

AVANÇOS E DESAFIOS NA REGULAÇÃO DIGITAL COM O MARCO CIVIL DA INTERNET: PERSPECTIVAS DAS POLÍTICAS PÚBLICAS PARA A NEUTRALIDADE DA REDE

Edna Raquel Hogemann

Universidade Federal do Estado do Rio de Janeiro (Unirio),
Rio de Janeiro.

edna.r.hogemann@unirio.br

Resumo: Este artigo explora a evolução das políticas públicas relacionadas ao Marco Civil da Internet no Brasil, analisando seus avanços, desafios e impactos na regulação digital na perspectiva da neutralidade da rede. O Marco Civil da Internet, promulgado em 2014, é uma legislação pioneira que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. A análise é dividida em três tópicos: a construção e aprovação do Marco Civil, os principais avanços e conquistas, e os desafios persistentes na sua implementação. O estudo destaca a importância de políticas públicas eficazes para assegurar uma internet livre, aberta, inclusiva e neutra o suficiente para a promoção de um ambiente digital justo e democrático.

Palavras-chave: Políticas públicas, Marco Civil da Internet, regulação digital, Brasil, neutralidade.

Advances and challenges in digital regulation with the Brazilian Civil Rights Framework for the Internet: perspectives on public policies for network neutrality

Abstract This paper explores the evolution of public policies related to the Marco Civil da Internet in Brazil, analyzing its advancements, challenges, and impacts on digital regulation from the perspective of network neutrality. Enacted in 2014, the Marco Civil da Internet is pioneering legislation that establishes principles, guarantees, rights, and duties for the use of the internet in Brazil. The analysis is divided into three topics: the development and approval of the Marco Civil, the main advancements and achievements, and the ongoing challenges in its implementation. The study highlights the importance of effective public policies to ensure a free, open, inclusive, and sufficiently neutral internet to foster a fair and democratic digital environment.

Keywords: Public policies, Marco Civil da Internet, digital regulation, Brazil, neutrality.

INTRODUÇÃO

A evolução tecnológica e a crescente digitalização da sociedade têm imposto novos desafios regulatórios, exigindo a formulação de políticas públicas eficazes que garantam um ambiente digital seguro, justo e democrático. A internet se tornou uma parte essencial da vida cotidiana, influenciando a comunicação, a economia, a educação e a política. No Brasil, o Marco Civil da Internet, sancionado em 2014, representa um marco significativo na regulação digital. É considerada uma das legislações mais importantes e inovadoras no campo da regulação digital. Ele estabelece princípios, garantias, direitos e deveres para o uso da internet no país, com especial destaque para a neutralidade da rede. A neutralidade da rede é um princípio que garante que

todos os dados na internet sejam tratados de forma igualitária, sem discriminação ou prioridade, independentemente de origem, destino, conteúdo ou tipo de serviço.

No Brasil, a implementação de políticas públicas na regulação digital é crucial para assegurar os direitos dos usuários, promover a inovação e garantir a igualdade de acesso à internet, razão pela qual o presente artigo busca analisar as políticas públicas relacionadas ao Marco Civil da Internet, avaliando seus avanços, desafios e impactos na sociedade brasileira, tendo como foco especial o dilema da neutralidade das redes. Nesse propósito o estudo inicia demonstrando em que medida o Marco civil da Internet se revela como verdadeiro exemplo de regulação digital em nosso país, trazendo uma breve reflexão a respeito de seus pilares principiológicos fundamentais. A seguir, o texto avança para se debruçar sobre os avanços e as conquistas alcançadas a partir do advento da referida lei, não sem refletir em relação aos desafios que persistem em razão de sua implementação, mormente no que diz respeito ao aspecto necessário da neutralidade da rede para, a seguir, debruçar-se sobre uma análise, ainda que não exaustiva, a respeito da importância das políticas públicas relativas à regulação digital.

O estudo conclui no sentido de apontar para a necessidade objetiva de uma internet que seja simultaneamente livre, aberta, neutra e inclusiva na perspectiva do fortalecimento das próprias políticas públicas que promovam a cooperação proativa entre governos, sociedade civil e setor privado.

1 O MARCO CIVIL DA INTERNET: UM EXEMPLO DE REGULAÇÃO DIGITAL

É evidente que o Direito se manifesta de maneira abrangente, envolvendo também a regulação do ambiente digital. Com o intuito de estabelecer diretrizes e princípios para o uso da internet no Brasil, o governo brasileiro promulgou em 2014 a Lei nº 12.965, amplamente conhecida como Marco Civil da Internet¹.

A Lei nº 12.965/14, ou Marco Civil da Internet, também denominada por alguns como a Constituição da Internet, que completou uma década desde a sua entrada em vigor em nosso ordenamento jurídico, estabelece um conjunto de princípios e diretrizes fundamentais para a regulamentação do uso da internet no Brasil. O Marco Civil da Internet é amplamente celebrado por sua natureza inovadora, tanto em termos de forma quanto de conteúdo, no que tange à regulamentação dos direitos humanos no ambiente digital. Esta legislação, composta por 32 artigos, abrange uma variedade de temas, incluindo os direitos e garantias dos usuários, a provisão de conexão e serviços da internet, a responsabilidade dos provedores e a atuação do poder público, entre outros.

