Contribuição da ISOC-BR à Consulta Pública CGI.br:

Proposta de princípios para regulação de plataformas de redes sociais

Autora

Gabriela Paz

Revisão

Laura Pereira

Flávio Rech Wagner

Danielle Novaes

Camila Tsuzuki

Marina Quezia

Consulta Pública CGI.br: Proposta de princípios para regulação de plataformas de redes sociais

A ISOC Brasil parabeniza o Comitê Gestor da Internet no Brasil (CGI.br) pela iniciativa de submeter à consulta pública a proposta preliminar de princípios para orientar a futura regulação das plataformas de redes sociais. A abertura de um processo participativo e multissetorial reforça o compromisso histórico do CGI.br com o desenvolvimento de políticas públicas ancoradas em diálogo, legitimidade técnica e respeito aos fundamentos que estruturam a Internet, corroborando a Recomendação 3 desta ISOC Brasil, no seu Decálogo para o Modelo Brasileiro de Responsabilidade de Intermediários[1]. Além disso, saudamos o esforço em promover um processo contínuo de participação, dando sequência e encaminhamento à consulta anterior em 2024.

Reconhecendo a importância do tema e a oportunidade de qualificar o debate público, a ISOC Brasil apresenta esta contribuição com base em sua missão institucional de promoção de uma Internet aberta, segura, confiável, interoperável e globalmente conectada, oferecendo subsídios técnicos informados por evidências, experiências internacionais e princípios já consolidados no campo da governança da Internet.

1. Apresentação Institucional

A ISOC (Internet Society) é uma associação sem fins lucrativos, criada em 1992, com atuação internacional, que tem por objetivo promover liderança no desenvolvimento dos padrões da Internet, bem como fomentar iniciativas educacionais e políticas públicas ligadas à rede mundial de computadores. Para tanto, propicia a interação com governos, empresas e entidades em geral para adoção de políticas em relação à Internet que estejam de acordo com seus princípios: uma rede aberta, segura, confiável, interoperável e universalmente acessível, dando apoio à inovação, à criatividade e às oportunidades comerciais. A ISOC, por exemplo, oferece amparo financeiro e administrativo para o IETF (*Internet Engineering Task Force*), responsável pelo desenvolvimento e discussão das diretrizes de funcionamento e padrões da Internet. A instituição possui mais de 120 escritórios locais (capítulos), e mais de 100 mil membros individuais e organizacionais espalhados pelo mundo.

A ISOC Brasil é o capítulo brasileiro da Internet Society, contando com 1185 membros ativos, espalhados por todo o país. Os membros da ISOC Brasil provêm de diversas comunidades: comunidade técnica envolvida no desenvolvimento tecnológico da Internet e na sua operação; comunidade empresarial envolvida na infraestrutura e na operação da Internet (como provedores de acesso) e no desenvolvimento de conteúdos (como empresas de mídia e de aplicações); comunidades acadêmicas de diferentes áreas que desenvolvem pesquisas sobre o

[1] Disponível em: https://isoc.org.br/files/Dec%C3%A1logo_de_Recomenda%C3%A7%C3%B5es_sobre_o_Modelo_Brasileiro_de_Responsabilidade_de_Intermedi%C3%A1rios.pdf.

desenvolvimento e uso da Internet e seus impactos sociais e econômicos; e organizações da sociedade civil que se preocupam com os impactos sociais e econômicos do desenvolvimento e uso da Internet e tecnologias associadas. A ISOC Brasil é o veículo que traz para a sociedade brasileira a promoção e a discussão dos princípios defendidos pela Internet Society, assim como de suas ações e seus posicionamentos. Por sua vez, o Grupo de Trabalho de Responsabilidade de Intermediários (GT-RI) atua no Capítulo com foco em modelos de responsabilidade de provedores, incluindo regulação de plataformas digitais. O GT atua de forma técnica e propositiva, participando de consultas públicas, acompanhando legislações e defendendo modelos regulatórios que não prejudiquem a arquitetura e o funcionamento da Internet.

2. Princípios para a Regulação de Plataformas de Redes sociais:

2.1 Definições Importantes

Com base na sistematização da Consulta do CGI.br de regulação de plataformas digitais, realizada em 2023, e para fins desta contribuição, adotaram-se as seguintes definições[2]:

Plataformas digitais operam sobre uma infraestrutura tecnológica digital, que usa a tecnologia de Internet para conectar suas aplicações de interface e estruturá-las de forma específica e reprogramável, com o objetivo principal de intermediar a relação entre diversos atores — conectando, por exemplo, fornecedores de serviços e produtos a consumidores e usuários —, tendo como características marcantes o uso intensivo de dados e de tecnologias de Inteligência Artificial (IA) e efeitos de rede.

Redes sociais, por sua vez, são um tipo de serviço de plataformas digitais, que pode ser definido como: uma plataforma digital cuja principal finalidade seja a conexão entre usuários para estabelecer relações sociais diversas, que produzem conteúdos (como informações, opiniões, e ideias em formatos distintos como textos ou arquivos de imagens, sonoros ou audiovisuais). Em plataformas de redes sociais, a circulação desses conteúdos e a interação entre usuários é qualificada pela ação de mecanismos automatizados (algoritmos de aprendizagem de máquina e modelos avançados de Inteligência Artificial).

De acordo com a **Tipologia de Provedores de Aplicação elaborada pelo CGI.br**, Plataformas de Redes Sociais podem ser enquadradas como aquelas que possuem funcionalidades de alta interferência sobre a circulação de conteúdo gerados pelos seus usuários. Os sistemas de automatização organizam e distribuem os conteúdos por meio do emprego de técnicas de coleta e tratamento de dados para perfilização, difusão em massa,

[2] As definições de Plataformas digitais e Redes sociais foram propostas pelo CGI.br nesta Consulta, mas não estavam abertas à contribuições. A menção a elas tem a finalidade de contextualizar a contribuição e não deve ser entendida como uma concordância da ISOC-BR sobre os conceitos adotados.

recomendação algorítmica, microssegmentação, estratégias de incentivo ao engajamento contínuo, impulsionamento próprio ou pago, publicidade direcionada, dentre outras. Ainda que essa intermediação, por vezes, seja benéfica aos atores envolvidos, as atividades desses provedores oferecem riscos, considerando seus incentivos e a forma como são realizadas. Exemplos de funcionalidades que promovem alta interferência na circulação e na disponibilidade de conteúdos produzidos por terceiros são os sistemas de impulsionamento e recomendação de conteúdo baseados em perfilização, veiculação de anúncios, propaganda programática etc.

2.2 Proposta de Princípios

A partir desta conceituação, o CGI.br propõe 10 Princípios para a Regulação de Plataformas de Redes Sociais, objeto desta Consulta Pública.

A ISOC Brasil considera a iniciativa positiva e oportunamente estruturada, e entende que o debate sobre a formulação e aplicação desses princípios é essencial para a construção de um modelo regulatório que preserve a abertura, a segurança, a interoperabilidade e a confiabilidade da Internet. Nesse espírito, as contribuições a seguir buscam fortalecer e aprimorar o alinhamento dos princípios propostos com tais valores.

Estas contribuições estão organizadas em formato estruturado: para cada princípio, apresenta-se um comentário técnico que visa qualificar seu conteúdo, com base em evidências, boas práticas e princípios já consolidados no campo da governança da Internet. Quando aplicável, é incluída ao final de cada comentário uma proposta de redação, que traduz objetivamente as recomendações formuladas. Para facilitar a leitura, textos tachados indicam sugestões de exclusão ou substituição de trechos, e textos em vermelho correspondem às adições ou modificações sugeridas.

Princípio 1 – Soberania e segurança nacional

> *As atividades das plataformas devem respeitar a supremacia da Constituição Federal e o ordenamento jurídico do país, garantindo a prevalência do direito soberano do Estado brasileiro de adotar medidas e políticas para a proteção do Estado Democrático de Direito, da democracia, da segurança nacional, de seus cidadãos e a promoção da diversidade das expressões culturais em seu território.*

Comentários:

A referência à Constituição Federal e à proteção do Estado Democrático de Direito é um avanço relevante. No entanto, a formulação atual apresenta amplitude excessiva e ausência de salvaguardas técnicas e jurídicas que orientem a aplicação desse princípio.

