das Nações Unidas sobre a Eliminação de Todas as Formas de Discriminação Racial, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial.

- As políticas devem prevenir discriminação com relação a usuários individuais ou grupos com base em classes e características legalmente protegidas na prestação de serviços de Internet.

Conhecimento do usuário

- O acesso a informações sobre os termos de serviço associados à hospedagem, curadoria e moderação de conteúdo gerado pelo usuário capacita os usuários a fazer escolhas informadas sobre os serviços que utilizam.
- As políticas devem incentivar uma transparência significativa sobre como o conteúdo será hospedado, curado e moderado.

Acesso do usuário a serviços competitivos

- A Internet tem sido historicamente um ótimo espaço para pequenos inovadores e empreendedores iniciarem e desenvolverem negócios.
- Os formuladores de políticas, ao aplicarem políticas de concorrência, devem ter cuidado para não enfraquecer as proteções de intermediários.

Riscos ao usuário

- Novas funções intermediárias ou a aplicação de funções conhecidas a novas situações podem ter consequências não intencionais para os usuários. Isso pode incluir riscos à segurança, proteção e privacidade dos usuários, bem como da própria Internet.
- As políticas devem incentivar uma abordagem baseada em riscos para o exercício de funções intermediárias, recompensando a mitigação de efeitos adversos, reconhecendo, ao mesmo tempo, que o risco zero não existe.

Relato pelo usuário

- Em vista do vasto volume de conteúdo carregado e compartilhado a cada segundo, os usuários podem ser os primeiros a identificar conteúdo problemático.
- As políticas devem incentivar entidades que oferecem funções intermediárias que exibem conteúdo gerado por usuários a fornecerem meios fáceis para os usuários relatarem conteúdo problemático.

5 Destaques — Considerações Sobre Políticas Para Funções Intermediárias Específicas

Nesta seção, nos baseamos nas considerações de políticas mencionadas acima. Os "destaques" identificam cenários específicos que merecem uma discussão mais aprofundada. Mais detalhes sobre a gama completa de funções intermediárias estão descritos no Anexo deste documento.

5.1 Destaque: Considerações Sobre Políticas Para Plataformas de "Mídias Sociais" Que Hospedam, Selecionam e Moderam Conteúdo Gerado Por Usuários

Grande parte da atenção das políticas públicas globais voltadas às entidades que hospedam conteúdo gerado por usuários tem se concentrado em um pequeno número de grandes "plataformas", especialmente sites de mídias sociais amplamente utilizados por usuários em todo o mundo. Muitas dessas preocupações *não* estão diretamente relacionadas às proteções de intermediários que abrangem o conteúdo gerado por usuários. Em vez disso, os formuladores de políticas estão preocupados com questões como coleta e uso de dados pessoais dos usuários, práticas de publicidade, discriminação, falta de transparência e controle por parte dos usuários, bem como técnicas para manter o engajamento contínuo dos usuários na plataforma, apenas para citar alguns dos tópicos em alta. Nenhuma dessas preocupações está relacionada ao objetivo geral das proteções de intermediários: proteger e incentivar a participação individual na Internet. Não é apropriado abordar

essas preocupações removendo ou impondo condições às proteções de intermediários.

Do ponto de vista das proteções de intermediários, uma grande plataforma de mídia social que hospeda conteúdo gerado por usuários não é essencialmente diferente de um pequeno site que faz o mesmo. Nenhum dos dois poderia operar se fossem responsabilizados por conteúdo difamatório, assediador ou ilegal publicado por seus usuários. Há maneiras mais eficazes de lidar com conteúdos problemáticos que evitam expor intermediários à responsabilidade pelo conteúdo gerado por usuários (detalhadas na seção 4.3 acima). Ambos os tipos de intermediários precisam de fortes proteções para as funções intermediárias envolvidas na hospedagem de conteúdo gerado por usuários. Um pequeno site não tem os recursos para revisar previamente todo o conteúdo gerado por usuários e não pode operar sob o risco de ameaças de enormes responsabilidades. Uma grande plataforma enfrenta restrições semelhantes, mesmo que tenha mais recursos, devido à imensa quantidade de conteúdo gerado por usuários — em vários idiomas — carregado por milhões de usuários a cada minuto.

No entanto, as proteções de intermediários contra responsabilidade por conteúdo gerado por usuários não significam que os formuladores de políticas estejam impotentes para lidar com preocupações importantes de políticas públicas. Por exemplo, se a preocupação for que uma plataforma está curando conteúdo de forma a apresentar sistematicamente uma seleção discriminatória de conteúdo aos usuários, então leis existentes ou novas de não discriminação poderiam ser aplicadas à plataforma. Se a preocupação for que uma plataforma está projetando sua interface de usuário para "viciar" os usuários, então leis de saúde ou de proteção ao consumidor poderiam ser usadas para proteger os usuários de uma interface prejudicial à saúde ou que os sujeite a manipulação. Se a preocupação for que uma plataforma está usando indevidamente os dados pessoais de seus usuários, leis de privacidade e proteção de dados poderiam ser aplicadas para punir e deter essas práticas. Se a preocupação for que uma plataforma está enganando seus usuários sobre seus serviços, leis antifraude podem ser aplicadas.

Existem riscos em *todos* os locais de interação social, sejam eles off-line sejam online. Apesar das melhores intenções, o engajamento social de crianças em um playground pode, às vezes, envolver bullying e outros comportamentos indesejados. O engajamento social presencial entre colegas de trabalho pode, às vezes, envolver assédio. O ecossistema

online pode simultaneamente exacerbar e mitigar alguns desses problemas — a ausência de interação física direta pode aumentar o assédio ou o bullying, mas também pode abrir oportunidades para suporte entre pares. Além disso, o espaço online contém um vasto número de locais para interação social, permitindo que as pessoas abandonem um ambiente virtual excessivamente tóxico e se juntem a um mais acolhedor.

Uma área importante de preocupação é o uso de algoritmos por plataformas para selecionar e exibir conteúdo aos usuários. Os formuladores de políticas identificaram o risco de que algoritmos possam ser usados para manipular o comportamento dos usuários com efeitos adversos, discriminá-los ou disseminar conteúdo ilícito ou prejudicial. No entanto, os algoritmos sempre foram usados pelas plataformas de mídia social e um número crescente de outros sites, e são essenciais para suas operações. O enorme volume de conteúdo compartilhado na Internet exige uma dependência crescente de algoritmos que automaticamente organizam e exibem o conteúdo. Os algoritmos procuram por conteúdo malicioso ou incorreto. Eles melhoram sites de comércio eletrônico e gerenciam o conteúdo exibido em plataformas de mídias sociais. Eles também são vitais para aumentar a acessibilidade e converter voz em legendas de texto para pessoas com deficiência auditiva.[44]

Nosso conselho aos formuladores de políticas é lembrar que os algoritmos não são problemáticos *por si só*, mas sim a forma como são usados. Por exemplo, um algoritmo que produz sistematicamente resultados discriminatórios contra membros de classes protegidas, como raça ou religião, é um alvo legítimo para formulação de políticas. O objetivo deve ser criar políticas que abordem diretamente a questão, permitindo o uso apropriado da moderação e curadoria algorítmica.

5.2 Destaque: Considerações Sobre Políticas Para "Redes Federadas" Que Viabilizam Novas Abordagens Para Engajamento dos Usuários

As "redes federadas" têm atraído cada vez mais atenção nos últimos anos. Destacamos essas redes porque elas aplicam uma abordagem mais descentralizada para a hospedagem, compartilhamento, curadoria e

44 Para uma discussão mais detalhada sobre as questões, consulte o parecer amicus curiae da Internet Society no caso Gonzalez v. Google LLC, 598 US 617 (2023), disponível em https://www.internetsociety.org/wp-content/uploads/2023/01/Internet-Society-Gonzalez-v-Google-Amicus-Brief.pdf.

moderação de conteúdo gerado por usuários do que as plataformas de mídias sociais mais tradicionais. Em vez de uma única entidade controlar uma comunidade de mídia social, por exemplo, as tecnologias federadas permitem que muitas comunidades menores se conectem e compartilhem conteúdo em todo o ecossistema federado. Isso cria uma experiência social semelhante, mas com uma abordagem mais local para a moderação.

Os serviços "federados" têm aparecido recentemente nas notícias porque alguns agora competem mais diretamente com algumas das grandes empresas e plataformas de mídias sociais. Um exemplo é o Mastodon, baseado no padrão ActivityPub do World Wide Web Consortium.[45] As funções do Mastodon são diretamente análogas às do Twitter/X em termos de capacidade de discussão global. Uma diferença significativa, no entanto, é que o Mastodon é uma coleção de servidores operados por diferentes entidades que optaram por participar da rede federada, em vez de um conjunto de servidores controlados por uma única empresa. Cada servidor individual que participa da rede federada Mastodon pode definir e controlar suas próprias regras de moderação de conteúdo de forma significativa.[46]

Embora as mídias sociais federadas tenham sido um tópico em alta recentemente, os serviços federados não são um fenômeno novo na Internet. Por exemplo, o e-mail na Internet utiliza um modelo federado: milhões de entidades operam seus próprios servidores de e-mail separados para suas empresas, organizações, universidades ou até mesmo famílias. Nos bastidores, esses servidores federados usam protocolos de e-mail para enviar e receber mensagens sem necessidade de acordos prévios.

No campo das mídias sociais, essas redes federadas emergentes têm o potencial de democratizar a hospedagem de mídias sociais. Elas oferecem a possibilidade de uma curadoria e moderação de conteúdo muito mais detalhadas e próximas do usuário final . O modelo distribuído requer muitos servidores Mastodon e deu origem a uma nova função de intermediário: hospedar um servidor Mastodon, o equivalente ao provedor de hospedagem na web ou serviço de e-mail.[47] O sucesso

45 https://www.w3.org/TR/activitypub/.

46 O Mastodon ganhou rapidamente popularidade depois que o X alterou drasticamente suas políticas de moderação de conteúdo. O Mastodon oferece aos usuários maior controle sobre o conteúdo que veem e com quais outros usuários interagem. É uma abordagem distribuída para as mídias sociais que capacita entidades menores e até mesmo indivíduos a hospedar mídias sociais geradas por usuários e tomar decisões sobre qual conteúdo permitir ou não em seu próprio servidor e com quais outros servidores do Mastodon se conectar.

47 Por exemplo, o provedor de SaaS Cloudflare oferece um produto: "Welcome to Wildebeest: The Fediverse on Cloudflare" (Bem-vindo ao Wildebeest: O Fediverso no Cloudflare), Blog do Cloudflare, 02 de agosto de 2023, https://blog.cloudflare.com/welcome-to-wildebeest-the-fediverse-on-cloudflare.

atual das redes de mídias sociais federadas levou a Meta a explorar a possibilokidade de permitir que os usuários do Threads compartilhem suas publicações com outros servidores compatíveis com o ActivityPub, alcançando assim os usuários do Mastodon.[48]

Nossa preocupação é que as redes federadas possam ser prejudicadas inadvertidamente por regulamentações ou leis que não considerem como essas redes modernas se encaixam no cenário de "mídias sociais". Como exemplo, se um país promulgasse uma lei para se aplicar a "serviços de mídias sociais" com a intenção de atingir as maiores plataformas, essa terminologia poderia abranger toda a rede federada do sistema Mastodon e seus milhares de servidores cooperantes. Uma lei direcionada às maiores empresas de tecnologia poderia acabar afetando — e prejudicando — um conjunto completamente diferente de entidades.

Nosso conselho aos formuladores de políticas que buscam regulamentar plataformas de mídias sociais é agir com cuidado e estar atentos ao impacto provável de uma regra ou regulamentação proposta nas redes federadas. Sem esse cuidado, pode haver impactos prejudiciais não intencionais nessas redes, que oferecem uma alternativa às grandes plataformas de mídias sociais.

5.3 Destaque: Considerações Sobre Políticas Para o Ecossistema de Jogos Interativos Online

Os jogos online têm recebido atenção particular das políticas públicas, pois muitos de seus usuários são crianças e adolescentes. Por exemplo, em 2011, a Coreia do Sul aprovou (mas posteriormente revogou) a Lei de Revisão da Proteção à Juventude, que restringia os horários em que menores de 16 anos podiam jogar videogames online, bloqueando o acesso entre meia-noite e 6h.[49] Em 2019, a China limitou os menores a 90 minutos de jogo por dia útil e proibiu-os de jogar online entre 22h e 8h, impondo restrições adicionais em 2021.[50] As preocupações vão desde o vício até comportamentos semelhantes a jogos de azar, exposição a conteúdo inadequado, contato com estranhos e violações de privacidade.

48 O Threads entrou no fediverso, Blog de Engenharia da Meta, 21 de março de 2024, https://engineering.fb.com/2024/03/21/networking-traffic/threads-has-entered-the-fediverse/.

49 A lei foi posteriormente abolida em 2021. Consulte https://en.wikipedia.org/wiki/Shutdown_law.

50 China mantém limite diário de 1 hora para jogos online para crianças, Associated Press, Zen Soo, 19 de janeiro de 2023, https://apnews.com/article/gaming-business-children-00db669defcc8e0ca1fc2dc54120a0b8.

Os jogos online geralmente são interativos com outros usuários e frequentemente incluem ferramentas de comunicação em tempo real. As ferramentas de comunicação mais comuns nos jogos são recursos de áudio e mensagens, mas existem métodos mais sutis de comunicação: escolha e modificação de avatares, comportamentos específicos durante o jogo e compartilhamento de pontuações, classificações e outras conquistas. Alguns jogos online também permitem que os usuários façam upload e compartilhem modificações no jogo. Os jogos online também inspiraram novos gêneros de engajamento em outras plataformas, como YouTube e Twitch, além do campo dos e-sports.[51]

Nosso conselho aos formuladores de políticas é estar atentos às funções de intermediários desempenhadas pelas plataformas de jogos interativos online. Atualmente, a maioria dos sistemas de jogos interativos conectados à Internet, com ou sem console de hardware, permite uma ampla gama de "conteúdo gerado por usuários", desde conversas simples entre jogadores até módulos adicionais desenvolvidos por jogadores que complementam e expandem o ambiente de jogo. As plataformas de jogos interativos desempenham funções de intermediários, e os principais regimes de proteção de intermediários se aplicam igualmente ao ecossistema de jogos.

No entanto, como observado no nosso destaque acima sobre plataformas de mídias sociais, os formuladores de políticas não estão impotentes para lidar com práticas prejudiciais. Por exemplo, se a preocupação for que algumas "loot boxes" em um jogo constituem práticas enganosas ou jogos de azar ilegais, as leis de proteção ao consumidor ou de proibição de jogos de azar ilegais devem ser aplicáveis diretamente a esses comportamentos.

5.4 Destaque: Considerações Sobre Políticas Para Sistemas de Realidade Virtual e Realidade Aumentada Conectados à Internet

Os produtos de realidade virtual (RV) e realidade aumentada (RA) estão sendo rapidamente adicionados ao ecossistema da Internet. Os propósitos da RV e RA são diversos, mas frequentemente são usados como parte de

51 Para obter mais informações sobre Esports, consulte a Wikipedia em https://en.wikipedia.org/wiki/Esports.

um sistema interativo de comunicação.[52] Alguns desses sistemas requerem dispositivos especializados, como óculos, luvas ou headsets, enquanto outros são acessíveis por meio de smartphones.

Assim como no ecossistema de jogos, os sistemas de RV e RA conectados à Internet geralmente suportam "conteúdo gerado por usuários", incluindo uma ampla gama de comunicações entre usuários.[53] Portanto, assim como os jogos, a maioria dos principais regimes de proteção de intermediários pode ser aplicável a sistemas de RV e RA.

Do ponto de vista das políticas públicas, os sistemas de RV e RA se sobrepõem consideravelmente às mídias sociais e a outros serviços de comunicação um-para-um ou um-para-muitos. No entanto, a RV e a RA apresentam desafios adicionais, como:

- A configuração e o uso de avatares representativos podem criar, ao menos na percepção, uma conexão mais estreita entre a identidade real do indivíduo e sua identidade na realidade virtual.
- Alguns sistemas de RA podem ser usados em qualquer lugar no espaço físico, superpondo elementos virtuais ao ambiente físico. Teoricamente, esses sistemas poderiam causar danos diretos no mundo físico, como acidentes de trânsito ou lesões pessoais.[54]
- Os sistemas de RA podem ser capazes de incluir pessoas que não estão online e que não deram consentimento no ambiente aumentado.