Além disso, o artigo 3º dessa lei estabelece os princípios que orientam a utilização da internet no Brasil. Especificamente, ele define que a internet no Brasil deve ser guiada pelos seguintes princípios: a) Respeito à liberdade de expressão: A internet deve garantir a liberdade de expressão e acesso à informação; b) Privacidade: Deve ser assegurada a privacidade dos usuários, protegendo seus dados pessoais; c) Neutralidade da rede: As redes devem operar de forma

¹ Importante sublinhar que, “em um primeiro momento, foi submetido à sociedade um texto que continha princípios gerais para regulação da rede em que foi recebido mais de 800 comentários, opiniões e propostas que poderiam incrementar a posterior regulamentação. Em seguida, já na segunda fase do processo, as sugestões foram sistematizadas em uma minuta do projeto de lei que foi novamente submetida a consulta pública e envolveu uma série de debates públicos. Com o fim desses procedimentos, em 24 de agosto de 2011, o PL nº 2.126/2011 foi apresentado à Câmara dos Deputados, tramitando durante 3 anos entre as casas legislativas, nasceu em 2014 a Lei nº 12.965, sancionada pela presidente Dilma Rousseff na abertura da Conferência Net Mundial”. (Ramos, 2021, p. 01)

neutra, sem discriminação ou preferência por determinados conteúdos ou serviços; d) Transparência: É necessário garantir transparência nas práticas de tratamento e proteção de dados dos usuários; e) Segurança: As plataformas e serviços devem garantir a segurança dos dados. Desses, três princípios são considerados fundamentais, verdadeiros pilares da legislação: a liberdade de expressão, a neutralidade de rede e a privacidade.

O princípio da liberdade de expressão, estabelecido no inciso IX do artigo 5º da Constituição Federal, refere-se ao direito de pensar e adotar livremente ideias, bem como de participar da circulação de informações nas redes digitais sem sofrer censura. No entanto, conforme estipulado pela Constituição, o anonimato é vedado, o que implica que esse direito não é absoluto e que o indivíduo pode ser responsabilizado civil ou criminalmente caso exceda os limites estabelecidos para a expressão.

O segundo pilar é a neutralidade de rede, prevista no artigo 9º do Marco Civil da Internet, será detalhadamente analisada em tópico próprio no presente estudo, na medida em que compõe objeto de reflexão deste. No entanto, é possível, desde já, afirmar que este princípio determina que os provedores de internet devem tratar todos os pacotes de dados de maneira equânime, sem discriminação com base no conteúdo, origem, destino ou aplicação dos dados. A neutralidade de rede, um dos aspectos mais controversos durante a discussão do projeto de lei, assegura que os usuários possam acessar qualquer conteúdo na internet sem que os provedores possam interferir na velocidade da navegação ou bloquear o acesso a determinados sites.

Por fim, a privacidade, também garantida pelo artigo 5º da Constituição Federal, é um dos pilares fundamentais do Marco Civil da Internet. Este princípio visa proteger os dados pessoais dos usuários, exigindo seu consentimento expresso para qualquer operação realizada com essas informações. Além disso, a lei prevê a possibilidade de indenização por danos materiais ou morais resultantes de violações à intimidade, comunicações sigilosas e à vida privada dos usuários.

No que se refere aos direitos e garantias dos usuários da internet, o artigo 7º da Lei nº 12.965/14 é enfático ao assegurar a inviolabilidade e o sigilo tanto do fluxo das comunicações quanto das comunicações privadas armazenadas, salvo em casos específicos autorizados por ordem judicial. Este dispositivo legal proporciona uma proteção robusta contra a exposição não autorizada das informações pessoais dos usuários, garantindo que estas só possam ser acessadas em situações excepcionais e devidamente justificadas.

O artigo 10º, § 1º da mesma lei detalha de maneira específica as normas para a proteção dos registros, dados pessoais e comunicações privadas. Ele esclarece que, no caso de requisição judicial, o responsável pela guarda desses dados está legalmente obrigado a disponibilizá-los. Essa obrigação decorre da necessidade de cumprimento de ordens judiciais e é essencial para garantir a eficácia de investigações e procedimentos legais que requerem o acesso a informações privadas.

Ademais, a lei estipula que a recusa em fornecer os dados solicitados por uma ordem judicial pode ter consequências legais severas. Especificamente, se o responsável pela guarda dos dados se negar a atender a uma requisição judicial, ele poderá ser considerado culpado pelo crime de desobediência, conforme previsto no artigo 330 do Código Penal Brasileiro. Tal disposição reforça a importância do cumprimento das ordens judiciais e a seriedade das implicações jurídicas para a não colaboração com o processo judicial.

Esses dispositivos refletem o equilíbrio que o Marco Civil da Internet busca estabelecer entre a proteção dos direitos individuais dos usuários e a necessidade de acesso a informações para fins legais e de segurança pública.