Inicialmente, chama-se atenção para a ausência de especificação adequada do termo "plataformas", tal como empregado na redação. Considerando que esta consulta pública trata da regulação de plataformas de redes sociais, conforme definição expressa no próprio documento do CGI.br, recomenda-se que o princípio utilize a terminologia precisa, evitando interpretações extensivas que possam abranger serviços digitais de naturezas diversas.

Embora seja legítimo que o Estado brasileiro adote medidas para proteção da democracia, da segurança nacional e da diversidade cultural, um princípio estruturante como este deve oferecer bases e orientações mais precisas para a aplicação de uma futura legislação. Organismos Internacionais, como ONU e UNESCO, recomendam que regulações respeitem os direitos humanos, promovam a interoperabilidade da Internet e evitem medidas que levem à sua fragmentação, especialmente quando justificadas por interesses unilaterais[3]. Isso, pois, justificativas como "soberania nacional" ou "ordem pública" vêm sendo usadas, em diferentes contextos nacionais[4], para impor restrições incompatíveis com os direitos fundamentais, incluindo localização obrigatória de dados, filtragem de conteúdo e vigilância sem garantias adequadas.

Para além disso, observa-se um crescimento em legislações e decisões judiciais que buscam um efeito extraterritorial impositivo para suas determinações. Embora em algumas situações isso possa ser percebido como justificável, o crescimento dessa tendência é preocupante e exige que as disposições dos ordenamentos jurídicos estejam alinhados a orientações e tratados internacionais, incluindo as recomendações técnicas e padrões estabelecidos por órgãos como o (IETF) Internet Engineering Task Force.

A Internet Society alerta[5,6] que medidas regulatórias, quando não fundamentadas em critérios (inclusive técnicos) claros, tendem a comprometer características estruturais da Internet. Tais medidas interferem diretamente na forma como os dados circulam pela rede e podem gerar impactos negativos concretos, como:

- **Perda de eficiência no roteamento de dados**, com impacto na velocidade, estabilidade e desempenho dos serviços;
- **Redução da interoperabilidade** entre redes e sistemas, especialmente a nível global e regional, tornando a infraestrutura mais vulnerável e menos resiliente;
- **Obstáculos à inovação aberta**, dificultando a entrada de novos agentes e limitando o desenvolvimento de soluções descentralizadas;
- **Aumento de custos operacionais** para empresas e provedores de infraestrutura, devido à necessidade de duplicação de recursos e armazenamento redundante;

[3] Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000387339/PDF/387339eng.pdf.multi
[4] Disponível em: https://docs.un.org/en/A/HRC/38/35
[5] Disponível em: https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf
[6] Disponível em: https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-Use-Case-Data-Localization-EN.pdf

- **Riscos à segurança cibernética** e à integridade do fluxo global de informações, especialmente em contextos de redes segmentadas por critérios territoriais.

Essas preocupações, por sua vez, dialogam diretamente com a contribuição submetida pela ISOC Brasil à Pergunta 16 da Consulta sobre Regulação de Plataformas Digitais[7] promovida pelo CGI.br em 2023[8] , que buscava identificar os possíveis riscos relacionados à soberania digital e ao desenvolvimento tecnológico que não foram previamente mencionados. Na oportunidade, destacamos que uma definição ampla e imprecisa de "soberania digital" poderia levar precisamente a tais riscos regulatórios, comprometendo a estabilidade técnica e jurídica do ambiente digital brasileiro.

Nesse contexto, é essencial que qualquer referência à prevalência do direito soberano do Estado brasileiro venha acompanhada de salvaguardas normativas claras, como a referência expressa aos princípios da **legalidade**, da **proporcionalidade** e do **devido processo legal** para garantir que eventuais medidas regulatórias adotadas pelo Estado não se transformem em instrumentos de censura, restrição arbitrária de serviços ou discriminação de usuários. Tais salvaguardas estão consagradas na Constituição Federal, no Marco Civil da Internet (Lei 12.965/2014, arts. 7º e 9º) e em compromissos internacionais assumidos pelo Brasil.

Além disso, ressaltamos naquela consulta, e reforçamos agora, ser fundamental reconhecer que determinadas intervenções regulatórias, quando desconsideram a arquitetura distribuída e transfronteiriça da Internet, podem gerar impactos técnicos irreversíveis, comprometendo a resiliência e a escalabilidade da rede. Medidas como bloqueios indiscriminados de serviços, exigência de interconexão local obrigatória, ou regras que favoreçam infraestruturas fechadas e centralizadas, podem não apenas fragmentar a experiência dos usuários brasileiros, mas também afetar negativamente a conectividade com outras regiões do mundo, criando precedentes jurídicos e técnicos de difícil reversão.

Exemplos internacionais e nacionais evidenciam os riscos de fragmentação técnica e de governança que podem emergir de decisões regulatórias mal calibradas. Conforme alerta a Rede de Políticas sobre Fragmentação da Internet (PNIF)[9] do IGF, práticas como filtragem centralizada, exigência de contratos comerciais compulsórios entre redes e o uso do bloqueio de plataformas como instrumento de sanção jurídica impactam diretamente na interoperabilidade da rede e na liberdade de expressão. No caso brasileiro, os bloqueios do WhatsApp e do Telegram demonstram como decisões unilaterais, mesmo que motivadas por interesses legítimos, podem afetar milhões de usuários e causar efeitos colaterais extraterritoriais, prejudicando também países vizinhos pela natureza interligada da infraestrutura da Internet.

Assim, recomenda-se que este princípio incorpore, em sua redação, uma referência clara à necessidade de que todas as medidas de proteção à soberania e à segurança nacional sejam

[7] Disponível em: https://dialogos.cgi.br/documentos/debate/consulta-plataformas/
[8] Disponível em: https://isoc.org.br/files/Contribui%C3%A7%C3%A3o%20CGI%20-%20Final_compressed.pdf
[9] Disponível em: https://www.intgovforum.org/en/filedepot_download/256/26218

transparentes, pautadas por critérios técnicos que respeitem a arquitetura da rede, baseadas em padrões abertos e respaldadas por mecanismos institucionais que garantam o escrutínio democrático. Esse cuidado é essencial para evitar decisões de efeito irreversível que comprometam o caráter aberto, globalmente conectado, seguro e interoperável da Internet, bem como os direitos fundamentais dos cidadãos brasileiros.

Cabe destacar que o próprio CGI.br, no **Princípio 7** do presente Decálogo, reconhece a interoperabilidade, o uso de padrões abertos e a portabilidade de dados como fundamentos regulatórios essenciais para garantir a funcionalidade técnica e a liberdade dos usuários. Ao ancorar a regulação nesses princípios, o texto contribuirá para assegurar previsibilidade normativa, controle institucional e compatibilidade com o regime democrático de direitos.

Resumo da recomendação:

I. a substituição do termo "plataformas" por "plataformas de redes sociais", em consonância com o escopo da consulta pública; e
II. a inclusão expressa de critérios como legalidade, proporcionalidade e preservação das propriedades críticas e da arquitetura da Internet para garantir que eventuais medidas regulatórias não se transformem em instrumentos de censura, restrição arbitrária de serviços ou discriminação indevida de usuários.

Redação sugerida:

"As atividades das plataformas de redes sociais devem respeitar a supremacia da Constituição Federal e o ordenamento jurídico do país, garantindo a prevalência do direito soberano do Estado brasileiro de adotar medidas e políticas para a proteção do Estado Democrático de Direito, da democracia, da segurança nacional, de seus cidadãos e a promoção da diversidade das expressões culturais em seu território, observados os princípios da legalidade, da proporcionalidade, do devido processo legal e da preservação da Internet como uma infraestrutura aberta, interoperável, descentralizada, baseada em padrões técnicos globais e voltada para o interesse público."