Assim como nas mídias sociais e nos jogos online, nosso conselho aos formuladores de políticas é que as preocupações relacionadas a questões como privacidade, vício de usuários e segurança pessoal sejam melhor resolvidas usando as leis existentes nessas áreas, em vez de modificar as proteções de intermediários ou tentar construir um novo conjunto de políticas específicas para RV e RA.

52 Uma visão de como a realidade virtual (RV) pode ser usada é o "metaverso", descrito pela primeira vez no romance de ficção científica de 1992 "Snowcrash", de Neal Stephenson. Em sua visão, o metaverso é um espaço de realidade virtual no qual os usuários podem interagir uns com os outros usando um avatar em um ambiente tridimensional gerido por computador.

53 Por sua natureza, os sistemas de RV e RA podem suportar um conjunto rico de ferramentas de comunicação: escrita, falada e não verbal, como movimentos de cabeça e mãos, expressões faciais, orientação corporal, proximidade e postura.

54 Consulte, por exemplo, o "Pokémon Go Death Tracker" ("Rastreador de Mortes" do Pokémon Go) em https://pokemongodeathtracker.com/.

5.5 Destaque: Considerações Sobre Políticas Para Funções Intermediárias Que Viabilizam Publicidade na Internet Advertising on The Internet

O conteúdo publicitário é um tipo especial de conteúdo online. Embora frequentemente apareça ao lado de conteúdo gerado por usuários, ele geralmente não é contribuído por indivíduos. Alguns anúncios podem ser considerados conteúdo original do site, como uma propaganda de um jantar especial no Dia de Ano Novo no site de um restaurante. No entanto, a grande maioria do conteúdo publicitário exibido na Internet é criado por entidades diferentes dos proprietários do site com o propósito específico de publicidade e é colocado para gerar receitas de anúncios. Esse conteúdo é geralmente incorporado e dinâmico.

A capacidade de exibir conteúdo publicitário na Internet permitiu que empresas oferecessem seus serviços com pouco ou nenhum custo monetário e que indivíduos ganhassem dinheiro por meio de sites de compartilhamento de conteúdo gerado por usuários. Alguns argumentam que o sistema publicitário deve ser protegido de responsabilidade, pois, sem a publicidade "pagando as contas", a Internet teria muito menos serviços e recursos e uma menor participação individual. Sem a receita publicitária, mais serviços cobrariam pelo uso, aumentando assim a exclusão digital.

Outros acreditam que o sistema publicitário — especialmente o sistema de publicidade comportamental — é muito problemático e deveria ser significativamente restringido. Eles argumentam que a publicidade direcionada explora proteções de privacidade insuficientes, permitindo que serviços online e a indústria lucrem financeiramente com conteúdo gerado por usuários e interações online.

Devido à natureza global da Internet, o alcance e o impacto da publicidade online podem ser muito maiores do que a publicidade em jornais, televisão e rádio. Os anúncios online podem ser personalizados e direcionados para um usuário individual ou grupos muito pequenos de pessoas em termos de tempo, localização física e contexto. Os anunciantes e o ecossistema de empresas que suportam a publicidade online rastreiam usuários entre dispositivos e até no mundo real.

Além dos debates a respeito do sistema publicitário existente, é inegável que o sistema de anúncios depende de proteções de responsabilidade

de intermediários em alguns contextos.[55] Na ponta visível dos sistemas de anúncios — os sites e serviços onde os anúncios são exibidos — essas proteções podem entrar em jogo. Na maioria dos serviços, o conteúdo dos anúncios exibidos ao lado do conteúdo gerado por usuários está fora do controle do usuário e, geralmente, também fora do controle do proprietário do site. Tecnicamente, o conteúdo publicitário exibido por meio de um site, geralmente, não é hospedado na infraestrutura do serviço, mas em um servidor gerenciado pela rede de anúncios.

Nosso conselho aos formuladores de políticas é agir com cautela ao elaborar regulamentações para o ecossistema publicitário, devido ao difícil equilíbrio entre os benefícios esperados e os potenciais danos. O ecossistema de publicidade online desempenha um papel importante ao sustentar o amplo acesso à expressão, mas, ao mesmo tempo, levanta preocupações políticas sobre privacidade, segmentação inadequada e desinformação. No entanto, como qualquer outra função de intermediário, isso não significa que um governo não possa regular diretamente os sistemas de anúncios. Por exemplo, na União Europeia, a primeira Diretiva de Comércio Eletrônico impôs diretamente alguns requisitos específicos de transparência para anúncios online, e o mais recente Ato de Serviços Digitais expandiu significativamente esses requisitos de transparência e proibiu certas técnicas de design que buscavam manipular ou enganar os usuários.

5.6 Destaque: Considerações Sobre Políticas Para Pagamentos e Outras Compensações Econômicas Por "Conteúdo Gerado Pelo Usuário" Abrangidas Pelos Princípios de Intermediários da Internet

O sistema de publicidade na internet levanta uma questão muito mais ampla: se as proteções para intermediários são apropriadas para cobrir conteúdo pelo qual dinheiro ou outra forma de valor econômico tenha sido trocado como parte da colocação do conteúdo em um site. A questão pode se manifestar em uma série de cenários diferentes:

55 O funcionamento interno dos sistemas de publicidade online é bastante opaco, com múltiplas entidades interconectadas e independentes trabalhando juntas, tanto de forma explícita quanto implícita. Desembaraçar esses sistemas para entender como as proteções de responsabilidade de intermediários podem se aplicar está além do escopo deste documento.

- Se um site publica artigos escritos por usuários, mas só o faz se o usuário pagar ao site para publicar o artigo, o site deve ser protegido da responsabilidade pelo conteúdo que foi pago para publicar? E se o pagamento for muito pequeno? E se for grande?
- Se um site paga a um fornecedor de conteúdo (como um "influenciador" conhecido ou outra figura) para postar conteúdo no site, o site deve ter alguma responsabilidade legal pelo conteúdo que pagou para publicar e depois hospedou? O valor do pagamento faria diferença na análise?
- Se um site compartilha a receita de publicidade com o fornecedor de conteúdo, isso altera a relação e a responsabilidade do site?[56]
- Se a relação comercial entre anunciantes e sites remove as proteções e torna o operador do site responsável pelo conteúdo dos anúncios, como isso afetaria o sistema de publicidade? Isso prejudicaria sites que recebem uma quantia modesta de receita com um nível baixo de publicidade?
- Se as proteções de responsabilidade forem removidas para funções intermediárias de hospedagem de conteúdo gerado por usuários que foi produzido por compensação econômica, isso causaria impactos econômicos, sociais ou técnicos no mercado de conteúdo? As empresas criariam alternativas artificiais ou menos responsáveis para evitar a responsabilidade?[57]
- Se o mercado de conteúdo pago for dominado por algumas entidades que são fortemente integradas horizontal e verticalmente em serviços online, como isso prejudicaria o cenário competitivo de conteúdo?

No contexto dos Estados Unidos, pagamentos por conteúdo em qualquer direção, geralmente, não influenciam as proteções para intermediários.[58] As questões que levantamos acima ajudam a mostrar as complexidades, vantagens e desvantagens de se concentrar na compensação econômica.

56 Por exemplo, o YouTube possui um sistema amplamente acessível a todos os usuários que publicam vídeos no site. Em troca da permissão para exibir anúncios ao lado dos vídeos de um usuário, o YouTube compartilha uma parte da receita publicitária proveniente dos anúncios exibidos. Se os vídeos do usuário forem muito populares, ele receberá uma renda com os anúncios, às vezes, uma quantia substancial. Alguns criadores de conteúdo agora ganham ou suplementam significativamente sua renda com os pagamentos do YouTube. Se o YouTube fosse responsabilizado pelos vídeos pelos quais os usuários são pagos, o YouTube poderia continuar oferecendo esses pagamentos?

57 Por exemplo, eles buscariam evitar a responsabilidade compensando determinados criadores de conteúdo por "ter uma conta" em vez do conteúdo que eles produzem, ou ofereceriam outros serviços e assinaturas gratuitamente?

58 Propostas para remover as proteções da lei dos EUA para certos tipos de anúncios pagos não tiveram sucesso.

5.7 Destaque: o Impacto de Níveis Nacionais Variados de Proteção à Liberdade de Expressão

Ao entender e criar políticas relacionadas às proteções contra responsabilidade por funções intermediárias, é importante reconhecer a influência que as proteções legais nacionais para a fala e a livre expressão terão nas políticas que podem afetar a capacidade dos indivíduos de se comunicarem online, seja compartilhando seu próprio conteúdo ou o conteúdo de terceiros.

Existem proteções significativamente diferentes para a fala e a livre expressão em diferentes países ao redor do mundo, e essas diferenças afetam as escolhas políticas disponíveis dentro de um país. Alguns países estabelecem o direito à liberdade de expressão em suas constituições, incluindo Brasil,[59] Equador,[60] Japão,[61] Peru,[62] e os Estados Unidos.[63] Outros países e jurisdições têm menos restrições sobre a capacidade do governo de, por exemplo, exigir que empresas privadas tomem medidas para restringir ou impedir certos tipos de discurso. Outros países podem priorizar outros objetivos de políticas, como a privacidade sobre a liberdade de expressão ou a coesão social sobre os direitos individuais. Regimes nacionais diferentes podem ajudar a explicar as abordagens nacionais distintas em relação às proteções contra a responsabilidade de intermediários. Um exemplo de abordagens diferentes impulsionadas por leis constitucionais ou nacionais são os regimes de "notificação e retirada", utilizados pela União Europeia e por alguns outros países para exigir a remoção de conteúdo online. Esse tipo de mandato enfrentaria

59 Consulte o Artigo 5 da Constituição da República Federativa do Brasil, disponível em https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.

60 See Article 66 section 6 of the Constitución del Ecuador, available at https://www.gob.ec/sites/default/files/regulations/2018-11/constitucion_de_bolsillo.pdf.

61 Consulte o Artigo 21 da Constituição do Japão, disponível em https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html.

62 Consulte o Artigo 2, seção 4, da Constitución Política del Perú, disponível em https://www.congreso.gob.pe/constitucionyreglamento/.

63 Consulte a Primeira Emenda da Constituição dos Estados Unidos, disponível em https://www.archives.gov/founding-docs/bill-of-rights/what-does-it-say.

sérias dificuldades constitucionais se implementado em países com fortes direitos à liberdade de expressão ou fala, como os Estados Unidos.[64]

Nosso conselho para os formuladores de políticas é compreender cuidadosamente quaisquer restrições sobre a regulação da fala impostas pelas leis constitucionais e estatutárias nacionais, bem como as convenções e acordos internacionais aplicáveis sobre a liberdade de expressão.

Além dessas questões, se um país deseja apoiar a capacidade de seus cidadãos de participar de conversas online e iniciar esforços empreendedores para criar novos serviços online, ele deve adotar proteções para funções intermediárias para garantir que os serviços de Internet possam carregar o discurso dos usuários sem riscos significativos de responsabilidade.

5.8 Destaque: Diferenciando a Proteção de Responsabilidade de Intermediários da Lei e Política de Direitos Autorais

Em muitos países e regiões — incluindo os Estados Unidos[65] e a União Europeia[66]—existem abordagens legais distintas que cobrem as proteções de intermediários contra responsabilidade por "conteúdo gerado por usuários" de forma diferente de "uso de conteúdo protegido por direitos autorais de terceiros". No caso do conteúdo gerado por usuários, a questão legal é se o conteúdo em si é ilegal ou causou dano. No caso dos direitos autorais, as questões legais pertinentes são se a pessoa que publicou o conteúdo (a) possui os direitos autorais, (b) tem uma licença para publicar o conteúdo, ou (c) está de alguma forma protegida por "uso justo" ou outras limitações da lei de direitos autorais. Este documento se concentra no primeiro cenário, e não no conteúdo que infringe direitos autorais.

64 Os regimes de "aviso e retirada" também têm sido notoriamente sujeitos a abusos e usos indevidos. Consulte, por exemplo, "Warning: repressive regimes are using DMCA takedown demands to censor activists" (Aviso: regimes repressivos estão usando exigências de remoção de DMCA para censurar ativistas), 13 de janeiro de 2023, disponível em https://www.accessnow.org/dmca-takedown-demands-censor-activists/; "Notice and Takedown Mechanisms: Risks for Freedom of Expression Online" (Mecanismos de aviso e retirada: riscos para a liberdade de expressão online), 07 de setembro de 2020, disponível em https://www.eff.org/files/2020/09/04/mcsherry_statement_re_copyright_9.7.2020-final.pdf; ; "Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech" (Problemas com remoções de campanhas: como reivindicações de direitos autorais sem mérito ameaçam o discurso político online), setembro de 2010, disponível em https://cdt.org/wp-content/uploads/pdfs/copyright_takedowns.pdf.

65 Consulte o "Digital Millennium Copyright Act" (Lei do Milênio Digital sobre Direitos Autorais), código 17 dos EUA § 512, disponível em https://www.law.cornell.edu/uscode/text/17/512.

66 Consulte o Artigo 17 da Diretiva de Direitos Autorais da UE (Diretiva sobre os Direitos Autorais no Mercado Único Digital), disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.130.01.0092.01.ENG&toc=OJ:L:2019:130:TOC.

Muitas leis específicas de direitos autorais contêm requisitos de notificação e remoção, nos quais o proprietário dos direitos autorais pode notificar uma empresa de hospedagem sobre conteúdo que se alega ser protegido por direitos autorais. Após a notificação, o host tem um certo tempo para remover o conteúdo especificado. A abordagem centrada nos direitos autorais, que geralmente não exige uma ordem judicial, às vezes levou a abusos, com pessoas usando notificações de retirada de direitos autorais para impedir discursos legítimos.[67] Por outro lado, como observado na Seção 3.5, os poucos países que adotaram uma abordagem de notificação e retirada para conteúdo problemático gerado por usuários geralmente exigem uma ordem judicial.

5.9 Destaque: Inteligência Artificial

Após o lançamento de serviços de IA[68], generativa voltados para o consumidor, uma pergunta comum que surgiu entre os formuladores de políticas é se, e em que medida, as proteções para intermediários se aplicam aos serviços que utilizam "inteligência artificial" (IA). IA é um termo muito amplo que abrange desde algoritmos simples até redes neurais artificiais. Ferramentas de IA podem realizar tarefas específicas (por exemplo, reconhecer imagens), reagir a situações específicas (por exemplo, filtrar spam, aumentar a eficiência de roteamento) e aprender e adaptar respostas (por exemplo, interagir com os usuários como robôs de bate-papo). A IA já está presente em todo o ecossistema da Internet, como o roteamento de tráfego, a busca e a localização de páginas da web e o gerenciamento de literalmente bilhões de peças de conteúdo.

No contexto de conteúdo online, há pelo menos três aspectos da IA que merecem destaque. O primeiro diz respeito ao uso de IA na oferta de serviços online. Diversos tipos de IA têm sido usados para fornecer serviços online há muitos anos. Por exemplo, a tecnologia usada para selecionar e curar conteúdo a ser exibido aos usuários inclui aspectos de IA desde pelo menos 2006.[69] O uso de IA na busca online remonta a um

67 Às vezes chamado de "censura por meio de direitos autorais". Para obter alguns exemplos, consulte "Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Speech" (2010), Center for Democracy & Technology, disponível em https://cdt.org/wp-content/uploads/pdfs/copyright_takedowns.pdf; "Copyright shouldn't be a tool of censorship" (2017) de Daniel Nazer e Mitch Stoltz, Electronic Frontier Foundation, disponível em: https://www.eff.org/deeplinks/2017/01/copyright-shouldnt-be-tool-censorship.

68 Para uma explicação sobre inteligência artificial generativa, consulte a Wikipedia em https://en.wikipedia.org/wiki/Generative_artificial_intelligence.

69 Consulte o artigo de Cait McNamara, "The Evolution of AI on Social Media" (A Evolução da IA nas Mídias Sociais), maio de 2024, disponível em https://favola.co.uk/the-evolution-of-ai-on-social-media/.

período ainda mais antigo.[70] Conforme discutido anteriormente neste artigo e no Anexo, as leis de proteção de intermediários geralmente protegem atividades que incluem curadoria, filtragem, triagem, escolha e busca de conteúdo. Essas proteções provavelmente se aplicam independentemente de a tecnologia incluir ou não um componente de IA.