Princípio 2 – Liberdade de expressão, privacidade e direitos humanos

> *A regulação deve assegurar a proteção da dignidade humana e dos direitos fundamentais, incluindo a liberdade de expressão, consideradas suas dimensões individual e coletiva, a privacidade, igualdade, o direito a não discriminação e a proteção absoluta aos direitos da criança e adolescente, buscando combater a incitação à violência, ao discurso de ódio e a todas as formas de discriminação nas plataformas.*

Comentários:

A formulação reconhece corretamente a centralidade dos direitos fundamentais no ambiente digital, com destaque para a liberdade de expressão, a privacidade e a igualdade. No entanto, dois pontos exigem maior precisão jurídica e técnica para garantir segurança regulatória e alinhamento com o ordenamento nacional.

A expressão "discurso de ódio", embora amplamente utilizada no debate público — e inclusive destacada na Pergunta 29 da Consulta prévia realizada pelo CGI.br como um dos riscos associados às infodemias — não possui definição jurídica consolidada no ordenamento brasileiro. Não se trata de categoria tipificada no Código Penal nem reconhecida como cláusula jurídica nos principais instrumentos normativos que regem o ambiente digital. Como advertiu o Relator Especial das Nações Unidas para a Liberdade de Opinião e Expressão[10], a escala e a complexidade do enfrentamento do discurso de ódio podem levar as plataformas a restringirem conteúdos que não estejam claramente vinculados a resultados lesivos ou ilegais.

Não se trata de consideração meramente hipotética: diversos governos, ao redor do mundo, vêm utilizando termos como "discurso de ódio" e "desinformação" para classificar manifestações legítimas de oposicionistas ou grupos minoritários, reprimindo-se com base em dispositivos legais que, em um primeiro momento, pareciam ter propósitos nobres.

Nesse sentido, é válido advertir que a ausência de critérios normativos claros sobre discurso de ódio favorece decisões automatizadas desproporcionais, bloqueios indevidos e efeitos inibidores sobre a expressão legítima, sobretudo de grupos minoritários ou politicamente sensíveis. Essa realidade evidencia a importância de critérios bem definidos e de medidas de mitigação proporcionais, em sintonia com o que se propôs na Pergunta 30 da consulta anterior já referenciada, que busca aperfeiçoar as formas de combater infodemias, para evitar que o combate ao discurso de ódio sirva de pretexto a restrições desproporcionais à liberdade de expressão.

No ordenamento jurídico brasileiro, quaisquer limitações a esse direito devem observar os princípios constitucionais da legalidade (art. 5º, II), da liberdade de manifestação do pensamento (art. 5º, IV e IX) e do devido processo legal (art. 5º, LIV e LV).

Por essa razão, recomenda-se que o princípio evite a expressão genérica de "discurso de ódio", substituindo-a por formulações como "manifestações ilícitas de caráter discriminatório ou violento", vinculadas a danos concretos e ao ordenamento vigente. Isso porque a própria Constituição Federal (art. 5º, IV, IX e X), o Marco Civil da Internet (Lei nº 12.965/2014, arts. 7º e 19), a LGPD (Lei nº 13.709/2018) e tratados internacionais ratificados pelo Brasil fornecem parâmetros suficientes para a proteção de direitos fundamentais no ambiente digital sem necessidade de conceitos abertos e indeterminados.

[10] Disponível em: https://docs.un.org/en/A/HRC/38/35

Nesse cenário, torna-se ainda mais essencial que os princípios que orientem futuras legislações assegurem um equilíbrio adequado, a fim de evitar que o combate ao discurso de ódio seja utilizado como fundamento impreciso ou pretexto para a imposição de restrições desproporcionais à liberdade de expressão.

O mesmo cuidado se aplica à expressão "direito à não discriminação". Ainda que inspirada em tratados internacionais, sua aplicação no ordenamento jurídico nacional exige a qualificação daquilo que configura discriminação ilícita. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) define, entre os seus princípios fundamentais, a "prevenção à discriminação ilícita" (art. 6º, IX), reconhecendo que nem toda diferenciação de tratamento é, por si só, ilegal. É fundamental, portanto, que o texto do princípio reflita esse entendimento, alinhando-se aos instrumentos normativos já consolidados no país e garantindo segurança jurídica aos regulados.

Por se tratar de princípios orientadores para futuras normas, é ainda mais necessário que as formulações adotadas tragam diretrizes claras e tecnicamente embasadas, compatíveis com a arquitetura da Internet e com os riscos reais de moderação automatizada em larga escala. Isso é especialmente relevante no contexto de plataformas de redes sociais, onde decisões de moderação de conteúdo, muitas vezes automatizadas, operam em larga escala, com impactos diretos sobre o exercício de direitos fundamentais. A ausência de critérios objetivos pode favorecer cenários de *overblocking* e exclusão desproporcional de conteúdos lícitos.

Resumo da recomendação:

I. Substituir a expressão "direito à não discriminação" por "direito à não discriminação ilícita";
II. Reconhecer a ausência de definição legal de "discurso de ódio", substituindo-o por conceitos já consolidados no ordenamento jurídico brasileiro; e
III. Incluir salvaguardas contra excessos e remoções desproporcionais.

Redação Sugerida:

A regulação deve assegurar a proteção da dignidade humana e dos direitos fundamentais, incluindo a liberdade de expressão, consideradas suas dimensões individual e coletiva, a privacidade, igualdade, o direito a não discriminação ilícita e a proteção absoluta aos direitos da criança e adolescente, ~~buscando combater~~ promovendo a prevenção à incitação à violência, a manifestações ilícitas de caráter discriminatório ou violento, ~~ao discurso de ódio~~ e a todas as formas de discriminação nas plataformas de redes sociais, com salvaguardas que assegurem proporcionalidade e evitem restrições indevidas ao exercício desses direitos.

Princípio 3 – Autodeterminação informacional

> *A regulação deve promover meios que permitam aos usuários decidir quando, como e em que medida seus dados pessoais podem ser coletados, usados, armazenados e compartilhados, inclusive nos processos de perfilização, moderação e recomendação de conteúdos. Inclui também o direito de usuários e grupos escolherem a que informações quer ter acesso, como o padrão da oferta de conteúdos que lhe é destinada com base em seus dados pessoais. Deve promover, também, a garantia da preservação da memória, determinando a criação de mecanismos para organizar e armazenar conteúdos - mesmo que não disponíveis ao público, para fins de pesquisa e registro histórico.*

Comentários:

A consagração da autodeterminação informacional como princípio regulatório é bem-vinda, pois reafirma o protagonismo dos indivíduos na gestão de seus próprios dados pessoais. No entanto, a redação proposta mistura de maneira pouco delimitada dois temas distintos: os direitos dos usuários no tratamento de seus dados pessoais e a preservação de conteúdos para fins de memória ou pesquisa histórica.

No contexto brasileiro, a autodeterminação informacional é fundamento da Lei Geral de Proteção de Dados Pessoais ("LGPD" – Lei nº 13.709/2018), assegurada por meio dos princípios e direitos conferidos aos titulares de dados. Qualquer princípio regulatório voltado às plataformas de redes sociais deve alinhar-se à LGPD, evitando sobreposições normativas ou conflitos interpretativos.

A autodeterminação informacional visa garantir que os usuários controlem seus dados pessoais, decidindo "quando, como e em que medida" seus dados pessoais podem ser utilizados e divulgados. Em outras palavras, cada indivíduo deve ter garantido o direito de ser previamente informado sobre o tratamento de seus dados pessoais, inclusive sobre perfilamento e recomendações baseadas em algoritmos. Esse conceito amplia o direito constitucional à privacidade, relacionando-o ao livre desenvolvimento da personalidade: permite ao indivíduo escolher como exercer seus direitos ou mesmo se abster deles.

A LGPD estabelece direitos aos titulares – como acesso, correção e exclusão de dados – e obriga plataformas a prestarem contas do tratamento realizado. Nesse sentido, o princípio reforça que as plataformas devem oferecer meios claros para o usuário exercer controle sobre seus dados, conforme os artigos da LGPD. Por exemplo, estipular padrões de oferta de conteúdos (como algoritmos de recomendação) com base em dados pessoais só pode ocorrer mediante regras transparentes e previamente informadas ao usuário. A Internet Society destaca em seus documentos que o processamento de dados deve respeitar princípios éticos de transparência, equidade e respeito ao titular indo além do mero cumprimento formal da lei para proteger a confiança dos usuários. Assim, segue-se que os usuários devem ter informação e mecanismos para decidir sobre coleta e uso de dados (autonomia de escolha, portabilidade, revisão de decisões automatizadas etc.), em consonância com a LGPD e os direitos humanos.

Além disso, a menção à preservação de registros históricos e de memória é pertinente e necessária. Nesse sentido, é preciso ter cautela para que medidas voltadas ao fortalecimento da autodeterminação informacional dos usuários – inclusive aquelas fundamentadas na LGPD – não inviabilizem a preservação da memória individual e coletiva.

Em casos relacionados a informações e documentos de interesse público, há relatos feitos por organizações da sociedade civil que pedidos de acesso a informações públicas, realizados com base nos instrumentos previstos pela Lei de Acesso à Informação (LAI), têm sido indevidamente negados sob o argumento de proteção de dados pessoais.[11,12,13] É fundamental que a proteção de dados não seja interpretada como obstáculo à manutenção de conteúdos de interesse público, sobretudo aqueles com relevância histórica, científica ou cultural. Ao contrário, esses dois valores devem ser vistos como complementares.

Iniciativas como bibliotecas digitais, arquivos históricos e acervos acadêmicos – a exemplo do Internet Archive – exercem papel central na produção de conhecimento e no acesso à informação, devendo atuar em conformidade com a LGPD, mas sem que esta seja usada como pretexto para censura ou apagamento indevido de conteúdos. É importante, portanto, buscar o equilíbrio entre os direitos dos titulares de dados e o interesse público na preservação da memória coletiva. Ademais, também é importante reconhecer que tais ferramentas não devem ser os únicos mecanismos destinados à salvaguarda da memória digital. Nesse sentido, seria positivo conferir maior detalhamento ao princípio, inclusive no que diz respeito aos "[conteúdos] não disponíveis ao público".

Considerando a complexidade do tema e suas nuances próprias, sugerimos: (i) que, caso se opte por manter a matéria no "Princípio - Autodeterminação Informacional", que seja esclarecido o alcance da previsão, indicando o que se espera das redes sociais em relação à disponibilização de conteúdos para fins de pesquisa, documentação e memória histórica; ou (ii) que seja incluído um princípio específico voltado à preservação da memória, com enfoque na pesquisa e no registro histórico, de forma a permitir sua efetiva tradução em políticas e ações concretas por parte das redes sociais.

Em qualquer dos cenários, é importante reconhecer que a autodeterminação informacional possui também uma dimensão coletiva, intrinsecamente relacionada à proteção da memória e do patrimônio cultural da humanidade. Essa dimensão não deve ser negligenciada ou enfraquecida em nome de outros direitos igualmente relevantes para a sociedade, mas sim equilibrada de forma a garantir que interesses individuais e coletivos sejam preservados de maneira harmônica.

[11] Disponível em: https://fiquemsabendo.com.br/transparencia/lgpd-negativa-cgu.
[12] Disponível em: https://artigo19.org/2023/09/20/artigo-19-se-reune-com-anpd-para-discutir-aplicacao-indevida-da-lgpd-em-pedidos-de-acesso-a-informacao-via-lai/
[13] Disponível em: https://www.transparencia.org.br/downloads/publicacoes/lgpd_reforco_respostas_negativas_dez_2021.pdf

Resumo da recomendação:

I. Manter a consagração da autodeterminação informacional como princípio, mas com referência expressa à LGPD;
II. Fazer uma transição compreensível entre autodeterminação individual e coletiva;
III. Reconhecer que a autodeterminação informacional não pode ser invocada para impedir a preservação de conteúdos para fins de preservação da memória; e
IV. Esclarecer o alcance da previsão sobre preservação da memória, indicando o que se espera das redes sociais em relação à disponibilização de conteúdos para essa finalidade ou incluir um princípio apartado e específico sobre o tema.

Redação Sugerida:

A regulação deve promover meios que permitam aos usuários decidir quando, como e em que medida seus dados pessoais podem ser coletados, usados, armazenados e compartilhados, inclusive nos processos de perfilização, moderação e recomendação de conteúdos. Inclui também o direito de usuários e grupos escolherem a que informações querem ter acesso, como o padrão da oferta de conteúdos que lhes é destinada com base em seus dados pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Deve promover, também, a garantia da preservação da memória, determinando a criação de mecanismos para organizar e armazenar conteúdos - mesmo que não disponíveis ao público, para fins de pesquisa e registro histórico. Nesses termos, inclui também a compreensão de autodeterminação informacional em sentido coletivo, como garantia de preservação à memória e patrimônio cultural da humanidade.

Princípio 4 – Integridade da informação

> *A regulação deve atuar para proteger o direito à informação e promover a precisão, consistência e confiabilidade do conteúdos, dos processos e dos sistemas de informações. Para a manutenção de um ecossistema saudável e seguro devem ser promovidas informações de qualidade; conteúdos jornalísticos e científicos; e políticas de preservação da memória e de enfrentamento a fraudes e desinformação.*

Comentários:

A integridade informacional exige que o conteúdo disponível na rede seja preciso, não manipulado e confiável. Nesse contexto, integridade significa "garantir que a informação seja

precisa e que não tenha sido manipulada. Isso é crucial para evitar a propagação de desinformação"[14].

Os intermediários de serviços digitais são essenciais para a estabilidade e desempenho da rede. Qualquer regulação deve, portanto, diferenciar as funções técnicas de cada componente; regras genéricas podem ter "consequências de longo alcance para toda a infraestrutura". A própria estrutura da Internet "é aberta, distribuída, interconectada e transnacional" e prospera graças a processos multissetoriais que refletem sua natureza descentralizada. Portanto, abordagens regulatórias devem privilegiar mecanismos de controle democráticos: decisões sobre remoção de conteúdo devem envolver diversos atores (governo, sociedade civil, especialistas técnicos e independentes) com transparência e recursos de contestação.

A formulação proposta acerta ao reconhecer a importância da integridade informacional para a qualidade do ecossistema digital. No entanto, para garantir sua efetividade e alinhamento com os princípios constitucionais, é recomendável que o texto explicite salvaguardas à liberdade de expressão e à possibilidade de contestação de decisões sobre conteúdos, assegurando que ações destinadas a combater a desinformação não comprometam o pluralismo informacional nem resultem em exclusão arbitrária de conteúdos lícitos.

Como destaca a Internet Society, medidas de moderação e curadoria devem ser conduzidas com base em critérios de necessidade e proporcionalidade, acompanhadas de transparência e mecanismos de contestação. A referência à promoção de conteúdos jornalísticos e científicos é pertinente, dado seu papel na validação de informações relevantes para o debate público.

Importante ressaltar que a adoção de critérios regulatórios que confiram prevalência institucional a determinados emissores de informação pode gerar efeitos adversos ao pluralismo. Experiências internacionais recentes demonstram os riscos dessa abordagem: na Índia, por exemplo, a criação de uma unidade governamental com poderes para rotular informações como "notícias falsas" foi contestada judicialmente por favorecer a censura indireta de conteúdos críticos ao governo. O caso ilustra como estruturas centralizadas de verificação podem ser utilizadas para fins políticos, com impactos negativos sobre a liberdade de expressão e a integridade do debate público.

Nesse sentido, qualquer regulação que busque promover a integridade informacional deve favorecer abordagens multissetoriais, orientadas por evidências, com diversidade de verificadores independentes, transparência procedimental e respeito à ampla gama de conteúdos protegidos constitucionalmente.

[14] Disponível em: https://www.internetsociety.org/blog/2025/04/internet-trust-why-we-need-it-and-how-to-achieve-it/#:~:text=,online%20services%20and%20software%20updates

Além disso, conforme apontado no item anterior, a preservação de registros históricos e de memória possui importância indiscutível, especialmente no contexto do debate público. Diante da complexidade e das especificidades que o tema envolve, entendemos que seria interessante tratá-lo de forma mais aprofundada ou em um princípio próprio, de modo a conferir maior clareza à abordagem que se espera das redes sociais.