O segundo aspecto, mais recente, relaciona-se às respostas geradas por IA às buscas dos usuários por informações: se a produção de IA, que foi treinada com vastas quantidades de conteúdo gerado por usuários, deve ser vista como "conteúdo gerado por usuários". As opiniões variam sobre quando o conteúdo gerado por IA deve ser caracterizado como "conteúdo criado por terceiros" e, portanto, coberto pelas proteções de intermediários contra responsabilidade. Embora algumas produções desses serviços de IA possam conter conteúdo específico gerado por usuários, a totalidade da produção pode ser vista como conteúdo novo criado pelo serviço.

O terceiro aspecto da IA sendo amplamente discutido é se serviços de IA que produzem textos, imagens, sons ou vídeos em resposta a solicitações dos usuários devem ser responsáveis pela produção de conteúdo ilegal ou ilícito. Esses tipos de serviços de IA claramente podem permitir a criatividade individual dos usuários, mas também é discutível se o serviço de IA é cocriador do conteúdo gerado.

Não buscamos resolver essas questões neste artigo nem fornecer recomendações detalhadas de políticas sobre o tratamento de serviços baseados em IA. Essas não são questões fáceis de responder, e provavelmente levará algum tempo e uma análise cuidadosa para desenvolver abordagens políticas apropriadas. A IA oferece um enorme potencial para avanços nos campos médico, científico e até criativo, e as proteções para serviços baseados em IA podem ser adequadas. No entanto, alguns serviços de IA podem criar riscos significativos para a sociedade, e podem justificar uma consideração regulatória.

Como em todos os outros tipos de formulação de políticas discutidos neste artigo, a Internet Society recomenda que intervenções políticas para lidar com a IA sejam cuidadosamente delimitadas e direcionadas. Sem essa cautela, regulamentos ou restrições excessivamente amplas sobre a IA podem impactar negativamente outros usos em funções intermediárias que facilitam a comunicação dos indivíduos na Internet.

70 Consulte o artigo de Dan Katcher, "The Evolution of AI Search: Past, Present, Future" (A evolução da pesquisa por IA: passado, presente, futuro), 12 de fevereiro de 2024, disponível em https://www.rocketfarmstudios.com/blog/the-evolution-of-ai-search-past-present-future/.

6 Conclusão

Este documento oferece um modelo para entender as funções intermediárias da Internet e desenvolver políticas relacionadas à responsabilidade por conteúdo online. Nosso objetivo é fornecer informações aos formuladores de políticas para que possam construir políticas que preservem o que a Internet Society acredita serem as características mais importantes da Internet: ser aberta, globalmente conectada, segura e confiável. A Internet é cada vez mais importante para a vida das pessoas e para a prosperidade econômica e social. À medida que os formuladores de políticas lidam com preocupações legítimas da sociedade sobre o conteúdo online, é fundamental que as políticas garantam que a Internet continue sendo um recurso positivo para comunicação global, educação e discurso.

A responsabilidade pelo conteúdo gerado por usuários é uma questão que cresceu à medida que a Internet cresceu, tornando-se um meio de comunicação essencial para as sociedades modernas. Construir abordagens políticas que forneçam proteção contra responsabilidades para muitos tipos diferentes de funções intermediárias que possibilitam a comunicação na Internet continua sendo necessário para uma Internet saudável. Ao mesmo tempo, há uma variedade de ferramentas políticas para abordar preocupações online sem prejudicar a participação individual na Internet.

Acreditamos que há cinco estratégias-chave que os formuladores de políticas devem seguir ao construir políticas focadas na Internet:

1. Delimitar cuidadosamente a formulação de políticas para atingir os objetivos. Utilizar o conjunto mais restrito possível de políticas para controlar diretamente e mitigar a preocupação.
2. Sempre que possível, usar ferramentas políticas existentes para abordar preocupações específicas. Leis de privacidade, antidiscriminação e proteção ao consumidor, entre outras, já oferecem formas de proteger os usuários e melhorar a responsabilidade online.
3. Manter, ou onde ainda não existirem, construir proteções de responsabilidade para as funções que possibilitam a comunicação na Internet. Isso é especialmente importante para aquelas funções que fazem a Internet funcionar, mas também para aquelas que interagem diretamente com a comunicação dos usuários, como

hospedar e exibir conteúdo. Sem essas proteções, a Internet não poderá continuar a ser um meio de comunicação.

4. Proteger as entidades que fornecem as funções de curadoria e moderação de conteúdo gerado por usuários contra responsabilidade. A escala da Internet exige curadoria e moderação. Com transparência apropriada, uma entidade que hospeda conteúdo gerado por usuários deve ser capaz de aplicar curadoria e moderação automatizadas e manuais sem medo de atrair responsabilidade.
5. Trabalhar com as partes interessadas da Internet (incluindo a sociedade civil, as comunidades acadêmica e técnica, empresas e cidadãos) para realizar uma "Avaliação de Impacto da Internet" de qualquer política proposta, a fim de entender possíveis consequências ou efeitos não intencionais na Internet ou nos seus usuários.

A Internet Society se esforça para se envolver e trabalhar com governos em todo o mundo para ajudar a desenvolver políticas que abordem preocupações sociais, ao mesmo tempo em que apoiam a Internet. Trabalhamos para apoiar o desenvolvimento da Internet como uma infraestrutura técnica global, um recurso para enriquecer a vida das pessoas e uma força para o bem na sociedade. Acolhemos discussões sobre oportunidades, desafios e preocupações enfrentados pelos formuladores de políticas no ecossistema da Internet e maneiras de abordá-los.

Anexo A – Funções Intermediárias

Este anexo de "Uma Estrutura de Políticas para Intermediários da Internet" ("Estrutura de Políticas") descreve em detalhes o conjunto de funções intermediárias necessárias para a comunicação na Internet. Para cada uma dessas funções, fornecemos abordagens recomendadas de políticas.

Nosso foco principal é na proteção da responsabilidade dos intermediários. No entanto, conforme indicado na seção 4.3 da Estrutura de Políticas,[1] também existem outras abordagens políticas que podem ser aplicadas para tratar preocupações políticas relacionadas às funções dos intermediários, como as leis de privacidade e de proteção ao consumidor.

Para ajudar na organização dessas abordagens recomendadas de políticas, agrupamos as funções dos intermediários relacionadas em oito seções separadas (como estabelecido no sumário).

1 Seção 4.3 da Estrutura de Políticas: princípios legais e de políticas específicos que podem ser aplicados às funções de intermediários sem prejudicar as comunicações na Internet.

1 Transmissão de Pacotes de Dados

Esta seção descreve as funções intermediárias mais básicas e fundamentais envolvidas na transmissão de comunicações pela Internet — a transmissão de dados por fio ou sem fio.

- **A Seção 1.1** descreve a função de fornecer um meio de comunicação para comunicações pela Internet.
- **A Seção 1.2** descreve a função de fornecer um caminho de comunicação sobre um meio de comunicação.
- **A Seção 1.3** descreve a função de fornecer serviços de backbone ou tráfego que permitem aos provedores de acesso à Internet (também conhecidos como provedores de serviços de Internet) a capacidade de enviar e receber tráfego pela Internet.
- **A Seção 1.4** descreve a função de oferecer aos provedores de acesso à Internet a capacidade de trocar seu tráfego localmente, em vez de utilizar provedores de backbone ou tráfego.
- **A Seção 1.5** descreve a função de fornecer acesso à Internet a um endpoint (o dispositivo de um usuário).

1.1 Meios de Comunicações (Com Fio e Sem Fio)

Descrição da função: fornecer os meios de comunicação para suportar a transmissão de pacotes de rede do Protocolo de Internet (IP). Os meios de comunicação são utilizados em todas as partes da Internet, desde a conexão com uma residência ou dispositivo móvel, até provedores de rede "backbone" e cabos submarinos. Essa função intermediária é essencial para as comunicações mais básicas da Internet.

Considerações técnicas e práticas: pacotes IP podem ser transmitidos por "cabos", pelo ar e até pelo espaço, utilizando vários protocolos de rede específicos para o meio. Os meios de comunicação podem ser propriedade de, ou alugados para, um provedor de caminho de comunicação de Protocolo de Internet (veja a Seção 1.2) e podem transportar outros tipos de tráfego além de pacotes IP. Por exemplo, a capacidade de um cabo de fibra óptica submarino pode ser parcialmente

usada para tráfego IP e parcialmente para outros protocolos de transmissão de dados proprietários. Exemplos de meios de comunicação incluem: cabos submarinos, cobre, coaxial, fibra até a residência, comunicações sem fio em espectro de rádio licenciado ou não licenciado.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de meios de comunicação não devem ser responsabilizados pelo conteúdo que passa por seus meios.	Sem proteções contra responsabilidade, os provedores de meios de comunicação poderiam temer serem responsabilizados pelo conteúdo que trafega em suas infraestruturas. Isso os levaria a restringir o acesso aos seus meios apenas a conteúdo de um número limitado de fontes previamente avaliadas cuidadosamente. Tal restrição reduziria significativamente as fontes e os tipos de conteúdo transmitidos pelos meios de comunicação e prejudicaria a capacidade de indivíduos de participarem online. Isso também fragmentaria a Internet em diferentes redes de conteúdo.

1.2 Caminho de Comunicação do Protocolo de Internet

Descrição da função: envio e recebimento de pacotes de rede do Protocolo de Internet (IP) por meio de um sistema de comutação de pacotes de rede através de um ou mais meios de comunicação. Essa função inclui o acesso na "última milha" (discutido abaixo na seção 1.5). Na Internet, a comunicação de ponta a ponta é realizada por meio da travessia de caminhos de comunicação interconectados (movendo-se de uma rede para outra). Assim como os meios de comunicação (descritos acima), os caminhos de comunicação IP são utilizados em todas as partes da Internet. Uma rede IP entrega o tráfego IP sem que o cliente necessariamente saiba quais caminhos de comunicação serão ou estão

sendo usados. Essa função intermediária de fornecer o caminho de comunicação IP é essencial até mesmo para a comunicação mais básica na Internet.

Considerações técnicas e práticas: os principais caminhos de comunicação IP entre grandes redes de computadores estrategicamente interconectadas e roteadores centrais na Internet são coletivamente conhecidos como a espinha dorsal da Internet (descrita na seção 1.3 abaixo). Esses caminhos (também conhecidos como rotas) geralmente utilizam cabos de fibra óptica devido à sua grande largura de banda, velocidade e atenuação de sinal limitada. Redes que participam da espinha dorsal (backbone) da Internet frequentemente possuem acordos de "peering" sem custo com redes vizinhas para interconectar e transportar tráfego. Algumas redes, especialmente aquelas mais próximas do usuário final, podem precisar pagar pelo tráfego para que seu tráfego seja transportado até a Internet.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de caminhos de comunicação IP (serviços de rede IP) não devem ser responsabilizados pelo conteúdo que trafega em suas redes.	Sem proteções contra responsabilidade, os provedores de serviços de rede IP poderiam se preocupar em ser responsabilizados pelo conteúdo que passa por suas redes. Como resultado, eles poderiam restringir o acesso aos seus caminhos de comunicação a conteúdos de um pequeno número de fontes previamente avaliadas cuidadosamente. Em casos extremos, a falta de proteção contra responsabilidades poderia restringir o uso da Internet a conteúdos transmitidos por um pequeno número de empresas, impedindo que indivíduos compartilhem seus próprios conteúdos. Isso comprometeria gravemente a natureza aberta e globalmente conectada da Internet.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de caminhos de comunicação IP não devem ser obrigados a monitorar e interceptar o conteúdo do tráfego dos usuários.	Monitorar ou interceptar o conteúdo do tráfego em caminhos de comunicação IP (redes IP) provavelmente degradará severamente a velocidade e a confiabilidade das comunicações por esses caminhos. Isso também violará as expectativas dos usuários quanto à confidencialidade, segurança e privacidade. O "Internet Engineering Task Force" (Força Tarefa de Engenharia da Internet) considera o monitoramento generalizado[2] de redes IP um ataque, independentemente da motivação.

1.3 Redes de Backbone e Tráfego

Descrição da função: fornecimento de um tipo específico de caminho de comunicação IP conhecido como redes de backbone ou de tráfego. Essas redes interconectam e agregam tráfego de outras redes IP, como os provedores de acesso na última milha. Ao fazê-lo, elas permitem o fluxo de tráfego IP para conectar todas as outras partes da Internet. Essa função intermediária é essencial para as comunicações mais básicas da Internet.

Considerações técnicas e práticas: os provedores de serviços de backbone ou redes de tráfego estão tipicamente localizados em áreas geográficas onde a demanda é maior e onde é mais eficiente agregar tráfego. Essas redes são essenciais para transportar o tráfego da Internet de Provedores de origem e outros pontos finais até de destino e seus respectivos terminais.

2 "Pervasive Monitoring Is an Attack," Internet Engineering Task Force, Best Current Practice 188, RFC 7258, maio de 2024, disponível em https://datatracker.ietf.org/doc/html/rfc7258.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de redes de backbone ou de tráfego não devem ser responsabilizados pelo conteúdo que trafega em suas redes.	Sem proteções contra responsabilidade, esses provedores poderiam se preocupar em ser responsabilizados pelo conteúdo que passa por suas redes. Como resultado, poderiam restringir o acesso a um pequeno número de redes. Isso dificultaria a conectividade global e reduziria a capacidade dos indivíduos de se comunicarem online.
Os provedores de *backbone* e tráfego não devem ser obrigados a monitorar ou interceptar o conteúdo do tráfego dos usuários.	A função de fornecer serviços de redes de backbone ou de tráfego movimenta grandes volumes de tráfego na Internet de forma eficiente. A Internet não seria confiável ou segura se os provedores desses serviços monitorassem ou interceptassem o conteúdo do tráfego que transportam.

1.4 Troca de Tráfego

Descrição da função: fornecer um local físico em que várias redes IP e redes de entrega de conteúdo podem trocar pacotes. Essa função intermediária é crítica para uma Internet eficiente, robusta, confiável e segura. Com um ponto de troca de tráfego da Internet (IXP), os provedores de serviços de Internet podem trocar tráfego localmente, em vez de enviá-lo uns aos outros através de um provedor de backbone ou de tráfego.

Considerações técnicas e práticas: os IXPs são locais físicos e geralmente neutros onde diferentes redes locais se conectam para trocar tráfego entre si, bem como com provedores de backbone ou tráfego que participam do IXP, conforme necessário. Os IXPs criam rotas mais curtas, rápidas e diretas para o tráfego da Internet. Eles oferecem uma alternativa mais acessível e de menor latência em comparação ao roteamento de tráfego local por meio de redes internacionais. A troca de tráfego em IXPs reduz e otimiza o caminho de tráfego, diminuindo a latência e os custos.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os IXPs não devem ser responsabilizados pelo conteúdo que passa pela troca.	Sem proteções contra responsabilidade, é provável que ninguém esteja disposto a operar ou participar de um ponto de troca de tráfego da Internet. O tráfego seguiria caminhos ineficientes e mais lentos, os custos aumentariam, e a Internet se tornaria menos acessível, resiliente e sustentável.
Exceto para fins de gerenciamento eficaz do tráfego, as trocas devem ser desencorajadas de monitorar ou interceptar o conteúdo do tráfego que passa pela troca.	A função de fornecer um ponto de troca de tráfego da Internet geralmente é compartilhada por vários provedores de caminhos de comunicação IP ou provedores de serviços de rede IP. É crucial que as redes que utilizam um IXP confiem que o conteúdo de seu tráfego não está sendo monitorado ou interceptado. Caso contrário, elas podem relutar em usar a troca, pois seus clientes não querem que suas comunicações sejam monitoradas.
Os pontos de troca de tráfego da Internet não devem ser obrigados a interceptar, filtrar ou monitorar o tráfego que passa pela troca.	Exigir que os IXPs inspecionem ou analisem conteúdos específicos desencorajaria os de participar e prejudicaria a segurança das comunicações e a privacidade dos usuários. Tal abordagem minaria a confiança na Internet e dificultaria a troca eficiente de tráfego.

1.5 Acesso à Internet na Ultima Milha

Descrição da função: fornecer aos usuários finais (e seus dispositivos) acesso à Internet, comumente referido como “acesso na última milha”. Este é um tipo específico de caminho de comunicação IP (descrito

na seção 1.2 acima). Essa função, que inclui o transporte de tráfego IP proveniente do usuário final e para ele, é essencial para as comunicações mais básicas na Internet.