Por exemplo, ferramentas como o Internet Archive (Wayback Machine), mesmo que não sejam "repositórios digitais confiáveis" no sentido arquivístico tradicional (pois carecem de cadeia rigorosa de custódia), possuem elevada importância para guardar cópias de páginas publicadas na web. Segundo Caldas (2022)[15], o Internet Archive "potencializa a constituição da memória virtual, uma vez que cria coleções que salvaguardam cópias das páginas publicadas na web". Analogamente, hemerotecas digitais (como da Biblioteca Nacional) e arquivos jornalísticos garantem o acesso a reportagens históricas. Manter esses bancos de memória exige cuidado: remover dados retroativamente (por exemplo, sob a bandeira do "direito ao esquecimento") pode fragmentar o ecossistema de informação. Nesse contexto, seria interessante que o princípio incorporasse expressamente a preocupação com o risco de perda documental e apagamento da memória coletiva, assegurando a continuidade e integridade do patrimônio informacional.

A importância de não suprimir informações de interesse público foi explicitada na Declaração de Salta (Sociedade Interamericana de Imprensa)[16]: "a supressão ou desindexação de informações sobre fatos de interesse público viola o direito do cidadão de se informar e preservar a memória coletiva". Assim, qualquer medida de regulação deve explicitar salvaguardas que protejam acervos históricos e manifestações legítimas, sejam elas jornalísticas, científicas, culturais ou opinativas. O pluralismo informacional – incluindo vozes de mídia comunitária, educadores e movimentos culturais – deve ser garantido, pois enriquece o debate público e reforça a resistência a abusos.

Enfrentar fraudes e notícias falsas é importante, mas deve-se evitar mecanismos censórios ou excessivamente centralizados. Como destaca a Declaração de Salta (princ. 10), "a disseminação maliciosa ou deliberada de desinformação… não deve ser combatida por meio de mecanismos de censura nem sanções penais, mas com a adoção de políticas de alfabetização digital e midiática".

Isso corrobora iniciativas que preconizam educação midiática e transparência, em vez de punições severas. Experiências recentes mostram os riscos da via punitiva: na Índia, o Tribunal

[15] Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/237824/Artigo%20-%20Douglas%20de%20Souza%20Caldas.pdf?sequence=1&isAllowed=y#:~:text=Os%20resultados%20apurados%20pela%20pesquisa,das%20p%C3%A1ginas%20publicadas%20na%20web

[16] Disponível em: https://abraji.org.br/noticias/sociedade-interamericana-de-imprensa-aprova-declaracao-sobre-liberdade-de-expressao-na-era-digital

de Bombaim declarou inconstitucional[17] uma emenda que criava uma unidade governamental para rotular conteúdos como "falsos, enganosos ou tendenciosos". A corte observou que essa medida conferia ao governo "autoridade única" para decidir o que era verdade, adotando formato de "censura de conteúdo do usuário". Esse caso ilustra que atribuir poder centralizado de classificação tende a censurar críticas legítimas e ameaça a integridade informacional.

Por outro lado, organizações de mídia vêm mostrando que confiança pública cresce com padrões editoriais claros, colaboração com verificadores independentes e transparência nos processos. O mesmo vale para redes sociais: o uso de fact-checkers independentes (como AFP e o International Fact-Checking Network) e alertas de fontes duvidosas podem reduzir a disseminação sem excluir conteúdo legal[18].

Como princípio estruturante para uma futura regulação, portanto, sugere-se o estímulo, mas não a substituição, a essas práticas privadas, preservando sempre mecanismos de recurso judicial e permitindo ao usuário contestar remoções.

Resumo da recomendação:

I. Evitar formulações que possam induzir à hierarquização normativa entre tipos de conteúdo com base em sua origem institucional;
II. Incluir a expressão "de interesse público" para ampliar a proteção a diferentes formas legítimas de conteúdo informacional;
III. Prevenir interpretações que permitam estruturas centralizadas de verificação, favorecendo abordagens multissetoriais, transparentes e orientadas por evidências; e
IV. Acrescentar salvaguardas à liberdade de expressão, ao pluralismo informacional e a mecanismos de contestação de decisões sobre conteúdos;
V. Incorporar expressamente, no que diz respeito à preservação da memória, a preocupação com o risco de perda documental e apagamento da memória coletiva.

Redação Sugerida:

A regulação deve atuar para proteger o direito à informação e promover a precisão, consistência e confiabilidade dos conteúdos, dos processos e dos sistemas de informações. Para a manutenção de um ecossistema saudável e seguro devem ser promovidas informações de qualidade; conteúdos jornalísticos e científico e de interesse públicos; ~~e~~ políticas de preservação da memória, com atenção aos riscos de perda documental e apagamento da memória coletiva, e também de enfrentamento a

[17] Disponível em: https://verfassungsblog.de/india-fact-checking-unit-fake-news/#:~:text=,And
[18] Disponível em: https://www.internetsociety.org/blog/2020/04/disinformation-the-invisible-sword-dividing-society/#:~:text=In%20consuming%20news%20information%2C%20we,in%20the%20battle%20against%20disinformation

fraudes e desinformação, com salvaguardas à liberdade de expressão, ao pluralismo informacional e a mecanismos de contestação.

Princípio 5 – Inovação e desenvolvimento social

A regulação deve promover a inovação e o desenvolvimento social, econômico e tecnológico, possibilitando a geração de renda, visibilidade de produtos e serviços, novas formas de trabalho decente e dinamização da economia digital, especialmente para pequenos empreendedores, criadores de conteúdo, prestadores de serviços autônomos e negócios locais. A regulação deve fomentar um ambiente digital que sustente múltiplas alternativas tecnológicas, garantindo que indivíduos, grupos, comunidades e empresas possam criar e manter modelos que facilitem uma existência econômica digna, que valorize a colaboração, o bem comum e outras formas de geração de valor.

Comentários:

Este princípio expressa, de forma sintética e acertada, o potencial econômico das redes sociais no contexto brasileiro. Em um país marcado por altos níveis de informalidade, desigualdades estruturais e acesso limitado a crédito e infraestrutura, as plataformas digitais funcionam como ferramentas acessíveis para geração de renda, organização produtiva e visibilidade de pequenos negócios.

Ao reconhecer o papel de empreendedores individuais, criadores de conteúdo e prestadores de serviços autônomos, o princípio contribui para a construção de um ambiente digital inclusivo, que valorize modelos econômicos diversos.

De certa forma, a propositura deste princípio é alinhada com a Recomendação 7 do Decálogo da ISOC sobre o Modelo Brasileiro de Responsabilidade de Intermediários, quando se espera que a Internet seja respeitada como rede de propósitos múltiplos, inovadores, evitando, assim, regulações dedicadas a modelos específicos. A dinamicidade das aplicações na Internet favorece o surgimento de novas práticas laborais, que, por sua vez, carecem também de regulações mais duradouras.

O Princípio também destaca a necessidade de “múltiplas alternativas tecnológicas” e modelos diversos que sustentem “uma existência econômica digna”. Isso inclui incentivar soluções comunitárias e descentralizadas. Em consonância, estudos promovidos pelo CGI.br mostram que redes comunitárias de Internet – geridas por usuários locais – têm papel estratégico em conectar áreas remotas e menos assistidas. Essas redes não só levam

conectividade a quem não teria outra forma de acesso, mas também estimulam a apropriação da tecnologia pelas próprias comunidades, fomentando inovação local.

Assim, políticas regulatórias devem incentivar a concorrência e diversidade tecnológica – por exemplo, por meio de incentivos a provedores regionais ou uso de códigos abertos – para que empreendedores e negócios locais possam criar serviços digitais próprios. Iniciativas como o projeto Conectividade Centrada em Comunidades – que envolveu uma parceria da ISOC Brasil com o IRIS[19] – fortalecem redes comunitárias na América Latina justamente para expandir essas alternativas tecnológicas locais. Assim, a regulação deve fomentar concorrência e diversidade tecnológica, incentivando provedores regionais, software livre e outros modelos variados para que empreendedores e comunidades criem suas próprias soluções digitais.

Por fim, o princípio valoriza explicitamente a colaboração e o bem comum. Essa visão está alinhada ao modelo de governança multissetorial do CGI.br: a Internet deve ser um bem público que promova inclusão e compartilhamento de valor.

Em outras palavras, inovação deve servir ao interesse coletivo, e não apenas a lucros concentrados. Por isso, é importante que a regulação preserve direitos digitais (como privacidade e autodeterminação informacional) para que comunidades e grupos diversos possam participar e decidir sobre a tecnologia de forma independente. Dessa forma, amplia-se a confiança social para cooperar em plataformas digitais e desenvolver projetos colaborativos (como cooperativas de plataforma, redes comunitárias, iniciativas de dados abertos etc.), todos potenciais modelos de geração de valor econômico e social digno.

Princípio 6 – Transparência e prestação de contas

> *A transparência e prestação de contas são essenciais para o desenvolvimento adequado das atividades de redes sociais, considerando seu impacto social, econômico e político. As plataformas devem ser transparentes em relação a seus sistemas de moderação (inclusive quanto à composição das equipes de moderação), algoritmos de recomendação e políticas de impulsionamento e monetização, incluindo meios adequados de participação e verificação nas remoções de conteúdos, por padrões abertos e padronizados (quando aplicável) e aberturas qualificadas de dados relevantes para pesquisadores independentes e autoridades públicas.*

Comentários:

O princípio expressa corretamente a importância da transparência e da prestação de contas para um ambiente digital mais confiável e aberto, valor compartilhado pela ISOC e refletido nas Recomendações 8 e 9 do Decálogo da ISOC Brasil, que defendem mecanismos efetivos de transparência e *accountability* das plataformas, além do provimentos de informações claras e a possibilidade de defesa pelos usuários.

[19] Disponível em: https://www.isoc.org.br/noticia/projeto-conectividade-centrada-em-comunidades

No entanto, observamos que as aberturas qualificadas de dados relevantes para pesquisadores e autoridades públicas devem observar rigorosamente os direitos de proteção de dados pessoais, conforme estabelecido na LGPD (Lei nº 13.709/2018). Além disso, boas práticas internacionais, como as previstas no Digital Services Act (DSA) da União Europeia, reconhecem expressamente que a transparência deve respeitar a proteção de dados e a segurança dos serviços. É essencial que esse equilíbrio seja refletido desde a formulação dos princípios e, sobretudo, na construção de futuras obrigações normativas, para garantir que a transparência não se realize em detrimento da privacidade e da autodeterminação informacional dos usuários.

Resumo da recomendação:

I. Inserir salvaguarda explícita à proteção de dados pessoais, nos termos da LGPD.

Redação Sugerida:

A transparência e prestação de contas são essenciais para o desenvolvimento adequado das atividades de redes sociais, considerando seu impacto social, econômico e político. As plataformas de redes sociais devem ser transparentes em relação a seus sistemas de moderação (inclusive quanto à composição das equipes de moderação), algoritmos de recomendação e políticas de impulsionamento e monetização, incluindo meios adequados de participação e verificação nas remoções de conteúdos, por padrões abertos e padronizados (quando aplicável) e aberturas qualificadas de dados relevantes para pesquisadores independentes e autoridades públicas, observada a proteção de dados pessoais nos termos da legislação aplicável.

Princípio 7 – Interoperabilidade e portabilidade

A regulação deve garantir aos usuários das redes sociais os direitos de portabilidade e interoperabilidade. Deve ser possível solicitar, a pedido do titular dos dados, a transferência de dados em um formato estruturado, comumente usado e legível por máquina. A regulação deve promover, considerando os desafios técnicos e responsabilidades legais, a capacidade de diferentes serviços digitais trabalharem juntos e se comunicarem entre si, o emprego de protocolos e padrões abertos, permitindo que os usuários combinem vários serviços com funcionalidades complementares, inclusive por meio de obrigações que permitam a portabilidade em tempo real, de forma que o conteúdo possa ser lido e processado de forma instantânea e automática por computadores e sistemas digitais distintos.

Comentários:

O princípio afirma valores essenciais para um ambiente digital mais aberto e competitivo. A promoção da portabilidade e da interoperabilidade é coerente com os princípios defendidos pela ISOC, em particular com a Recomendação 7 do Decálogo da ISOC Brasil, que destaca a importância da interoperabilidade e do uso de padrões abertos para garantir um ecossistema de Internet plural, competitivo e inovador. É igualmente positivo que o princípio reconheça explicitamente os desafios técnicos e responsabilidades legais associados à implementação da interoperabilidade, o que está em linha com a Recomendação 4 do Decálogo da ISOC Brasil (assimetria regulatória e proporcionalidade).

No entanto, a formulação que prevê a portabilidade em tempo real, com leitura e processamento instantâneo e automático merece maior cautela. Embora se trate de um princípio orientador para futuras regulações, a redação desse trecho, se transposta de forma literal para normas vinculantes, poderia gerar riscos técnicos, comprometer a segurança da arquitetura da Internet e favorecer indevidamente grandes plataformas em detrimento de atores menores. É importante que as futuras obrigações de interoperabilidade e portabilidade sejam formuladas de forma proporcional e tecnicamente viável, respeitando a diversidade e a heterogeneidade do ecossistema digital.

Por exemplo, seria necessário manter APIs abertas permanentemente disponíveis e com alta escalabilidade, o que demanda infraestrutura robusta de computação e rede – algo natural para grandes plataformas, mas oneroso para provedores menores. Cada interface exposta deve contar com fortes medidas de segurança (autenticação, autorização e criptografia) para evitar vulnerabilidades. Em especial, todos os dados sensíveis devem ser cifrados tanto em trânsito quanto em repouso, prevenindo interceptações ou adulterações. É importante também respeitar a criptografia ponta-a-ponta adotada em muitos serviços (por exemplo, aplicativos de mensagens), de forma que a portabilidade não force a exposição de chaves privadas ou a decodificação dos conteúdos. Qualquer norma nesse sentido deve prever que a interoperabilidade funcione em conformidade com os padrões de segurança atuais e a legislação de proteção de dados, garantindo integridade e confidencialidade.

A arquitetura da Internet foi projetada em camadas modulares (física, enlace, rede, transporte, aplicação) que usam protocolos abertos (como IP, TCP/UDP, DNS, HTTP, SMTP etc.) para permitir a conexão de qualquer dispositivo ou rede ao conjunto global sem exigir permissão de terceiros. Cada camada oferece funções bem definidas – por exemplo, o IP cuida do endereçamento e roteamento entre redes heterogêneas, o TCP/UDP provê transporte confiável ou não, e protocolos como HTTP ou DNS operam na camada de aplicação. Essa arquitetura aberta de blocos interoperáveis permite inovação horizontal: qualquer pessoa pode adicionar novos serviços ou aplicações “sobre” esses blocos sem ter que modificar a rede subjacente. Não há uma autoridade central controlando quem conecta onde; em vez disso, um roteamento distribuído permite que milhões de redes se interliguem organicamente. Essa estrutura

assentada em padrões abertos é essencial, uma vez que habilita sua existência global e impulsiona inovação e crescimento.

Diferentemente disso, interoperabilidade funcional refere-se à capacidade de diferentes serviços de aplicação (como redes sociais, sistemas de mensagens ou provedores de conteúdo) trocarem dados ou comunicarem-se entre si para oferecer serviços integrados ao usuário. Isso ocorre numa camada acima da infraestrutura Internet – depende de APIs, formatos de dados e regras próprias de cada plataforma. Exemplos atuais incluem direitos de portabilidade de dados (como na LGPD/GDPR) e iniciativas de federação (como o Fediverso com o protocolo ActivityPub).

Distintamente dos protocolos técnicos universais, cada plataforma costuma ter arquitetura de aplicação fechada: seus dados (mensagens, perfis, arquivos) estão em silos proprietários. Para interoperar, seria preciso padronizar essas informações e disponibilizar interfaces (APIs) para transferência ou comunicação em tempo real. Protocolos abertos como o ActivityPub – "um protocolo de redes sociais descentralizado" que define APIs federadas cliente-servidor e servidor-servidor ilustram como a interoperabilidade funcional pode ocorrer sem centralizar o controle das plataformas.

Em geral, essa interoperabilidade funcional envolve questões organizacionais, de governança e segurança adicionais: ao contrário da camada de rede, aqui cada serviço define regras de negócio e proteção de dados próprias. Assim, técnicos e reguladores precisam lidar com formatos de dados, políticas de privacidade, criptografia ponta-a-ponta etc., que não existem na camada de protocolo puro da Internet.