Considerações técnicas e práticas: o acesso à Internet pode ser fornecido aos usuários finais por meio de um ou mais métodos, incluindo DSL, cabo, sem fio, conexões móveis, fibra óptica e satélite. O acesso à Internet é frequentemente fornecido por um provedor comercial de serviços de Internet (ISP), mas alguns usuários finais acessam a Internet por meio de uma rede comunitária. Do ponto de vista técnico, o acesso de última milha não difere de outros caminhos de comunicação IP, mas é frequentemente tratado de maneira diferente em algumas jurisdições devido à regulamentação histórica de provedores de serviços de comunicação para usuários finais.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de acesso à Internet para usuários finais não devem ser responsabilizados pelo conteúdo que trafega em suas redes.	Sem proteções contra responsabilidade, esses provedores poderiam temer serem responsabilizados pelo conteúdo que seus clientes enviam e recebem. Como resultado, eles podem restringir o conteúdo que os usuários finais podem acessar ou transmitir na Internet. Podem tentar impor filtros de download e upload, o que comprometeria a segurança e a privacidade do uso da Internet por seus clientes. Além disso, para reduzir o risco de responsabilidade, os provedores provavelmente bloqueariam excessivamente conteúdos, impedindo que os usuários finais compartilhem conteúdos legais online. Sem essas proteções, a Internet aberta, globalmente conectada, segura e confiável seria prejudicada

Abordagens recomendadas de políticas	Motivos para essa abordagem
Exceto para fins de segurança e gerenciamento eficaz do tráfego, os provedores de acesso à Internet para usuários finais devem ser desencorajados de monitorar ou interceptar o conteúdo do tráfego dos usuários.	Um princípio fundamental do acesso à Internet (frequentemente descrito como "neutralidade da rede") é que os provedores de acesso à Internet devem oferecer acesso sem levar em consideração o conteúdo transportado em suas redes. Caso os provedores de acesso à Internet para usuários finais não sigam esse princípio e apliquem acessos diferentes dependendo do conteúdo, isso violaria uma propriedade essencial da Internet, que é ser uma rede de propósito geral (conforme descrito na Internet Way of Networking, Defining the critical properties of the Internet[3]). Os usuários finais também podem restringir como se comunicam online, temendo que suas comunicações estejam sendo monitoradas.

3 Internet Society, "Internet Way of Networking, Defining the critical properties of the Internet," setembro de 2020, disponível em https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf.

2 Roteamento e Funções Auxiliares Que Facilitam as Comunicações na Internet

Esta seção descreve as diversas funções intermediárias envolvidas no endereçamento e roteamento, que são essenciais para uma Internet eficiente, robusta, confiável e segura.

2.1 Atribuição de Endereço IP

Descrição da função: atribuição de endereços IP exclusivos para redes e usuários. Essa função intermediária é essencial para as comunicações mais básicas na Internet, pois todo caminho de comunicação na Internet precisa de um ponto de partida, um destino e "saltos" intermediários, cada um identificado por um endereço IP exclusivo.

Considerações técnicas e práticas: endereços IPv4 e IPv6 (também conhecidos como recursos numéricos da Internet) são delegados pela Internet Assigned Numbers Authority (IANA) para os registros regionais da Internet (RIRs[4]) responsáveis pela atribuição justa em suas regiões. Dentro de uma região, os RIRs atribuem endereços IP para provedores de redes IP e organizações de usuários finais. Em alguns países, os RIRs também atribuem endereços IP para registros nacionais da Internet. A IANA e os RIRs são organizações sem fins lucrativos governadas por processos multissetoriais voltados para redes e usuários em todo o mundo. Os cinco RIRs incluem: AfriNIC[5] na África, o Asia Pacific Network Information

4 https://www.nro.net/about/rirs/.

5 https://www.afrinic.net/.

Centre (APNIC[6]), o American Registry for Internet Numbers (ARIN[7]), o Latin American and Caribbean Internet Addresses Registry (LACNIC[8]), e o RIPE Network Coordination Centre (RIPE NCC[9]).

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de atribuição de endereços IP não devem ser responsabilizados pelo conteúdo comunicado usando os endereços IP que atribuíram.	Sem proteções contra responsabilidade, os provedores de serviços de atribuição de endereços IP, preocupados com a possibilidade de serem responsabilizados pelo conteúdo comunicado usando os endereços IP que atribuíram, podem restringir significativamente para quem eles atribuem endereços IP e sob quais condições. Isso reduziria o tamanho da Internet e impediria muitos usuários de se comunicarem online.
Os serviços de atribuição de endereços IP não devem ser obrigados a controlar conteúdo ilegal ou indesejado na Internet.	Os endereços IP são frequentemente compartilhados por mais de um usuário final e podem ser reatribuídos a outros usuários no mesmo país ou em outro. Da mesma forma, endereços IP são muitas vezes compartilhados por mais de um host de conteúdo. A interferência na atribuição ou no uso de endereços IP para controlar conteúdo pode impedir diretamente os usuários de compartilharem conteúdos legais, bem como impedir hosts de conteúdo de disponibilizarem conteúdos legais na Internet.

6 https://www.apnic.net/.

7 https://www.arin.net/.

8 https://www.lacnic.net/.

9 https://www.ripe.net/.

2.2 Atribuição de Números de Sistemas Autônomos

Descrição da função: atribuir números exclusivos a um grupo de redes IP operado por um ou mais operadores de rede (provedores de caminhos de comunicação IP, descritos na seção 1.2 acima) que possuem uma política de roteamento externo única e claramente definida. Esse grupo de redes é chamado de Sistema Autônomo (AS), e o número exclusivo que o identifica é seu Número de Sistema Autônomo (ASN). Essa função é semelhante à função de atribuição de endereços IP (descrita acima). Trata-se de uma parte crítica do sistema de roteamento de tráfego da Internet, usada para ajudar a identificar quais caminhos de comunicação são utilizados para rotear o tráfego da Internet.

Considerações técnicas e práticas: os ASNs são delegados pela Internet Assigned Numbers Authority (IANA) para os registros regionais da Internet (RIRs) para atribuição em suas regiões. Os RIRs atribuem ASNs tanto para provedores de redes IP quanto para organizações de usuários finais. Veja a seção 2.1 acima, "Considerações técnicas e práticas", para obter mais informações sobre a IANA e os RIRs. Há muita diversidade nos ASNs. Alguns são muito complexos, compostos por várias redes e usuários independentes, enquanto outros são mais simples.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de atribuição de ASNs não devem ser responsabilizados pelo conteúdo comunicado usando os ASNs que atribuíram.	Sem proteções contra responsabilidade, os provedores de serviços de atribuição de ASNs podem estar dispostos a atribuir ASNs apenas para um número muito pequeno de grandes e estabelecidos provedores de serviços de rede, limitando o crescimento e a diversidade de redes na Internet. Isso provavelmente teria efeitos severos, negativos e imprevisíveis na Internet e no acesso à Internet.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os serviços de atribuição de ASNs não devem ser obrigados a controlar conteúdo ilegal ou indesejado na Internet.	Interferir na atribuição de um ASN pode impedir o roteamento confiável e eficiente do tráfego da Internet, pode impedir redes de participarem da Internet e corre o risco de impedir uma ampla gama de usuários de compartilhar e acessar conteúdos legais.

2.3 Registro e Gerenciamento de DNS

Descrição da função: facilitar o registro, a renovação e o gerenciamento de nomes de domínio para publicação no Sistema de Nomes de Domínio (DNS). Essa função intermediária é essencial para comunicações na Internet que envolvem o uso de nomes de domínio. Nomes de domínio são os endereços "legíveis por humanos" de redes, servidores, sites e outros terminais na Internet.

Considerações técnicas e práticas: os nomes de domínio são importantes porque permitem que os humanos naveguem na Internet sem precisar lembrar de endereços IP, como "192.0.2.1". O registro e o gerenciamento do DNS incluem o registro de nomes de domínio por meio de registradores credenciados, garantindo a integridade das zonas DNS e mantendo informações no serviço de diretório de dados de registro (RDDS, historicamente chamado WHOIS). Um gerenciamento eficaz inclui a conformidade com políticas, incluindo políticas de consenso definidas pela comunidade que trabalha por meio da "Internet Corporation for Assigned Names and Numbers" (ICANN) para "gTLDs" ("generic top-level domains") e políticas definidas por órgãos nacionais para "ccTLDs" ("country code top-level domains"), que são controlados por cada país.[10] Essa função é desempenhada por várias organizações que colaboram entre si. Isso inclui registros de DNS (que gerenciam os domínios de nível superior gTLD e ccTLD) e registradores (que lidam com o registro de nomes de domínio para indivíduos ou entidades, permitindo que utilizem o domínio na Internet).

10 Os países podem definir suas próprias políticas para ccTLDs. A operação de alguns ccTLDs foi delegada pelo país a uma entidade externa que aloca domínios em uma base comercial.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de registro e gerenciamento de DNS não devem ser responsabilizados pelo conteúdo comunicado usando nomes de domínio que eles registram ou gerenciam.	Não fornecer proteções contra responsabilidade para provedores de serviços de registro e gestão de DNS em relação ao conteúdo hospedado sob nomes de domínio específicos provavelmente teria um efeito prejudicial sobre a capacidade das pessoas de se expressarem online. Sem proteções contra responsabilidade, os provedores provavelmente restringiriam significativamente quem pode registrar nomes de domínio e como eles podem ser usados. Isso poderia até mesmo afastar concorrentes menores do mercado de DNS, reduzindo a concorrência e aumentando o custo de registro de nomes de domínio.
Os serviços de registro e gerenciamento de DNS não devem ser obrigados a controlar conteúdos ilegais ou indesejados na Internet.	Nomes de domínio são uma parte crítica de como as pessoas interagem com a Internet. Impor ao sistema de registro de DNS a responsabilidade de controlar conteúdo resultaria em limitações sobre quem pode registrar nomes de domínio e para qual propósito, reduzindo significativamente a capacidade das pessoas de usar a Internet.

2.4 Publicação de DNS

Descrição da função: disponibilizar os dados DNS registrados em servidores DNS autoritativos para que as informações estejam acessíveis para consultas DNS (discutidas na seção 2.5 abaixo) por qualquer pessoa na Internet. Essa função intermediária é essencial para comunicações na Internet que envolvem o uso de nomes de domínio. Ela também abrange

(a) a operação de "servidores raiz" que fornecem informações sobre como alcançar o servidor DNS autoritativo para cada domínio gTLD ou ccTLD de nível superior, e (b) o fornecimento de cópias das informações dos servidores DNS autoritativos para resiliência, confiabilidade e respostas mais eficientes às consultas DNS.

Considerações técnicas e práticas: o DNS é um sistema hierárquico. Para cada domínio de nível superior (como .com), existe um intermediário que publica as informações autoritativas sobre esse domínio em um servidor DNS conhecido como "servidor raiz."[11] Esses intermediários são frequentemente chamados de "operadores de servidores raiz". Eles geralmente são o registro DNS ao qual a ICANN delegou a função de gestão daquele domínio de nível superior. Praticamente toda comunicação na Internet depende do funcionamento adequado da função de publicação DNS para garantir que o tráfego seja direcionado ao local correto na Internet. A integridade e a confiabilidade do sistema de servidores DNS são cruciais para as operações da Internet. Cópias das informações DNS autoritativas são usadas para melhorar a eficiência e a velocidade do sistema DNS.

11 https://root-servers.org/.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de publicação DNS não devem ser responsabilizados pelo conteúdo comunicado por meio dos nomes de domínio que publicam.	A interrupção dos serviços de registro e gestão DNS prejudicaria diretamente as operações da Internet, dificultando a capacidade dos usuários de localizar os servidores onde conteúdos e outros recursos estão hospedados. Se os provedores de serviços de publicação DNS pudessem ser responsabilizados pelo conteúdo hospedado sob os nomes de domínio que publicam, poderiam deixar de fornecer a função de publicação DNS ou oferecê-la apenas a domínios previamente analisados cuidadosamente. Isso teria efeitos severos, negativos e imprevisíveis nas comunicações pela Internet.
Os serviços de publicação DNS não devem ser obrigados a controlar conteúdos ilegais ou indesejados na Internet.	O acesso confiável e rápido a dados DNS publicados confiáveis e verificados é essencial para operações eficientes da Internet. Impedir a publicação DNS ou determinar quais domínios podem ser publicados e em quais circunstâncias fragmentaria a Internet e a tornaria pouco confiável.

2.5 Consulta de DNS

Descrição da função: traduzir nomes de domínio para seus respectivos endereços numéricos IPv4 ou IPv6 (bem como algumas outras informações). Tipicamente, os usuários utilizam nomes de domínio para localizar websites e outros recursos na Internet que desejam acessar. Os nomes de domínio precisam ser convertidos para o endereço IP correto para permitir que redes, servidores e dispositivos de usuários finais se conectem entre si. Essa função é realizada por servidores especializados chamados servidores DNS recursivos, que obtêm suas informações DNS

de servidores DNS autoritativos (ver seção 2.4 acima). Eles armazenam o mapeamento entre nomes de domínio e endereços IP, e respondem às solicitações de consulta DNS retornando endereços IP (ou outras informações solicitadas).

Considerações técnicas e práticas: os servidores DNS recursivos estão localizados em diversas partes da Internet. Para acelerar o Sistema de Nomes de Domínio (DNS), a maioria dos computadores de usuários finais não se comunica diretamente com servidores DNS autoritativos. Em vez disso, eles solicitam informações DNS a servidores DNS recursivos. Alguns servidores recursivos estão disponíveis para o mundo inteiro (frequentemente chamados de "servidores DNS abertos"). Outros são operados por Provedores de Serviços de Internet (ISPs), operadores de rede e empresas privadas, destinados principalmente ao uso de seus usuários. Eventualmente, indivíduos operam seus próprios servidores recursivos para uso pessoal, que são operados por indivíduos em seus próprios computadores, geralmente para seu uso pessoal. Embora a função primária de consulta DNS seja a mesma, muitos usuários escolhem um provedor DNS específico por razões de segurança e privacidade.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de consulta DNS não devem ser responsabilizados pelo conteúdo comunicado por meio das respostas que eles fornecem a consultas DNS.	Sem proteções contra responsabilidades, os provedores de serviços de consulta DNS provavelmente limitariam a capacidade dos usuários de usar o sistema DNS para acessar conteúdo na Internet. O conteúdo seria inacessível sem o conhecimento do endereço IP específico do site ou outro recurso na Internet. Isso teria um impacto severo e negativo nas comunicações pela Internet.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os serviços de consulta DNS não devem ser obrigados a controlar conteúdos ilegais ou indesejados na Internet.	Bloquear o acesso a nomes de domínio por meio de serviços de consulta DNS (servidores DNS recursivos) cria riscos significativos de bloqueio excessivo de conteúdo, impedindo o acesso e fragmentando a Internet. Tentar exigir o filtro de conteúdo via servidores DNS recursivos compromete a integridade do DNS e o torna pouco confiável.

2.6 Serviços DNSSEC

Descrição da função: fornecer autenticação para registros de nomes de domínio armazenados em servidores DNS autoritativos. Essa função é realizada por meio da disponibilização de assinaturas criptográficas de chave pública para esses registros. O objetivo dessa função é proteger a integridade dos registros de nomes de domínio e fornecer um mecanismo para validar que o endereço IP (ou outras informações) retornado de uma consulta DNS é o que o operador do domínio pretendia fornecer. O DNSSEC é uma função intermediária crucial para garantir que não houve adulteração no registro do nome de domínio.

Considerações técnicas e práticas: o DNSSEC, um protocolo de segurança desenvolvido pela Internet Engineering Task Force (IETF), ajuda a prevenir uma série de ataques cibernéticos às comunicações pela Internet. Sem o DNSSEC, um invasor poderia, por exemplo, corromper dados DNS em trânsito, alterando o endereço IP correspondente ao site que o usuário deseja acessar, redirecionando-o para o site do invasor. Quando implementado corretamente, o DNSSEC protege todos os registros DNS relacionados a um nome de domínio. Esses registros podem ser usados para localizar serviços, como mensagens instantâneas e e-mails, além de oferecer suporte a medidas antispam que dependem de DNS.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços DNSSEC não devem ser responsabilizados pelo conteúdo comunicado usando domínios protegidos pelo DNSSEC.	O DNSSEC protege a integridade dos resultados DNS, independentemente do conteúdo subjacente. Sem proteções contra responsabilidade, os provedores de serviços DNSSEC poderiam reduzir diretamente o uso do DNSSEC. Isso teria o efeito de reduzir significativamente a segurança das comunicações na Internet.

2.7 Serviços de Certificados TLS

Descrição da função: criar, armazenar e emitir certificados de Transport Layer Security (TLS) assinados criptograficamente para estabelecer conexões seguras com um servidor na Internet. Os certificados TLS geralmente são emitidos por uma Autoridade Certificadora (Certificate Authority - "CA"). Um uso comum dos certificados TLS é a proteção do tráfego web para evitar interceptação e adulteração. A emissão de certificados TLS é uma função intermediária essencial para garantir uma Internet confiável e segura.

Considerações técnicas e práticas: um certificado TLS é assinado digitalmente e emitido por uma CA, contendo informações como o nome do domínio, a entidade (pessoa, organização ou dispositivo) para a qual foi emitido, o nome da CA emissora e seu período de validade. Os certificados TLS protegem a integridade e a autenticidade das chaves públicas criptográficas utilizadas para estabelecer sessões HTTP criptografadas (HTTPS), assegurando o tráfego web contra interceptação e adulteração. O TLS é uma ferramenta essencial para manter as comunicações na Web seguras.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Entidades que fornecem certificados TLS não devem ser responsabilizadas pelo conteúdo protegido por esses certificados TLS.	O TLS tem como objetivo proteger o tráfego na Internet, independentemente de seu conteúdo. Impor responsabilidade sobre o conteúdo aos provedores de certificados TLS comprometeria a segurança das comunicações na Internet. Se as entidades que fornecem certificados TLS pudessem ser responsabilizadas pelo conteúdo transmitido usando seus certificados, elas poderiam relutar em emitir certificados TLS, especialmente para indivíduos e pequenas entidades, tornando a Internet menos segura para todos os usuários.

3 Serviços de Hospedagem e Armazenamento em Cache

Os dois primeiros grupos de funções (descritos nas seções acima) viabilizam as comunicações pela Internet. Esta terceira seção descreve funções que permitem que conteúdos sejam disponibilizados na Internet, incluindo conteúdos gerados por usuários, criados por indivíduos e pequenas entidades.

3.1 Hospedagem na Web

Descrição da função: fornecer e operar servidores e outros recursos necessários para hospedar sites, recursos e aplicativos da web, tornando-os acessíveis pela Internet. Essa função intermediária permite que indivíduos e outras partes compartilhem conteúdo com usuários através da World Wide Web.

Considerações técnicas e práticas: hospedar um site envolve a operação de servidores que (a) armazenam os arquivos, bancos de dados, software e códigos de um site ou aplicativo web e (b) recebem e respondem a solicitações de usuários para acessar o conteúdo do site. Entidades que oferecem hospedagem também podem fornecer outros serviços relacionados, como suporte técnico, soluções de backup e segurança. Muitos indivíduos, empresas, organizações sem fins lucrativos e governos dependem de serviços de hospedagem terceirizados em vez de atuarem como seus próprios hosts. Esses serviços de hospedagem geralmente oferecem hospedagem de sites mais segura, econômica e confiável.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de hospedagem de sites não devem ser responsabilizados pelo conteúdo de seus clientes diretos ou pelo conteúdo disponibilizado pelos usuários dos sites de seus clientes.	Caso os provedores de serviços de hospedagem pudessem ser responsabilizados pelo conteúdo nos sites de seus clientes, eles poderiam relutar ou se tornar incapazes de oferecer serviços de hospedagem, especialmente para indivíduos e pequenas organizações. Sem proteções contra responsabilidade, os provedores poderiam restringir severamente quem pode publicar conteúdo online e quais conteúdos podem ser publicados, limitando significativamente a capacidade de comunicação de indivíduos na Internet.
Provedores de serviços de hospedagem de sites não devem ser obrigados a inspecionar ou remover conteúdos colocados por seus clientes.	Obrigar os provedores a inspecionar e remover conteúdos prejudicaria sua capacidade de operar como hosts de sites, especialmente os menores. Eles poderiam restringir seus serviços a conteúdos pré-aprovados de um pequeno número de sites, e os usuários teriam opções limitadas para disponibilizar seus conteúdos na Internet.
Os provedores de serviços de hospedagem de sites não devem ser obrigados a controlar conteúdos ilegais ou indesejados.	A responsabilidade por conteúdos problemáticos deve recair sobre a pessoa ou entidade que publicou o conteúdo, e não sobre o provedor de serviços que hospeda o conteúdo.

3.2 Hospedagem de e-mail

Descrição da função: fornecer e operar servidores de e-mail para enviar, receber, armazenar, encaminhar e gerenciar serviços de e-mail na Internet. Essa função intermediária é essencial para o e-mail, uma ferramenta fundamental de comunicação pela Internet.

Considerações técnicas e práticas: a hospedagem de e-mail envolve a operação de servidores que enviam, recebem, armazenam, encaminham e gerenciam e-mails. Provedores de hospedagem de e-mail também podem oferecer serviços relacionados, como suporte técnico, arquivamento, filtragem de spam e suporte a conformidade. A maioria dos usuários da Internet, sejam pessoas físicas ou organizações, agora depende de hospedagem de e-mail terceirizada. Em geral, provedores terceirizados podem oferecer serviços de e-mail mais seguros, econômicos e confiáveis do que muitos indivíduos e empresas poderiam prover por conta própria.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de e-mail não devem ser responsabilizados pelo conteúdo dos e-mails enviados ou recebidos por seus usuários.	Se as entidades que fornecem serviços de e-mail pudessem ser responsabilizadas pelo conteúdo dos e-mails enviados ou recebidos por seus clientes, os provedores poderiam relutar ou se tornar incapazes de oferecer esses serviços, especialmente para indivíduos e pequenas entidades. Sem proteções contra responsabilidade, os provedores de serviços de e-mail poderiam ser forçados a monitorar e censurar mensagens de e-mail. Como resultado, o e-mail deixaria de ser uma ferramenta útil para comunicações entre pessoas.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores não devem ser obrigados a remover conteúdo ou bloquear a capacidade dos usuários de utilizarem seus serviços.	A responsabilidade por conteúdos problemáticos deve recair sobre a pessoa ou entidade que transmitiu o conteúdo, e não sobre o provedor de hospedagem de e-mail ou outros provedores que facilitam a transmissão de e-mails. Impor esse ônus ao provedor de hospedagem prejudicaria a capacidade de pequenos provedores de operar no mercado, além de comprometer a confiança, a integridade e a confiabilidade do e-mail.

3.3 Outros Serviços de Hospedagem

Descrição da função: fornecer e operar servidores que hospedam conteúdos, arquivos, bancos de dados, softwares e códigos, além de outros recursos que permitem a operação de uma ampla gama de aplicativos, sites e serviços para enviar e receber comunicações pela Internet. Como a grande maioria dos aplicativos e ofertas na Internet, especialmente aqueles oferecidos por startups e pequenas ou médias empresas, utiliza serviços de hospedagem, essa função intermediária é essencial para a disponibilidade de um conjunto diversificado de serviços e aplicativos na Internet.

Considerações técnicas e práticas: a hospedagem envolve a operação de servidores que (a) armazenam conteúdos, arquivos, bancos de dados, softwares e códigos que compõem um serviço ou aplicativo online e (b) permitem que os usuários interajam com o serviço ou aplicativo. Os provedores dessa função de hospedagem também podem oferecer outros serviços relacionados, como suporte técnico, soluções de backup, segurança e acesso à Internet. Muitos usuários dependem de serviços de hospedagem terceirizados porque esses provedores geralmente oferecem hospedagem mais segura, econômica e confiável do que muitos indivíduos e empresas poderiam fornecer por conta própria.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de hospedagem não devem ser responsabilizados pelo conteúdo de seus clientes ou dos usuários dos clientes.	Caso os provedores de serviços de hospedagem pudessem ser responsabilizados pelo conteúdo enviado ou recebido pelos clientes ou pelos usuários dos clientes, os provedores poderiam relutar ou se tornar incapazes de oferecer essa função, especialmente para indivíduos e pequenas entidades. Sem proteções contra responsabilidade, a inovação na Internet diminuiria e a hospedagem de conteúdos seria limitada a um pequeno número de grandes provedores.
Os provedores de serviços de hospedagem não devem ser usados para controlar conteúdos ilegais ou indesejados na Internet.	A responsabilidade por conteúdos problemáticos deve recair sobre a pessoa ou entidade que transmitiu os conteúdos, e não sobre o provedor que os hospeda. Impor esse ônus ao provedor de hospedagem prejudicaria a capacidade de pequenos provedores de operar no mercado, e os usuários teriam opções mais limitadas para disponibilizar seus conteúdos online.

3.4 Serviços de Armazenamento em Cache e de Entrega de Conteúdo

Descrição da função: armazenar temporariamente cópias de conteúdos mais perto do usuário final para reduzir a latência e os custos de conteúdos frequentemente acessados. Os serviços de armazenamento em cache são um tipo especial de hospedagem, geralmente envolvendo o armazenamento temporário de cópias de outros conteúdos mais próximos do usuário final. As redes de entrega de conteúdo (CDNs) utilizam data centers e redes geograficamente distribuídas para entregar

o conteúdo de seus clientes de forma mais rápida aos usuários finais. Normalmente, os clientes são grandes distribuidores de conteúdo, como serviços de streaming. Esses serviços de armazenamento em cache e entrega de conteúdo são cruciais para o funcionamento eficiente da Internet.

Considerações técnicas e práticas: algumas funções de cache são fornecidas por navegadores (discutidas abaixo), mas, na Internet, a principal função de cache é geralmente oferecida por uma CDN, que opera uma rede de servidores distribuídos. A função de armazenamento em cache também pode ser oferecida por provedores de serviços de Internet (ISPs) para acelerar o acesso ao conteúdo para seus clientes. Em ambos os casos, os servidores de cache armazenam cópias temporárias de conteúdos populares, como páginas da web, vídeos ou imagens. Como esses servidores estão distribuídos em diferentes redes pela Internet, as cópias do conteúdo desejado estão mais próximas dos usuários e podem ser acessadas mais rapidamente. Isso reduz a distância que o conteúdo precisa percorrer, diminuindo o tempo de carregamento e a latência, além de melhorar a experiência do usuário. O armazenamento em cache também reduz os custos de distribuição de conteúdo, evitando a retransmissão repetida do mesmo conteúdo. As decisões sobre o que armazenar em cache e por quanto tempo são geralmente automatizadas com base em algoritmos específicos.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de armazenamento em cache e entrega de conteúdo não devem ser responsabilizados pelo conteúdo armazenado em cache.	Se as entidades que fornecem serviços de armazenamento em cache ou entrega de conteúdo pudessem ser responsabilizadas pelo conteúdo armazenado temporariamente em seus servidores, os provedores de serviços poderiam relutar ou se tornar incapazes de oferecer esses serviços, o que aumentaria os custos, reduziria diretamente a eficiência e afetaria negativamente a experiência do usuário.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de armazenamento em cache não devem ser usados como pontos de controle para conteúdos ilegais ou indesejados na Internet.	Se os provedores de serviços de armazenamento em cache fossem obrigados a controlar conteúdos, eles só armazenariam em cache conteúdos conhecidos e analisados cuidadosamente. Isso aumentaria os custos para pequenos provedores de conteúdo e os tornaria menos atraentes para os usuários da Internet devido à qualidade reduzida da experiência do usuário. Os usuários perderiam o acesso a uma rica diversidade de conteúdos, com conteúdos locais, provavelmente, sendo os mais prejudicados.

3.5 Entrega de Conteúdo via API (Interface de Programação de Aplicações)

Descrição da função: hospedar e fornecer conteúdo por meio de uma API (Interface de Programação de Aplicações), que é um conjunto de regras ou protocolos que permitem que servidores de computador comuniquem informações de uma máquina para outra. As APIs são ferramentas muito comuns usadas em uma ampla gama de contextos para enviar e receber informações pela Internet e, em alguns desses contextos, são usadas para transmitir conteúdo gerado por usuários. Em um caso de uso comum, por exemplo, as APIs podem permitir a exibição de publicações em blogs ou redes sociais incorporadas em outras páginas da web.

Considerações técnicas e práticas: essa função é muito semelhante à hospedagem geral de conteúdo baseado na web discutida anteriormente, mas, às vezes, utiliza diferentes protocolos ou capacidades técnicas para solicitar e enviar o conteúdo.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de API não devem ser responsabilizados pelo conteúdo de usuários entregue por meio de seus serviços.	Caso as entidades que fornecem serviços de API pudessem ser responsabilizadas pelo conteúdo de usuários transmitido por seus serviços, elas poderiam relutar ou se tornar incapazes de oferecer esses serviços, reduzindo, assim, a capacidade das pessoas de publicar e receber conteúdo legal na Internet.
Os serviços de API não devem ser usados como mecanismos para controlar conteúdo ilegal ou indesejado na Internet.	As APIs são ferramentas fundamentais em todo o ecossistema da Internet, e qualquer tentativa de usá-las como meio de controle de conteúdo online corre o risco de isolar conteúdos dentro de serviços, reduzindo significativamente a interoperabilidade e a inovação.

3.6 Curadoria, Moderação e Exibição de Conteúdo

Descrição da função: organizar e, em alguns casos, selecionar conteúdo para exibição aos usuários. Isso se distingue da hospedagem na web, descrita acima na seção 3.1, pelas funções adicionais fornecidas, como curadoria ou moderação. Essas funções são muito comuns em sites de conteúdo gerado por usuários. Elas podem ser realizadas de forma automatizada, utilizando algoritmos e automação, e, em alguns casos, de forma manual por indivíduos.

Considerações técnicas e práticas: a função de curadoria é, geralmente, realizada por hospedeiros de conteúdo gerado por usuários, que precisam gerenciar e organizar um grande volume de submissões. Existem várias razões para oferecer essa função. Por exemplo, os hosts podem filtrar conteúdo que viole seus termos de serviço. Além disso, eles provavelmente apresentarão o conteúdo aos usuários com base em seus interesses e preferências, histórico de visualização ou outros critérios.

Essas funções possibilitam o gerenciamento prático de conteúdo em sites de conteúdo gerado por usuários. Decisões de curadoria e moderação tendem a ser mais relevantes para os usuários e mais bem compreendidas por eles quando levam em conta fatores culturais, linguísticos e contextuais.

Abordagens recomendadas de políticas	Motivos para essa abordagem
As organizações que realizam as funções de curadoria, moderação e exibição de conteúdo para usuários devem poder fazê-lo sem risco de responsabilidade pelo conteúdo.	Caso as entidades que oferecem essas funções pudessem ser responsabilizadas pelo conteúdo ou por essas atividades, elas poderiam relutar ou se tornar incapazes de fornecê-las. Sem curadoria e moderação, o conteúdo gerado por usuários ficaria desordenado e desorganizado. Isso dificultaria para os usuários compartilhar conteúdo com suas audiências e localizar o conteúdo que desejam.
A capacidade de realizar curadoria e moderação não deve ser restringida.	Sem essas funções — essenciais para bloquear spam e conteúdo irrelevante e para oferecer conteúdos de interesse aos usuários — os sites de hospedagem de conteúdo provavelmente se tornariam não administráveis para os operadores e pouco atrativos para os visitantes.

4 Comunicações De e Para Pessoas

Esta seção inclui um quarto grupo de funções que se concentram em diferentes modos de comunicação que permitem que as pessoas se envolvam em comunicações de pessoa para pessoa pela Internet. Essas funções são essenciais para que indivíduos, pequenas organizações e empresas interajam pela Internet.

Alguns aspectos dessas funções se sobrepõem a outras funções intermediárias descritas neste Anexo. No entanto, é importante descrevê-las de forma independente, pois elas são funções fundamentais que surgem repetidamente em novos serviços oferecidos pela Internet. Por exemplo, aplicativos de mensagens são uma inovação relativamente recente que combinam funções de comunicação de um para um e de um para muitos.

4.1 Comunicações de Um para Um

Descrição da função: fornecer um meio confiável para enviar, receber, exibir, rotear e dar suporte a comunicações discretas — em tempo real (de forma síncrona) ou para entrega posterior (de forma assíncrona) — entre um remetente e um destinatário. Essa função pode, em alguns casos, ser combinada com uma função de "descoberta" para procurar outros usuários de um serviço específico (por exemplo, pelo nome ou número de telefone) e permitir que os usuários se conectem com outros usuários.