A distinção acima indica que qualquer exigência regulatória de interoperabilidade deve respeitar as propriedades críticas da arquitetura da Internet, em vez de subvertê-las, em especial o respeito à arquitetura de rede. Devem-se preservar os padrões abertos e a descentralização inerentes à Internet. Obrigações legais só devem atuar na camada de aplicação dos provedores, sem impor mecanismos que comprometam a estabilidade ou o roteamento da rede.

Por exemplo, obrigar redes sociais a transferir dados em tempo real não deve levar à adoção de protocolos proprietários ou "gargalos" centralizados, nem a mudanças fundamentais no IPv4/IPv6 ou no modelo de multiplexação da Internet. Obrigações de transferência instantânea de dados entre plataformas geram vários desafios técnicos e de segurança. Do ponto de vista técnico, fluxos em tempo real de grande volume podem sobrecarregar redes e servidores, criando instabilidades ou latências impraticáveis.

Em termos de segurança e privacidade, abrir plataformas para comunicação mútua expõe novas superfícies de ataque: por exemplo, exigências de interoperar podem forçar os sistemas a renunciar à criptografia ponta-a-ponta ou a criar APIs públicas vulneráveis. Além disso, sincronizar informações dinamicamente entre diferentes algoritmos de moderação ou perfis de usuários pode levar a vazamentos de dados ou manipulação de informações.

Por fim, portabilidade em tempo real sem critérios claros pode criar "fragmentação" ao invés de integração, desrespeitando a coerência da infraestrutura subjacente. Por outro lado, a interoperabilidade entre plataformas pode ser positiva se baseada em padrões abertos e respeitar a descentralização da Internet. Soluções federadas mostram que é possível combinar serviços mantendo a rede distribuída: cada servidor ou aplicação pode implementar funcionalidades próprias, mas comunicar-se usando protocolos compartilhados. Por isso, propõe-se que o regulador estimule a interoperabilidade funcional por meio de padrões abertos reconhecidos, garantindo múltiplas alternativas tecnológicas sem criar pontos únicos de falha – preservando assim a resiliência e a diversidade do ecossistema digital.

Resumo da recomendação:

I. Ajustar a formulação referente à portabilidade em tempo real, para garantir proporcionalidade técnica e segurança.

Redação Sugerida:

A regulação deve garantir aos usuários das redes sociais os direitos de portabilidade e interoperabilidade. Deve ser possível solicitar, a pedido do titular dos dados, nos termos da legislação aplicável, a transferência de dados em um formato estruturado, comumente usado e legível por máquina. A regulação deve promover, considerando os desafios técnicos e responsabilidades legais, a capacidade de diferentes serviços digitais trabalharem juntos e se comunicarem entre si, o emprego de protocolos e padrões abertos, permitindo que os usuários combinem vários serviços com funcionalidades complementares, inclusive por meio de obrigações que permitam a portabilidade de forma tecnicamente viável e segura, respeitando as limitações operacionais aplicáveis ~~em tempo real, de forma que o conteúdo possa ser lido e processado de forma instantânea e automática por computadores e sistemas digitais distintos~~.

Princípio 8 – Prevenção de danos e responsabilidade

As plataformas de redes sociais devem envidar seu melhor esforço para prevenir e precaver os potenciais danos decorrentes de suas atividades, sobretudo aqueles advindos da circulação de conteúdos. As redes sociais são responsáveis pelos danos decorrentes de riscos sistêmicos inerentes ao serviço prestado, devendo repará-los ou mitigá-los. Entende-se por danos decorrentes de riscos sistêmicos, aqueles causados pelo ambiente da rede resultante de suas políticas de transparência, moderação (incluindo ações de redução de alcance ou ocultamento), recomendação e impulsionamento de conteúdos.

Comentários:

O princípio reconhece corretamente que plataformas de redes sociais devem adotar práticas responsáveis para reduzir e mitigar riscos associados às suas atividades. A ISOC Brasil compartilha essa visão, em linha com a Recomendação 8 do seu Decálogo, que defende mecanismos efetivos de transparência, prestação de contas e mitigação de riscos, com respeito aos direitos fundamentais. No entanto, a formulação que afirma que "as redes sociais são responsáveis pelos danos decorrentes de riscos sistêmicos inerentes ao serviço prestado" merece maior precisão.

O Marco Civil da Internet estabeleceu, no Brasil, um modelo de responsabilidade civil dos provedores de aplicações de Internet baseado na responsabilidade subjetiva, condicionado, em regra, à existência de ordem judicial para a remoção de conteúdos ilícitos (art. 19). Esse regime, que está atualmente em debate no Supremo Tribunal Federal, permanece vigente e a introdução, mesmo em nível principiológico, de uma responsabilidade automática ou objetiva por danos decorrentes de "riscos sistêmicos" — conceito que carece de definição jurídica consolidada no Brasil — poderia gerar tensão e comprometer a segurança jurídica.

É fundamental que, na formulação de obrigações futuras com base neste princípio, sejam respeitadas essas garantias, evitando a criação indireta de um regime de responsabilidade objetiva para intermediários. Essa visão está de acordo com a Recomendação 5 de nosso Decálogo, mas, principalmente, com o aspecto substancial da Recomendação 6 do nosso Decálogo.

Além disso, o conceito de "riscos sistêmicos", como utilizado no DSA, é aplicado dentro de um sistema normativo específico, que impõe obrigações de diligência e mitigação proporcionais, sem converter as plataformas em responsáveis automáticas por quaisquer danos que possam emergir de seus sistemas. A transposição acrítica desse conceito, sem definição legal e salvaguardas adequadas, gera insegurança jurídica e tem uma alta probabilidade de ser interpretado de forma extensiva e equivocada, criando regimes de responsabilidade prejudiciais ao bom funcionamento da Internet e limitadores da ampla circulação de informação, incluindo manifestações legítimas e benéficas ao regime democrático, no ambiente digital.

A definição dada no último parágrafo, de que danos recorrentes de riscos sistêmicos seriam "*aqueles causados pelo ambiente da rede resultante de suas políticas de transparência, moderação (incluindo ações de redução de alcance ou ocultamento), recomendação e impulsionamento de conteúdos",* também parece ampla e carece de precisão, indo potencialmente além do escopo observado em outras legislações, como a europeia.

O uso do termo "políticas" no início dessa definição faz com que quase tudo que seja realizado pela plataforma (incluindo definições sobre transparência) seja classificável como

"risco sistêmico". É preciso lembrar que existem práticas de moderação e recomendação em quase qualquer intermediário no ambiente digital, inclusive os de natureza estritamente técnica e os realizados pela própria comunidade, como no caso da Wikipedia. Tornar o mero uso de qualquer mecanismo de recomendação e moderação como ensejador de risco sistêmico parece ser inadequado e arriscado.

Por fim, a regulação de riscos e responsabilidades deve sempre observar os princípios de proporcionalidade regulatória e de assimetria entre os diferentes atores do ecossistema digital, conforme previsto no Princípio 9 da proposta do CGI.br e na Recomendação 4 do Decálogo da ISOC Brasil, de modo a evitar distorções e impactos desproporcionais, especialmente sobre atores de menor porte.

Resumo da recomendação:

I. Evitar a formulação de um regime de responsabilidade objetiva com base em conceito indeterminado de "riscos sistêmicos";
II. Recomendar que o princípio enfatize obrigações de diligência e mitigação proporcionais, compatíveis com o regime vigente de responsabilidade intermediária no Brasil; e
III. Reformular ou suprimir a definição dada a "danos decorrentes de riscos sistêmicos", considerando que em sua atual forma ela poderia englobar a totalidade das atividades exercidas por plataformas.

Redação Sugerida:

As plataformas de redes sociais devem envidar seu melhor esforço para prevenir e precaver os potenciais danos decorrentes de suas atividades, sobretudo aqueles advindos da circulação de conteúdos. ~~As redes sociais são responsáveis pelos danos decorrentes de riscos sistêmicos inerentes ao serviço prestado, devendo repará-los ou mitigá-los. Entende-se por danos decorrentes de riscos sistêmicos, aqueles causados pelo ambiente da rede resultante de~~ Elas devem adotar medidas adequadas de diligência e mitigação para reduzir riscos associados às suas políticas de transparência, moderação (incluindo ações de redução de alcance ou ocultamento), recomendação e impulsionamento de conteúdos, podendo ser responsabilizadas caso não o façam, dentro dos limites do ordenamento jurídico brasileiro vigente.