Considerações técnicas e práticas: essa função define uma ampla capacidade para pessoas (e organizações) se comunicarem entre si. Ela está presente em uma vasta gama de serviços, incluindo o que, frequentemente, é chamado de e-mail, mensagens de texto, chat, mensagens diretas e outras ferramentas. Pode incluir comunicações de pessoa para pessoa em diversos ambientes, como sites baseados na web, videoconferências, jogos, redes sociais e outros contextos. Alguns ambientes também podem permitir que um indivíduo direcione o mesmo conteúdo para mais de um destinatário ao mesmo tempo (o que se

sobrepõe à função de um para muitos discutida na seção 4.2). Alguns desses serviços oferecem segurança e privacidade aprimoradas como característica distintiva, baseando-se em criptografia de ponta a ponta (E2EE), descentralização ou outras tecnologias.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de comunicação de um para um não devem ser responsabilizados pelo conteúdo enviado ou recebido por seus usuários.	Se as entidades que fornecem serviços de comunicação de um para um pudessem ser responsabilizadas pelo conteúdo das comunicações de seus usuários, elas poderiam relutar ou ser incapazes de oferecer esses serviços, especialmente para indivíduos e pequenas entidades. Sem proteções contra responsabilidade, os provedores podem ser forçados a interromper a oferta do serviço ou a censurar excessivamente as mensagens — incluindo discursos legais — para evitar responsabilidades. O resultado seria uma redução na capacidade das pessoas de se comunicarem online.
Os provedores de serviços de comunicação de um para um não devem ser responsáveis por lidar com conteúdos problemáticos enviados ou recebidos por clientes.	A responsabilidade pelo conteúdo problemático deve recair sobre a pessoa ou entidade que transmitiu o conteúdo, e não sobre o provedor do serviço que hospeda ou entrega o conteúdo. Impor encargos de revisão proativa de conteúdo aos provedores de comunicações de um para um pode levar os provedores (especialmente os menores) a sair do mercado, reduzindo a capacidade dos usuários de se comunicarem diretamente. Além disso, essa exigência pode levar à remoção de proteções críticas de privacidade e segurança, como a criptografia de ponta a ponta.

4.2 Comunicações de Um Para Muitos

Descrição da função: fornecer um meio confiável para enviar, receber, exibir, encaminhar e, de outras formas, suportar comunicações discretas — em tempo real (de maneira síncrona) ou para entrega posterior (de maneira assíncrona) — de um remetente para um grupo definido de destinatários (que pode ou não ser definido ou controlado pelo remetente). Os destinatários podem ou não ter a capacidade de responder e engajar-se em uma conversa dentro do grupo maior.

Considerações técnicas e práticas: essa função define uma ampla capacidade para pessoas (e organizações) se comunicarem com grupos de destinatários. A função está presente em uma variedade de serviços, que vão desde as antigas listas de distribuição de e-mail até os serviços mais modernos de webinars em vídeo. Alguns desses serviços podem oferecer segurança e privacidade aprimoradas como diferencial, como criptografia de ponta a ponta (E2EE) ou descentralização. Geralmente, os participantes de comunicações de um para muitos têm opções para sair ou "cancelar a assinatura" do grupo, ou bloquear comunicações de remetentes específicos.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de comunicações de um para muitos não devem ser responsabilizados pelo conteúdo enviado ou recebido por seus usuários.	Se as entidades que fornecem serviços de comunicações de um para muitos pudessem ser responsabilizadas pelo conteúdo das comunicações de seus usuários, elas poderiam se mostrar relutantes ou incapazes de continuar oferecendo tais serviços. Sem proteções contra responsabilidade, os provedores poderiam ser forçados a cessar a prestação do serviço ou a censurar excessivamente as mensagens — incluindo discursos legais — para evitar responsabilidades. O resultado seria uma redução na capacidade das pessoas de se comunicarem online.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de comunicações de um para muitos não devem ser responsáveis por abordar conteúdos problemáticos enviados ou recebidos por clientes por meio de revisão e filtragem de conteúdo.	A responsabilidade pelo conteúdo problemático deve recair sobre a pessoa ou entidade que transmitiu o conteúdo, e não sobre o provedor do serviço que hospeda ou entrega o conteúdo. Caso os provedores sejam obrigados a monitorar proativamente o fórum para identificar conteúdos indesejados, esse ônus provavelmente reduziria a capacidade dos provedores (especialmente os menores) de hospedar tais fóruns. Os provedores devem ser protegidos caso optem por remover ou bloquear um usuário que viole os termos de serviço ou as normas do grupo.

4.3 Comunicações de Muitos Para Muitos

Descrição da função: fornecer um meio confiável de enviar, receber, exibir, encaminhar e, de outra forma, apoiar as comunicações — em tempo real (de maneira síncrona) ou para entrega posterior (de maneira assíncrona) — de remetentes/criadores de conteúdo para todos os usuários de um serviço ou para outro grupo amplo de destinatários não controlados pelo remetente. Os destinatários ou visualizadores podem ou não ter a capacidade de responder e participar da conversa dentro do grupo maior.

Considerações técnicas e práticas: esta função define uma capacidade ampla para pessoas (e organizações) se comunicarem com o público ou outros grandes grupos de pessoas (como todos os usuários de um serviço específico). A função faz parte de uma ampla gama de serviços, incluindo, entre outros, sites colaborativos de "wiki", sites colaborativos de desenvolvimento de conteúdo/software, sites de compartilhamento de imagens/vídeos pré-gravados, serviços de transmissão de vídeo ao vivo e redes sociais. Alguns desses serviços podem oferecer aos usuários a capacidade de limitar a distribuição de suas publicações ou conteúdo para

um grupo definido de pessoas (sobrepondo-se assim à função de um para muitos descrita no item 4.2 acima). Alguns provedores de comunicações de muitos para muitos oferecem aos usuários a capacidade de bloquear comunicações de remetentes específicos ou de cancelar sua inscrição do grupo.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de comunicação de muitos para muitos não devem ser responsabilizados pelo conteúdo enviado ou recebido por seus usuários.	Se as entidades que fornecem serviços de comunicação de muitos para muitos pudessem ser responsabilizadas pelo conteúdo das comunicações de seus usuários, elas seriam relutantes ou incapazes de fornecer os serviços. Sem proteções contra responsabilidade, elas poderiam ser forçadas a parar de oferecer o serviço ou a censurar excessivamente mensagens, incluindo discursos legais, para evitar responsabilidades. O resultado seria uma redução na capacidade das pessoas de se comunicarem online.
Os provedores de serviços de comunicação de muitos para muitos não devem ser responsáveis por lidar com conteúdo problemático enviado ou recebido por clientes por meio de monitoramento e filtragem de conteúdo.	A responsabilidade pelo conteúdo problemático deve recair sobre a pessoa ou entidade que transmitiu o conteúdo, e não sobre o provedor do serviço que hospeda ou entrega o conteúdo. Se os provedores forem obrigados a monitorar proativamente o fórum em busca de conteúdo indesejado, esse ônus provavelmente reduziria a capacidade deles (especialmente os menores) de hospedar comunicações de muitos para muitos. Os provedores devem ser protegidos de responsabilidade caso escolham remover ou bloquear um usuário que viole os termos de serviço ou as normas do grupo.

5 Pesquisa

Esta seção abrange um quinto grupo de funções que inclui os métodos principais usados pelas pessoas para localizar conteúdo na Internet. As funções de pesquisa são utilizadas tanto porque as pessoas querem acessar novas informações ou conteúdos quanto porque desejam revisitar conteúdos previamente visualizados.

Muitas ferramentas e técnicas de pesquisa exibem uma parte do conteúdo do recurso sugerido em resposta a um termo de pesquisa.[12] Portanto, a função de busca não inclui apenas localizar conteúdo, mas também a exibição de conteúdo gerado por usuários. As funções de pesquisa são essenciais para permitir que os usuários descubram e acessem conteúdo na Internet.

5.1 Pesquisa na Web

Descrição da função: responder a solicitações de pesquisa com meios para conectar o pesquisador ao conteúdo e, frequentemente, exibir uma parte do conteúdo. A pesquisa é mais comumente realizada por "motores de busca", que são serviços de terceiros permitindo que os usuários pesquisem recursos relevantes na World Wide Web fornecendo palavras-chave, uma pergunta e carregando ou vinculando a uma imagem.

Considerações técnicas e práticas: fornecer esta função de busca geralmente envolve (a) indexar o conteúdo na Internet usando algoritmos que avaliam e registram informações como relevância de palavras-chave, tipo de conteúdo, atualidade do conteúdo, engajamento do usuário e qualidade da página e (b) identificar, fornecer um link de acesso e exibir os resultados sugeridos (frequentemente com "trechos" do conteúdo) em resposta a uma consulta de pesquisa do usuário, utilizando algoritmos que avaliam fatores como localização do usuário, idioma do usuário, histórico de pesquisa anterior e tipo de dispositivo.

12 Embora algumas ferramentas de busca agora forneçam resumos de conteúdo gerados por IA em resposta a consultas de pesquisa. Para uma discussão sobre essas questões, consulte a Seção 5.9 da Estrutura de Políticas: Inteligência Artificial.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de pesquisa não devem ser responsabilizados pelo conteúdo da Internet criado por terceiros que é exibido aos usuários em resposta a consultas.	Se os motores de busca fossem responsáveis pelo conteúdo gerado por usuários, provavelmente parariam de indexar a maior parte do conteúdo na Web. Isso teria como resultado prático deixar vastas áreas da Internet efetivamente inacessíveis para usuários ao redor do mundo.
Os provedores de serviços de pesquisa não devem ser responsáveis por lidar com conteúdo problemático exibido nos resultados de pesquisa.	A pesquisa é uma função intermediária vital que possibilita a comunicação na Internet, pois facilita o acesso dos usuários ao *conteúdo criado por terceiros*, ajudando-os a encontrar e localizar conteúdo "relevante" na Web. Sem a pesquisa, os usuários precisariam saber antecipadamente o URL ou endereço IP de cada site ou outro recurso online que desejam acessar, o que é impossível em escala na Internet.

5.2 Pesquisa Integrada

Descrição da função: fornecer resultados de pesquisa específicos de sites incorporados como um serviço para sites e outros que não possuem os recursos técnicos ou meios financeiros para desenvolver suas próprias ferramentas de pesquisa específicas do site.

Considerações técnicas e práticas: ao terceirizar uma função de pesquisa interna para um motor de busca de terceiros, um site pode oferecer pesquisas diretamente em seu próprio site para os usuários. Essa função é frequentemente, mas não exclusivamente, oferecida por motores de busca que, por sua vez, fornecem pesquisas focadas na web (como discutido acima). Os resultados de pesquisa podem ser adaptados para atender às necessidades do site específico que usa a busca incorporada.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de pesquisa integrada não devem ser responsabilizados pelo conteúdo da Internet que é gerido pelo site subjacente que utiliza o serviço para uma funcionalidade de pesquisa integrada.	Se os provedores de pesquisa integrada fossem responsáveis pelo conteúdo exibido nos resultados de pesquisa, provavelmente, eles deixariam de oferecer esse serviço, especialmente para sites menores e empresas ou organizações menos estabelecidas, o que impactaria diretamente a experiência do usuário na Internet, pois os sites não teriam boas funções de pesquisa.
Os provedores de serviços de pesquisa integrada não devem ser responsáveis por lidar com conteúdo problemático exibido nos resultados de pesquisa integrada.	Se os provedores de motores de pesquisa integrada fossem obrigados a monitorar o conteúdo do site, o serviço provavelmente se tornaria muito caro para sites menores e empresas ou organizações menos estabelecidas. Isso dificultaria diretamente a capacidade de pequenos sites de competir com sites maiores.

5.3 Pesquisa Específica

Descrição da função: fornecer resultados de pesquisa focados em mídias ou tópicos específicos (como, por exemplo, serviços de áudio reverso ou ferramentas de busca para podcasts ou imagens) provenientes de sites operados por terceiros, diferentes do provedor de pesquisa. Essa função aumenta a capacidade dos usuários de localizar conteúdos de interesse na Internet, especialmente aqueles que não são facilmente encontrados por meio de motores de busca gerais.

Considerações técnicas e práticas: as ferramentas de pesquisa geral, frequentemente, são muito amplas e, por isso, uma variedade de ferramentas de pesquisa mais focadas surgiu para permitir que os usuários da Internet pesquisem tipos específicos de conteúdo de forma mais eficaz e eficiente. Os resultados de pesquisa podem ser adaptados aos tipos de mídia ou conteúdo desejados.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de pesquisa específicos não devem ser responsabilizados pelo conteúdo da Internet criado por terceiros que é exibido aos usuários em resposta a consultas de pesquisa.	Caso as empresas de pesquisa específicas fossem responsabilizadas pelo conteúdo exibido em seus resultados, provavelmente, elas não poderiam continuar operando, o que resultaria na perda de ferramentas vitais para os usuários da Internet e essenciais para a descoberta de conteúdos valiosos online.
Os provedores de serviços de pesquisa específicos também não devem ser responsáveis por lidar com conteúdos problemáticos exibidos nos resultados de pesquisa.	Assim como a pesquisa na web é uma ferramenta central que permitiu que a Internet se tornasse uma enorme fonte de informação, as ferramentas de pesquisa específicas oferecem o mesmo valor para tipos de conteúdo menos abrangidos por motores de busca gerais. Impor encargos a esses provedores, provavelmente, levaria alguns a eliminar ou restringir esse tipo de ferramenta de pesquisa valiosa.

5.4 Pesquisa Fornecida Pelo Site

Descrição da função: oferecer pesquisa de conteúdo dentro de um site. Alguns grandes serviços online (especialmente aqueles que hospedam um grande volume de conteúdo gerado por usuários, como serviços de mídias sociais) disponibilizam suas próprias ferramentas de pesquisa interna, adaptadas ao serviço, para permitir que os usuários localizem conteúdos em seus sites.

Considerações técnicas e práticas: disponibilizar ferramentas para que os usuários localizem conteúdo é uma função básica de sites que suportam conteúdo gerado por usuários. Os resultados de pesquisa podem ser personalizados de acordo com os tipos específicos de conteúdo suportados pelo site e/ou pelas preferências individuais do usuário.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os operadores de sites que oferecem suas próprias ferramentas de pesquisa para localizar conteúdo no site não devem ser responsabilizados por conteúdo criado por terceiros, apenas por disponibilizarem uma ferramenta de pesquisa interna para facilitar a localização desse conteúdo.	Caso esses sites não pudessem fornecer ferramentas de pesquisa internas, os usuários seriam privados de meios eficientes para localizar conteúdo localmente.

6 Proteção de Segurança Cibernética, Proteção de Privacidade e Controles de Conteúdo do Usuário

Esta seção abrange um sexto grupo de funções que:

- (a) buscam combater ataques cibernéticos na Internet, essenciais para uma Internet segura, robusta, confiável e eficiente,
- (b) permitem que usuários individuais tomem medidas para proteger a segurança e privacidade de suas próprias comunicações na Internet, e
- (c) possibilitam que os usuários exerçam controle sobre as categorias de conteúdo que podem receber.

Observação: algumas leis de proteção contra responsabilidade de intermediários estendem explicitamente suas proteções a softwares e serviços que permitem aos usuários controlar o conteúdo que recebem pela Internet. Por exemplo, os provedores de softwares de filtragem controlados por usuários, voltados para famílias, podem ser protegidos contra ações judiciais movidas por sites bloqueados pelo software. *Consulte, por exemplo,* o Código Estatutário dos EUA, 47 U.S.C. §§ 230(f)(2) e (4).

6.1 Proteção de Tráfego em Escala de Rede

Descrição da função: proteger redes, serviços online, sites e outros recursos da Internet contra uma ampla gama de tráfego malicioso, incluindo ataques de negação de serviço distribuído (DDoS) e outras ameaças cibernéticas. Essa função faz parte de um esforço colaborativo geral de segurança cibernética[13] para proteger as comunicações na Internet.

Considerações técnicas e práticas: as proteções em escala de rede envolvem o uso de técnicas diversas e em constante evolução (como bancos de dados de assinaturas, detecção de anomalias e inteligência artificial) e infraestruturas dedicadas para defender contra ataques cibernéticos e mitigar o impacto do tráfego malicioso na disponibilidade, acessibilidade ou confiabilidade de redes, serviços online, sites e outros recursos da Internet. Algumas dessas técnicas exigem que as comunicações passem por uma rede operada por um provedor de serviços de segurança cibernética antes de alcançar a rede de destino. Assim, em algumas situações, as redes dos provedores de serviços de segurança cibernética carregam "conteúdo gerado por usuários" e outros tipos de conteúdo "criados por terceiros" na Internet.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de proteção de tráfego em escala de rede não devem ser responsabilizados pelo conteúdo que passa por suas redes.	Sem proteções contra responsabilidades, os provedores poderiam se preocupar com a possibilidade de serem responsabilizados pelo conteúdo que trafega por suas redes ou que examinam para fins de segurança. Isso poderia levá-los a retirar ou restringir a proteção de redes ou outros recursos na Internet, aumentando significativamente o risco de ataques cibernéticos prejudiciais na Internet.