Princípio 9 – Proporcionalidade regulatória

A regulação deve reconhecer a pluralidade de atores no ecossistema digital, prevendo obrigações de acordo com as diferenças de porte e impacto das plataformas, adotando

modelos assimétricos e proporcionais que considerem os riscos decorrentes das atividades.

Comentários:

O princípio expressa corretamente um dos fundamentos essenciais para a construção de um modelo regulatório equilibrado para as plataformas de redes sociais. A proporcionalidade regulatória e a adoção de modelos assimétricos são condições indispensáveis para garantir que a regulação seja eficaz, viável e respeitosa da diversidade do ecossistema digital.

A ISOC Brasil compartilha integralmente essa orientação, em linha com as Recomendações 1 e 4 do seu Decálogo sobre o Modelo Brasileiro de Responsabilidade de Intermediários, que enfatiza que as políticas públicas para o ambiente digital devem considerar as múltiplas assimetrias de capacidade, função e risco entre os diferentes tipos e portes de plataformas. O relatório global da Internet Society, *A Policy Framework for Internet Intermediaries and Content*[20], também reforça que abordagens regulatórias proporcionais e diferenciadas, com base nas funções e capacidades dos intermediários, são essenciais para evitar distorções, favorecer indevidamente plataformas dominantes ou inibir a inovação.

É, acima de tudo, importante que este princípio seja compreendido como transversal, orientando a aplicação de todos os demais princípios propostos — inclusive aqueles que tratam de transparência, mitigação de riscos e responsabilidades. Tal abordagem contribuirá para a construção de um marco regulatório equilibrado, que promova a proteção de direitos sem comprometer a abertura e a inovação da Internet.

Resumo da recomendação:

I. Explicitar que esse é um princípio que deve ser transversal aos outros princípios do Decálogo;

Redação Sugerida:

A regulação deve reconhecer a pluralidade de atores no ecossistema digital, inclusive quando aplicando os outros princípios deste Decálogo, prevendo obrigações de acordo

[20] *Disponível em: https://www.internetsociety.org/wp-content/uploads/2024/12/2025-Policy-Framework-Report-EN.pdf*

com as diferenças de porte e impacto das plataformas, adotando modelos assimétricos e proporcionais que considerem os riscos decorrentes das atividades.

Princípio 10 – Governança multissetorial e ambiente regulatório

A regulação das redes sociais deve se basear em um arranjo institucional que envolva uma governança multissetorial e órgãos independentes dotados das necessárias capacidades para sua atuação, a exemplo de capacidade técnica e fiscalizatória.

Comentários:

O princípio afirma corretamente que a regulação das redes sociais deve se apoiar em um modelo de governança multissetorial, condição essencial para assegurar a legitimidade, o equilíbrio e a eficácia das políticas públicas relativas à Internet. Esse princípio está em conformidade com a faceta procedimental e formal da Recomendação 6 do Decálogo da ISOC Brasil.

Do ponto de vista técnico, a governança multissetorial não é apenas um modelo normativo desejável, mas um componente essencial para a preservação da arquitetura descentralizada da Internet, isso porque a eficácia da Internet como rede de redes depende de cinco propriedades críticas: acessibilidade com protocolos abertos, arquitetura modular, gerenciamento descentralizado, identificadores globais comuns e neutralidade tecnológica.

O desenvolvimento de normas que afetem plataformas digitais sem considerar essas propriedades pode gerar fragmentações técnicas, rupturas na interoperabilidade ou impactos negativos à escalabilidade e à inovação na borda da rede. Além disso, o modelo multissetorial é o único capaz de garantir que decisões sobre aspectos técnicos – como alocação de identificadores, interoperabilidade entre protocolos, moderação de conteúdo com base algorítmica e preservação de padrões abertos – sejam tomadas com base em evidências, transparência e consenso multissetorial.

Como já defendido anteriormente pela ISOC Brasil, qualquer iniciativa regulatória que comprometa essas condições técnicas e institucionais tende a prejudicar não apenas os direitos dos usuários, mas a própria viabilidade de longo prazo da Internet como infraestrutura crítica. Por fim, recomenda-se que o princípio também afirme expressamente que a estrutura institucional da regulação deve incorporar mecanismos contínuos de avaliação de impacto regulatório, com base em parâmetros técnicos e jurídicos, como àqueles contidos na

Metodologia de Avaliação de Impacto da Internet[21] (IIAT) proposta pela ISOC, de modo a antecipar e mitigar riscos à rede como um todo.

A ISOC Brasil valoriza que este princípio reafirme de forma expressa o compromisso com uma governança multissetorial efetiva, especialmente por se tratar de uma proposição oriunda do CGI.br, instância reconhecida internacionalmente por seu modelo multissetorial. Nesse contexto, é desejável que esse modelo permeie todas as etapas do ciclo regulatório e que a atuação de órgãos independentes, quando prevista, se dê de forma integrada e coerente com a governança multissetorial, fortalecendo e não substituindo seu papel central no ecossistema da Internet no Brasil.

Resumo da recomendação:

I. Considerar as propriedades críticas da internet, tais como propostas pela ISOC, no desenvolvimento de normas que afetem plataformas digitais;
II. Incorporar mecanismos contínuos de avaliação de impacto regulatório, com base em parâmetros técnicos e jurídicos, a fim de antecipar e mitigar riscos à rede; e
III. Garantir que o modelo de governança multissetorial permeie todo o ciclo regulatório, garantindo que a atuação de órgão independentes ocorra de forma integrada e coerente com tal modelo.

Redação Sugerida:

A regulação das redes sociais deve se basear em um arranjo institucional que envolva uma governança multissetorial e órgãos independentes dotados das necessárias capacidades para sua atuação, a exemplo de capacidade técnica e fiscalizatória, devendo-se incorporar mecanismos contínuos de avaliação de impacto regulatório, com base em parâmetros técnicos e jurídicos.

3. Observações adicionais

A ISOC Brasil aproveita o espaço de manifestação pública para adicionar aspectos que não estavam abertos à contribuição no formato proposto, salientando que consultas públicas que tenham espaços para observações adicionais e prazos maiores auxiliam na participação da comunidade.

Alertamos em relação às definições adotadas para plataformas e também para redes sociais. Nesse sentido e tendo participado da consulta pública inicial que deu insumo à

[21] Disponível em: https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/

conceituação apresentada, consideramos que a definição de plataformas digitais deve apontar de forma manifesta como elas operam sobre a infraestrutura da Internet, e principalmente evitar listar características de algumas plataformas (particularmente, as grandes) como se fossem uniformes para todo o grupo.

Já em relação ao conceito de redes sociais, apontamos que a definição adota uma visão centrada nas redes sociais mais popularmente conhecidas, mas sem abrir espaço de inclusão conceitual, por exemplo, para redes sociais federadas. Consideramos que é importante se atentar à diversidade de modelos existentes e em desenvolvimento no ecossistema digital.

4. Conclusão

A ISOC Brasil reafirma seu compromisso com a construção de um modelo de regulação de plataformas de redes sociais que seja proporcional, eficaz e alinhado com os princípios que estruturam a arquitetura da Internet. Nesse sentido, valoriza a iniciativa do CGI.br em promover um debate multissetorial e técnico, capaz de orientar o desenvolvimento de políticas públicas que preservem a abertura, a interoperabilidade, a inovação e os direitos fundamentais no ambiente digital.

As contribuições aqui apresentadas têm por objetivo aprimorar a formulação dos princípios propostos, assegurando que seu futuro desdobramento normativo respeite o regime brasileiro de responsabilidade de intermediários, as garantias constitucionais e os padrões internacionais de governança e funcionamento da Internet.

A ISOC Brasil coloca-se à disposição para contribuir com o aprofundamento deste debate, reiterando seu apoio ao papel central do CGI.br como instância legítima e reconhecida de governança multissetorial da Internet no Brasil.