13 Internet Society, "Collaborative Security: An approach to tackling Internet Security issues," abril de 2015, disponível em https://www.internetsociety.org/wp-content/uploads/2015/04/Collaborative-Security.pdf.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de proteção de tráfego em escala de rede não devem ser responsáveis por lidar com conteúdos problemáticos enviados ou recebidos pelas redes, serviços online, sites e outros recursos da Internet que protegem.	A proteção de tráfego em escala de rede é um processo altamente dinâmico e iterativo para responder a ataques cibernéticos em constante evolução. Impor encargos adicionais e não relacionados, como tentar bloquear certos tipos de conteúdo, prejudicaria a eficácia do esforço mais amplo de proteção cibernética. Isso também poderia incentivar os provedores a exigir que seus clientes permitam a descriptografia do tráfego enquanto ele passa por seus sistemas. Isso prejudicaria a confidencialidade, integridade e segurança das comunicações dos usuários da Internet. Qualquer esforço para escanear conteúdos específicos exigiria a tentativa de reconstruir, no meio da rede, todos os pacotes de dados separados que compõem o item de conteúdo (para poder determinar qual conteúdo está sendo transmitido), o que seria extremamente difícil para um provedor de serviços realizar de forma consistente.

6.2 Filtros e Ferramentas de Conteúdo Controlados Pelos Usuários

Descrição da função: fornecer aos usuários ferramentas para bloquear ou limitar determinados tipos de conteúdo de serem entregues aos seus dispositivos. Há uma variedade de ferramentas disponíveis. Por exemplo, as ferramentas de filtragem de conteúdo controladas pelos usuários podem ser utilizadas para reduzir o recebimento de e-mails de spam, bloquear a entrega de códigos maliciosos por um site ou evitar que conteúdos indesejados da web, como pornografia, sejam visualizados por uma residência ou dispositivo do usuário.

Considerações técnicas e práticas: os filtros e as ferramentas controlados pelos usuários oferecem proteções importantes (como contra spam e malware em páginas da web) e opções de proteção familiar (como contra pornografia ou outros tipos de conteúdo). Essas ferramentas utilizam diversos métodos técnicos e nem sempre são totalmente eficazes, mas ainda assim podem ser muito úteis. Às vezes, elas são oferecidas como um serviço adicional por provedores de Internet, mas também são comumente disponibilizadas como softwares para instalação nos computadores e dispositivos dos usuários. A legislação de proteção contra responsabilidade de intermediários dos EUA, a Seção 230, reconhecendo o valor dessas ferramentas para permitir que os usuários decidam quais conteúdos bloquear, inclui especificamente proteções para entidades que fornecem essas ferramentas. Consulte, por exemplo, o Código Estatutário dos EUA 47 §§ 230(f)(2) e (4).

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de filtros e ferramentas controlados pelos usuários não devem ser responsabilizados pelo conteúdo que passa por suas ferramentas, nem por bloquearem determinados conteúdos.	Sem proteções contra responsabilidade, os provedores, provavelmente, não conseguiriam operar, privando os usuários da Internet de proteções importantes contra cibersegurança, spam e ferramentas de filtragem de conteúdo.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de filtros e ferramentas controlados pelos usuários não devem ser responsáveis por lidar com conteúdos problemáticos enviados ou recebidos por seus usuários.	O objetivo dessas ferramentas é capacitar os *usuários* a decidir quais conteúdos desejam acessar e quais preferem bloquear. Uma exigência para que os provedores *bloqueiem* previamente conteúdos problemáticos complicaria o funcionamento das ferramentas (e, em muitos casos, poderia nem ser viável). Tal exigência comprometeria a autonomia dos usuários para controlar os conteúdos que recebem e geraria preocupações de que suas comunicações na Internet estão sendo monitoradas. Como resultado, é provável que os usuários evitem utilizar essas ferramentas para proteger suas interações online, levando a uma redução geral na cibersegurança da Internet.

6.3 Proteção de Tráfego Focada Nos Usuários

Descrição da função: permitir que usuários individuais protejam seu tráfego na Internet contra ataques cibernéticos, monitoramento (por entidades privadas e governos) e censura.

Considerações técnicas e práticas: as proteções de tráfego voltadas para o usuário são aquelas aplicadas a critério do próprio usuário para direcionar seu tráfego na Internet por caminhos e protocolos de rede confiáveis. Essas proteções também podem ajudar os usuários a ocultar sua identidade ou localização, aumentando assim sua privacidade e segurança. Esses serviços de proteção de tráfego utilizam diversos métodos técnicos, incluindo redes privadas virtuais (VPNs), serviços de roteamento em camadas (mais conhecida como a rede Tor) e outras abordagens. Na maioria dos casos, os provedores desses serviços não conseguem, e muitas vezes não podem, determinar quais conteúdos trafegam em suas redes.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de proteção de tráfego voltada para o usuário não devem ser responsabilizados pelo conteúdo que passa por suas redes.	Sem proteções contra responsabilidade, os provedores, provavelmente, não conseguiriam operar, privando os usuários da Internet de uma importante ferramenta de segurança cibernética que os protege contra ataques cibernéticos, roubo de identidade, monitoramento e censura.
Os provedores de proteção de tráfego voltada para o usuário não devem ser responsáveis por lidar com conteúdos problemáticos enviados ou recebidos por seus usuários.	Inspecionar e, possivelmente, bloquear tráfego específico seria diretamente contrário à finalidade dos serviços oferecidos por esses provedores. Isso comprometeria a eficácia desses serviços, reduzindo a privacidade e aumentando os riscos de segurança para os usuários.

7 Aplicativos, Software e Seu Desenvolvimento e Distribuição

O sétimo grupo de funções intermediárias inclui os aplicativos, programas e bibliotecas de software mais comuns utilizados no envio, recebimento e exibição de comunicações pela Internet. Esta seção também aborda as funções intermediárias relacionadas à distribuição de aplicativos e softwares. Os aplicativos e softwares discutidos nesta seção podem incluir funcionalidades que não estão relacionadas diretamente às comunicações na Internet.

Devido ao papel abrangente do software em facilitar, exibir, proteger e filtrar conteúdos na Internet, algumas leis de proteção contra responsabilidade de intermediários incluem especificamente, dentro de suas proteções, os criadores e distribuidores de software utilizado em comunicações pela Internet. *Consulte, por exemplo,* o Código Estatutário dos EUA, 47 U.S.C. §§ 230(f)(2) e (4).

As funções mencionadas nesta seção (como o desenvolvimento de softwares para web e e-mail) estão intimamente ligadas às funções discutidas nas Seções 3 e 4 acima (incluindo, por exemplo, hospedagem de sites e comunicações de um a um). No entanto, esta seção se concentra no desenvolvimento e na distribuição do software subjacente utilizado para oferecer os serviços abordados anteriormente, o que pode justificar proteções para intermediários de forma independente da prestação dos serviços.

7.1 Software de Sistema Operacional

Descrição da função: fornecer software para dispositivos que permite (1) que o dispositivo se conecte à Internet e envie ou receba comunicações pela Internet, (2) que os usuários do dispositivo insiram conteúdo para transmissão na Internet, e (3) que os usuários do dispositivo recebam

e visualizem conteúdos transmitidos pela Internet. Essas funções estão entre muitas outras atividades e funções desempenhadas por um sistema operacional em um dispositivo.

Considerações técnicas e práticas: o sistema operacional de um dispositivo desempenha funções essenciais que permitem a transmissão, o recebimento e a exibição de comunicações de e para a Internet. Praticamente todos os dispositivos de computação possuem um sistema operacional subjacente, desde dispositivos de consumo, como computadores, telefones móveis e TVs, até roteadores, comutadores, servidores e outros dispositivos que são fundamentais para o funcionamento da Internet.

Abordagens recomendadas de políticas	Motivos para essa abordagem
As entidades que fornecem sistemas operacionais não devem ser responsabilizadas pelo conteúdo da Internet transmitido, recebido ou exibido por meio do sistema operacional.	Os sistemas operacionais são essenciais para as comunicações na Internet e para o funcionamento da própria Internet. Impor responsabilidade pelo conteúdo da Internet criado ou transmitido por usuários ou terceiros aos provedores de sistemas operacionais limitaria severamente, se não eliminaria, a capacidade dos usuários de se comunicarem pela Internet.
Os sistemas operacionais não devem ser obrigados a bloquear ou interferir de outra forma em conteúdos problemáticos na Internet.	A segurança, estabilidade, confiabilidade e integridade dos sistemas operacionais são cruciais para o acesso à Internet e para toda a computação de maneira geral. Exigências que os sistemas operacionais monitorem ou bloqueiem o acesso a conteúdos comprometeria a velocidade, segurança e confiabilidade de suas funções.

7.2 Software de Navegação e de Servidor Web

Descrição da função: fornecer software para solicitar, enviar, receber e exibir conteúdo usando protocolos da World Wide Web. Essas ações são realizadas por dois tipos amplos de software: o software de "servidor" web (que recebe e responde às solicitações de clientes web para conteúdo online) e o software de "cliente", mais comumente os navegadores da web, que permite aos usuários solicitar, receber e visualizar uma ampla variedade de conteúdos da web. Essa função intermediária também inclui os "apps" — softwares executados em smartphones, computadores e outros dispositivos — que recuperam conteúdo usando protocolos da World Wide Web. Uma enorme quantidade de conteúdo na Internet é entregue aos usuários por meio das funções dos softwares de servidor e cliente web, sendo um método essencial para acessar conteúdos online.

Considerações técnicas e práticas: a Web depende da interoperabilidade proporcionada pelos protocolos da World Wide Web, mais conhecidos como Linguagem de Marcação de Hipertexto (HTML), para formatação de conteúdo, e o Protocolo de Transferência de Hipertexto Seguro (HTTPS), para solicitar e entregar conteúdo de forma segura. Essa interoperabilidade oferece um dos benefícios fundamentais da Internet — permitir que qualquer pessoa crie, formate e vincule conteúdo que outras pessoas, em qualquer lugar do mundo, possam acessar. Muitos sites incorporam conteúdos de várias fontes (por exemplo, um vídeo incorporado de um serviço de streaming ou uma foto de um serviço de compartilhamento de imagens que aparece no meio de uma página da web). Os navegadores da web são uma ferramenta comum para acessar conteúdos na Internet, oferecendo aos usuários um conjunto abrangente de opções para controlar o conteúdo apresentado e, em certa medida, proteger sua privacidade e segurança.

Abordagens recomendadas de políticas	Motivos para essa abordagem
As entidades que fornecem software de cliente e servidor web não devem ser responsabilizadas pelo conteúdo transmitido, recebido ou exibido por meio do software.	Os programas de navegação na web e de serviço web são essenciais para permitir que indivíduos acessem conteúdo na Internet. Sem proteções contra responsabilidade, as entidades que fornecem essas funções intermediárias vitais estariam preocupadas com a possibilidade de serem responsabilizadas pelo conteúdo manipulado por seu software. Elas poderiam restringir o uso de suas ferramentas para limitar a responsabilidade, por exemplo, limitando o uso a recursos web que tenham sido inspecionados ou que tenham concordado em indenizá-las em caso de qualquer ação legal. Os sites e recursos da web modernos, geralmente, contêm conteúdo dinâmico que pode mudar com frequência e sem aviso prévio. Isso torna praticamente impossível para qualquer pessoa avaliar se o conteúdo que os usuários desejam enviar ou receber poderia gerar responsabilidade. O risco de responsabilidade provavelmente restringiria drasticamente o conteúdo disponível na web e prejudicaria a capacidade dos indivíduos de se comunicar online.

Abordagens recomendadas de políticas	Motivos para essa abordagem
O software de navegação na web não deve ser obrigado a bloquear ou, de outra forma, interferir no conteúdo problemático na Internet.	Exigir que o software de servidor ou cliente web monitore ou bloqueie o acesso ao conteúdo provavelmente prejudicaria a velocidade, segurança, confiança e confiabilidade da Internet. Por exemplo, se os navegadores filtrarem ou bloquearem conteúdos de maneiras que são incontroláveis e impossível de gerenciar pelo usuário, os usuários recorreriam a ferramentas alternativas para modificar ou substituir seu navegador (o que poderia expô-los a malware e roubo de identidade).
O software de navegação na web não deve ser obrigado a reduzir a segurança para permitir que terceiros examinem e bloqueiem conteúdo problemático na Internet.	Políticas foram propostas que exigem que os navegadores reduzam a segurança geral para permitir que terceiros examinem e bloqueiem o tráfego que, de outra forma, seria criptografado entre o navegador da web e o servidor web. Por exemplo, a exigência de instalar certificados raiz controlados[14] pelo governo permitiria esse tipo de bloqueio, mas também prejudicaria a segurança, a confiança e a confiabilidade da Internet.

7.3 Software de e-mail

Descrição da função: fornecer software para enviar, receber, armazenar e exibir e-mails. Essas ações são realizadas por dois tipos amplos de software: software de servidor de e-mail e software de cliente de e-mail. O software de servidor executa as funções de "back-end" de transmissão,

14 Internet Society, "Mauritius Must Not Fall into the 'Mass Surveillance' Trap," 28 de maio de 2021, disponível em https://www.internetsociety.org/blog/2021/05/mauritius-must-not-fall-into-the-mass-surveillance-trap/.

recebimento e armazenamento de e-mails, enquanto o software de cliente permite que os usuários enviem, recebam, encaminhem e visualizem e-mails. O e-mail é um mecanismo de comunicação amplamente utilizado, geralmente, baseado em um modelo assíncrono, federado e de armazenamento e encaminhamento, com servidores de e-mail ou sistemas independentes transmitindo e recebendo e-mails em nome dos remetentes e destinatários.

Considerações técnicas e práticas: a interoperabilidade de servidores e clientes de e-mail usando protocolos de e-mail globalmente aceitos significa que remetentes e destinatários podem trocar e-mails independentemente do software ou dos provedores de serviço de e-mail que utilizam. Tecnologias de criptografia, como S/MIME e PGP, estão disponíveis para garantir a segurança do e-mail de ponta a ponta para usuários que escolhem criptografar seus e-mails.

Abordagens recomendadas de políticas	Motivos para essa abordagem
As entidades que fornecem software de cliente e servidor de e-mail não devem ser responsabilizadas pelo conteúdo transmitido, recebido ou exibido por meio do software.	O software de cliente e servidor de e-mail é uma ferramenta crítica para a comunicação na Internet. Sem proteções contra responsabilidade, os desenvolvedores de software, provavelmente, deixariam de fornecer e-mail para grandes grupos de usuários, limitando a capacidade dos usuários de se comunicarem por e-mail na Internet.
O software de e-mail não deve ser obrigado a bloquear ou, de outra forma, interferir em conteúdo problemático na Internet.	Exigir que o software de e-mail monitore ou bloqueie o acesso a conteúdo prejudicaria a segurança, a privacidade e a confiabilidade do e-mail. Isso também desestimularia os provedores de e-mail a oferecer aos seus clientes a capacidade de garantir suas comunicações de e-mail com criptografia de ponta a ponta.

7.4 Software de Mensagens

Descrição da função: fornecer software para uma ampla gama de ferramentas para enviar, receber, armazenar e exibir mensagens. Essas ações são realizadas por dois tipos amplos de software: software de "servidor" de mensagens (que executa funções de "back-end" de roteamento de mensagens e pode também receber, transmitir e armazenar mensagens) e software de "cliente" (que permite aos usuários enviar, receber e visualizar mensagens, e pode também armazená-las). Assim como o e-mail, as mensagens são um mecanismo de comunicação amplamente utilizado.

Considerações técnicas e práticas: existe uma ampla gama de sistemas de mensagens, e muitos deles não são interoperáveis entre si (e sua arquitetura interna de vários sistemas pode ser muito diferente). Alguns sistemas de mensagens são baseados em padrões da Internet amplamente desenvolvidos, enquanto outros desenvolveram tanto o software do cliente quanto o do servidor para suportar a comunicação. Alguns sistemas de mensagens suportam mensagens criptografadas de ponta a ponta, o que pode fornecer proteções críticas para manter as mensagens privadas e seguras.

Abordagens recomendadas de políticas	Motivos para essa abordagem
As entidades que fornecem software de mensagens, incluindo software de cliente e servidor, não devem ser responsabilizadas pelo conteúdo transmitido, recebido ou exibido por meio do software.	O software de mensagens é uma ferramenta crítica de comunicação na Internet, especialmente para comunicação segura e privada de ponta a ponta. Sem essas proteções, os provedores de software ficariam preocupados com a possibilidade de serem responsabilizados pelo conteúdo compartilhado por seus usuários. Como resultado, eles poderiam parar de fornecer essa função ou se sentir compelidos a enfraquecer a segurança e a privacidade das comunicações de seus usuários, desativando a criptografia de ponta a ponta ou inspecionando as comunicações dos usuários.
O software de mensagens não deve ser obrigado a bloquear ou, de outra forma, interferir com conteúdo problemático na Internet.	Exigir que o software de mensagens monitore ou bloqueie o acesso a conteúdo prejudicaria a velocidade, a segurança, a privacidade, a confiança e a confiabilidade das mensagens.

7.5 Outros Softwares Usados no Envio, Recebimento e Exibição de Comunicações da Internet

Descrição da função: fornecer um aplicativo ou programa com uma função secundária que oferece a capacidade de enviar, receber e exibir conteúdo e comunicações. Por exemplo, um aplicativo que fornece informações sobre trilhas de caminhada em uma área geográfica pode também permitir que os usuários publiquem comentários sobre as trilhas, que são enviados para outros usuários.

Considerações técnicas e práticas: existe uma grande diversidade de programas e aplicativos que permitem aos usuários publicar ou enviar conteúdo e receber conteúdo de terceiros.

Abordagens recomendadas de políticas	Motivos para essa abordagem
As entidades que fornecem aplicativos que permitem aos usuários publicar, transmitir ou receber conteúdo ou comunicações não devem ser responsabilizadas pelo conteúdo gerado pelo usuário que é transmitido, recebido ou exibido por meio do aplicativo.	Como um grande número de aplicativos permite que os usuários transmitam conteúdo e comunicações, regulamentações amplas poderiam facilmente englobar centenas ou até milhares de aplicativos, muitos de empresas iniciantes e pequenos provedores. Sem proteções contra responsabilidade pelo conteúdo gerado pelos usuários, os desenvolvedores e provedores de tais aplicativos, provavelmente, não ofereceriam a funcionalidade de comunicação adicional como parte de seus serviços, prejudicando a capacidade dos indivíduos de se comunicarem por meio desses aplicativos e limitando a inovação e o desenvolvimento de novos produtos na Internet. Isso também poderia levar alguns provedores, especialmente os menores, a saírem do mercado.
Os aplicativos não devem ser obrigados a bloquear ou, de outra forma, interferir com o conteúdo gerado pelo usuário na Internet.	xigir que entidades que fornecem funções de comunicação como parte de seus programas e softwares de aplicativo monitorem ou bloqueiem o acesso ao conteúdo gerado pelos usuários, provavelmente, limitaria as comunicações legítimas e prejudicaria a segurança, privacidade, confiança e confiabilidade da Internet.

7.6 Desenvolvimento e Distribuição de Software/Aplicativos

Descrição da função: desenvolver e facilitar a distribuição de software e aplicativos que suportam a comunicação de conteúdo pela Internet. Esta função inclui, por exemplo, aplicativos, softwares, bibliotecas de software e plug-ins de software que transmitem, recebem, exibem, encaminham, armazenam em cache, buscam, dividem em conjuntos, organizam, reorganizam, traduzem, filtram, verificam, permitem, impedem, selecionam, escolhem, analisam, digerem conteúdo ou, de outra forma, facilitam a comunicação de conteúdo pela Internet. Esta categoria de software e aplicativos, e sua distribuição, pode ser fornecida para usuários finais, provedores de infraestrutura da Internet ou outros participantes do ecossistema da Internet. Como poucas pessoas hoje têm o conhecimento técnico para criar seus próprios aplicativos cliente e servidor da Internet, a capacidade de localizar e recuperar software escrito por terceiros é uma função essencial para a operação da Internet.

Considerações técnicas e práticas: o desenvolvimento e a distribuição de ferramentas de software que permitem aos usuários acessar a Internet e se comunicar através dela são funções vitais. A função de desenvolvimento e distribuição assume uma ampla gama de formas, incluindo repositórios de software de código aberto (que fornecem alguns dos softwares mais fundamentais nos quais a Internet opera), espaços de desenvolvimento colaborativo de software (frequentemente usados para desenvolver software de código aberto), "lojas de aplicativos" disponíveis para usuários, "lojas" em navegadores e outros softwares para permitir que os usuários adicionem complementos de terceiros (por exemplo, para suportar o filtro de tráfego da web, atualização e correção de software instalado), e outras abordagens.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de desenvolvimento e distribuição de software não devem ser responsáveis pelo conteúdo que os usuários enviam e recebem utilizando o software desenvolvido ou distribuído.	Sem essas proteções contra responsabilidade, os provedores, provavelmente, não conseguiriam fornecer essas funções devido à preocupação com a responsabilidade potencial pelo conteúdo tratado pelo software desenvolvido ou distribuído. A responsabilidade ameaçaria a capacidade da Internet de continuar operando e seria particularmente prejudicial aos desenvolvedores de software de código aberto.[15]
Os desenvolvedores e provedores de software não devem ser obrigados a bloquear ou interferir de qualquer outra forma com conteúdo problemático gerado por usuários na Internet.	Mandatos desse tipo afetariam negativamente a conectividade global e o acesso dos indivíduos às ferramentas para comunicar conteúdo online. As contribuições para o software de código aberto provavelmente diminuiriam e o software crítico não seria mantido, levando a uma Internet muito menos segura e confiável.

15 Internet Society, "The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem," 24 de outubro de 2022, disponível em https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/.

8 Ambientes Complexos

Esta seção final discute sites e serviços que poderiam ser vistos como fornecendo uma única função distinta (como uma função de "mídia social") ou fornecendo uma combinação das funções discutidas nas seções anteriores para criar um ambiente mais enriquecido para a interação dos usuários. No fim das contas, a análise da política é muito semelhante, pois as entidades estão lidando com conteúdo criado por outras pessoas e, portanto, impor responsabilidade às entidades levanta preocupações significativas não apenas para esta categoria de funções, mas também para outras funções intermediárias críticas da Internet.

8.1 Mídias Sociais

Descrição da função: fornecer um ambiente de redes sociais que permita aos usuários se conectarem com outros usuários, bem como criar, compartilhar, trocar, receber e interagir com conteúdo criado por terceiros. A Seção 5.1 da Estrutura de Políticas[16] discute as mídias sociais com mais detalhes.

Considerações técnicas e práticas: sites de mídias sociais facilitam a comunicação, o networking e a descoberta de conteúdo entre os usuários, muitas vezes por meio de uma combinação de texto, imagens, vídeos e links. As funções adicionais realizadas pelos sites de mídias sociais incluem gerenciamento de contas de usuários, hospedagem e entrega de conteúdo, algoritmos para recomendação de conteúdo e personalização, e ferramentas para interação do usuário, como "curtidas", comentários e compartilhamentos. A função de fornecer um ambiente de redes sociais pode ser aplicada a uma ampla gama de sites, não apenas aos grandes e **conhecidos** serviços de mídias sociais. Por exemplo, muitos sites oferecem aos usuários a oportunidade de interagir entre si, trocar conteúdo e ideias, e desenvolver relacionamentos diretos com outros usuários. As funções de "mídias sociais" poderiam facilmente se aplicar a

16 Seção 5.1 da Estrutura de Políticas, Destaque: considerações de políticas para plataformas de "mídias sociais" que hospedam, curam e moderam conteúdo gerado pelos usuários.

serviços de mídias sociais pequenos e de público específico, e também a sites focados em comunidades de interesse específicas, como corredores de maratona, jardineiros, fãs de um time esportivo específico ou membros de um partido político ou clube.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de mídias sociais não devem ser responsabilizados pelo conteúdo criado, publicado, enviado ou recebido por seus usuários.	Se as entidades que fornecem serviços de mídias sociais pudessem ser responsabilizadas pelo conteúdo gerado pelos usuários (veja a seção 1.5 da Estrutura de Políticas[17] para uma discussão sobre conteúdo gerado por usuários), elas poderiam reduzir significativamente as oportunidades para os indivíduos participarem de discussões online, e poderiam censurar excessivamente a fala, incluindo a fala lícita, de seus usuários. Sem proteções contra responsabilidade, os provedores podem restringir severamente quem pode publicar conteúdo online, limitando significativamente a capacidade dos indivíduos de se comunicarem na Internet.
Os provedores de serviços de mídias sociais não devem ser responsáveis pelo conteúdo problemático criado, publicado, enviado ou recebido por seus usuários.	A responsabilidade por conteúdos problemáticos deve recair sobre a pessoa ou entidade que publicou o conteúdo, e não sobre o provedor de serviços que hospeda o conteúdo. Atribuir responsabilidade aos provedores prejudicaria a capacidade deles de hospedar grandes quantidades de conteúdo gerado por usuários.

17 Seção 1.5 da Estrutura de Políticas, comparando a responsabilidade pelo conteúdo gerado pelo site e pelo conteúdo gerado pelo usuário.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Quando as preocupações das políticas se concentram nas ações do provedor de serviços (e não no conteúdo das publicações dos usuários), as respostas das políticas não devem sobrecarregar a liberdade de expressão dos usuários.	Como mencionado na Seção 5.1 da Estrutura de Políticas, existe uma ampla gama de leis e políticas que podem ser aplicadas aos provedores de serviços de mídias sociais *sem* torná-los responsáveis pelo conteúdo criado ou comunicado por seus usuários.

8.2 Redes Federadas

Descrição da função: fornecer uma abordagem descentralizada para hospedagem de conteúdo gerado por usuários, compartilhamento, curadoria e moderação, incluindo, por exemplo, ambientes de redes sociais. Vários servidores independentes podem optar por participar de uma rede federada, permitindo que os usuários interajam entre si em toda a rede federada, enquanto cada servidor mantém o controle sobre seus próprios dados e comunidades. Por exemplo, em contraste com uma comunidade de mídias sociais controlada centralmente, um sistema de mídias sociais federado pode permitir que muitas comunidades independentes menores se conectem e compartilhem conteúdo em todo o ecossistema federado. Isso pode criar uma experiência de rede social semelhante, mas com uma abordagem mais local para a moderação. A Seção 5.2 da Estrutura de Políticas[18] discute as redes federadas em mais detalhes.

Considerações técnicas e práticas: as redes sociais federadas de servidores independentes, utilizando protocolos padronizados como o ActivityPub, se tornaram mais populares. Nesse tipo de rede, cada servidor independente define suas próprias regras e políticas, por exemplo, sobre moderação, privacidade de dados e outros tópicos, enquanto ainda participa de uma rede mais ampla. O sistema de e-mail global da Internet é outro exemplo de uma rede federada, pois uma grande quantidade de servidores de e-mail independentes troca e-mails entre si sem um arranjo prévio. O sistema de e-mail permite que cada entidade participante defina

18 Seção 5.2 da Estrutura de Políticas, Destaque: considerações de políticas para "redes federadas" que permitem novas abordagens para facilitar o engajamento dos usuários.

suas próprias políticas, por exemplo, sobre o gerenciamento de spam e limites de armazenamento de mensagens. Os provedores de serviços federados, muitos dos quais são pequenas empresas ou organizações, permitem que os usuários mantenham conexões amplas na Internet enquanto ainda podem escolher um provedor de serviços que ofereça políticas de privacidade, moderação e outros aspectos que atendam às suas preferências.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de conteúdo federados não devem ser responsabilizados pelo conteúdo criado, publicado, enviado ou recebido por seus usuários.	Se esses provedores pudessem ser responsabilizados pelo conteúdo gerado pelos usuários, eles poderiam não ser capazes, tecnicamente ou financeiramente, de continuar a oferecer esses serviços. As redes federadas, por sua natureza, atraem pequenas empresas e até indivíduos como provedores de serviços. Se essas entidades não puderem operar, os usuários da Internet perderiam ferramentas valiosas que oferecem opções alternativas às grandes empresas de mídias sociais e uma moderação de conteúdo mais granular.
Os provedores de serviços de conteúdo federados não devem ser responsáveis pelo conteúdo problemático criado, publicado, enviado ou recebido por seus usuários.	A responsabilidade pelo conteúdo problemático deve ser atribuída à pessoa ou entidade que publicou o conteúdo, e não ao provedor que hospeda o conteúdo. Colocar a responsabilidade no provedor federado prejudicaria o potencial positivo das redes federadas e restringiria consideravelmente sua disponibilidade.

8.3 Ambientes de Jogos

Descrição da função: facilitar a conexão de múltiplos jogadores para jogar videogames juntos em tempo real pela Internet, incluindo a facilitação de uma variedade de métodos para os jogadores interagirem e trocarem comunicações e conteúdo entre si. A Seção 5.3 da Estrutura de Políticas[19] discute os ambientes de jogos com mais detalhes.

Considerações técnicas e práticas: a maioria, senão todos, dos ambientes de jogos modernos estão, pelo menos parcialmente, conectados à Internet, e alguns são totalmente baseados na Internet. Os componentes comuns de comunicação nos ambientes de jogos incluem chat dentro do jogo e conexões diretas de voz e vídeo entre as pessoas. Os ecossistemas de jogos não são apenas espaços para os usuários participarem de jogos online com outros usuários ao redor do mundo, eles também fornecem um ambiente de mídia social.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de ambientes de jogos não devem ser responsáveis pelo conteúdo criado, publicado, enviado ou recebido pelos seus usuários.	Se os provedores puderem ser responsabilizados pelo conteúdo das comunicações de seus clientes, isso pode reduzir significativamente as oportunidades de interação entre os indivíduos, além de censurar excessivamente a fala, incluindo a fala lícita, que seus usuários desejam comunicar. Sem proteções contra responsabilidade, isso pode restringir severamente quem pode participar e qual conteúdo pode ser postado, alterando e limitando significativamente os ecossistemas de jogos.

19 Seção 5.3 da Estrutura de Políticas, Destaque: considerações de políticas para o ecossistema de jogos interativos online.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de ambientes de jogos não devem ser responsáveis pelo conteúdo criado, publicado, enviado ou recebido pelos seus usuários.	A responsabilidade por conteúdos problemáticos deve recair sobre a pessoa ou entidade que publicou o conteúdo, e não sobre o provedor de serviços que hospeda o conteúdo. Atribuir responsabilidade a um provedor de jogos, provavelmente, alteraria a dinâmica dos jogos e prejudicaria a viabilidade dos sistemas de jogos.

8.4 Ambientes de Realidade Virtual e Aumentada

Descrição da função: permitir que múltiplos usuários interajam e colaborem em um ambiente de realidade virtual (RV) ou realidade aumentada (RA) compartilhado. A Seção 5.4 da Estrutura de Políticas[20] discute os ambientes de RV e RA com mais detalhes.

Considerações técnicas e práticas: embora os ambientes de realidade virtual ou aumentada tenham emergido mais recentemente, sistemas de RA e RV estão, como os sistemas de jogos, se integrando cada vez mais à Internet. Muitos ambientes de RV e RA conectam-se diretamente à Internet, permitindo que os usuários interajam uns com os outros em tempo real. Em alguns casos, os ambientes de RV e RA podem gerar impactos diretos no mundo físico e em pessoas que não participam intencionalmente de um ambiente de realidade virtual ou aumentada.

20 Seção 5.4 da Estrutura de Políticas, Destaque: considerações de políticas para sistemas de realidade virtual e aumentada conectados à Internet.

Abordagens recomendadas de políticas	Motivos para essa abordagem
Os provedores de serviços de ambientes de realidade virtual ou aumentada não devem ser responsabilizados pelo conteúdo criado, publicado, enviado ou recebido por seus usuários.	Se os provedores de RV e RA pudessem ser responsabilizados pelo conteúdo das comunicações de seus usuários, é provável que eles reduzissem significativamente as oportunidades para que os indivíduos participem de debates online ou que censurassem excessivamente os discursos, incluindo aqueles lícitos, que seus usuários desejam comunicar. Sem proteções contra responsabilidade, os provedores podem restringir severamente quem pode colocar conteúdo online e qual conteúdo pode ser colocado, alterando e limitando significativamente o desenvolvimento contínuo das tecnologias e serviços de RV e RA.
Os provedores de ambientes de realidade virtual ou aumentada não devem ser responsáveis por conteúdos problemáticos criados, publicados, enviados ou recebidos por seus usuários.	A responsabilidade por conteúdos problemáticos deve recair sobre a pessoa ou entidade que publicou o conteúdo, e não sobre o provedor de serviços que hospeda o conteúdo. Atribuir responsabilidade aos provedores, provavelmente, teria impactos negativos no desenvolvimento das tecnologias de realidade virtual e aumentada.