A aplicação rigorosa dessas normas é crucial para assegurar que a privacidade e a segurança dos dados dos usuários sejam mantidas, ao mesmo tempo que as autoridades têm as ferramentas necessárias para realizar investigações e manter a ordem. Segundo Polido e Doneda (2015), "o processo de construção do Marco Civil foi um exemplo notável de participação cidadã e transparência na formulação de políticas públicas no Brasil". A proposta inicial foi apresentada em 2009, e após um extenso debate público, o projeto foi aprovado pelo Congresso Nacional e sancionado pela Presidência da República em abril de 2014.

Como demarcado, o Marco Civil estabelece esses princípios fundamentais como a neutralidade da rede, a privacidade e a proteção de dados pessoais, a liberdade de expressão e a garantia de direitos humanos no ambiente digital. De acordo com Doneda (2014), "o Marco Civil da Internet é uma das legislações mais avançadas do mundo no que diz respeito à regulação da internet, estabelecendo um equilíbrio entre direitos individuais e interesses coletivos". A neutralidade da rede impede práticas discriminatórias, promovendo um ambiente digital competitivo e inovador.

2 AVANÇOS E CONQUISTAS DO MARCO CIVIL DA INTERNET

Apesar de sua publicação em 23 de junho de 2014, o Marco Civil da Internet enfrentou questionamentos quanto a diversos de seus artigos, uma vez que muitas das questões abordadas na lei requeriam regulamentação adicional. Em resposta a essas necessidades, o governo federal editou o Decreto nº 8.771, em 2016, para esclarecer e regulamentar aspectos específicos, como a discriminação de pacotes de dados e a degradação do tráfego, os procedimentos para a guarda e proteção de dados por provedores de conexão e de aplicações, as medidas de transparência nas requisições de dados pela administração pública e os parâmetros para fiscalização e apuração de infrações.

Em relação ao legado do Marco Civil da Internet, é importante destacar que, com sua implementação, o Brasil estabeleceu-se como uma referência global na formulação de princípios fundamentais para uma internet livre e aberta, que garante os direitos dos usuários. O marco legal recebeu elogios de destacadas figuras do contexto digital, incluindo Tim Berners-Lee, criador da World Wide Web (WWW). Além disso, a legislação brasileira inspirou a Declaração Italiana de Direitos da Internet, influenciou as reformas legislativas na França voltadas à inclusão de direitos digitais e foi mencionada pela Suprema Corte da Argentina em uma decisão sobre a responsabilidade dos provedores de busca em relação aos resultados indexados (Ramos, 2021).

Desde sua promulgação e ao longo desses dez anos de vigência, o Marco Civil da Internet trouxe diversos avanços significativos para a regulação digital no Brasil. Um dos principais avanços é a garantia da neutralidade da rede, que impede provedores de internet de discriminar ou priorizar determinados tipos de conteúdo, aplicativos ou serviços. Esta medida assegura um ambiente digital justo e competitivo, promovendo a inovação e a liberdade de escolha dos usuários. a garantia da neutralidade da rede tem sido fundamental para manter a internet como um espaço livre e democrático. Este princípio impede que provedores de serviços de internet (ISPs) favoreçam ou bloqueiem determinados conteúdos, garantindo que todos os usuários tenham igual acesso à informação e aos serviços online. Isso promove um ambiente de inovação, onde novas empresas e ideias podem competir em pé de igualdade com os gigantes estabelecidos.

Outro avanço importante é a proteção da privacidade e dos dados pessoais dos usuários. O Marco Civil estabelece que os dados dos usuários só podem ser coletados, armazenados e utilizados com o consentimento expresso dos mesmos, e que os provedores de internet são responsáveis pela segurança dessas informações. Conforme afirma Bioni (2016), "a proteção de

dados pessoais no Marco Civil da Internet representa um passo crucial para a consolidação de um ambiente digital seguro e confiável". De tal modo que a legislação brasileira é vista como um exemplo global de como equilibrar a proteção dos direitos individuais com a necessidade de segurança e transparência no uso dos dados.

Além disso, o Marco Civil reforça a liberdade de expressão, garantindo que os usuários possam se expressar livremente na internet, sem medo de censura ou retaliação. Esta garantia é essencial para a promoção de uma sociedade democrática e pluralista, onde diversas vozes e opiniões podem ser ouvidas.

3 DESAFIOS PERSISTENTES NA IMPLEMENTAÇÃO DO MARCO CIVIL DA INTERNET E NA IMPLEMENTAÇÃO DA NEUTRALIDADE DA REDE

O fato de o Marco Civil da Internet estar em vigor em nosso país desde 2014 não impediu que em 2021, o Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS) tenha sido alvo de um ataque cibernético significativo, que expôs as vulnerabilidades de sistemas críticos e destacou a importância da proteção de dados pessoais e da segurança online. Este incidente foi um dos mais notáveis no Brasil, refletindo a crescente sofisticação e frequência dos ataques cibernéticos contra instituições públicas e privadas.

O ataque ao TJRS ocorreu em maio de 2021 e foi caracterizado por um *ransomware*, um tipo de malware que criptografa os dados da vítima e exige um resgate para a sua liberação. Os invasores conseguiram acessar e comprometer os sistemas internos do tribunal, afetando severamente a operação de diversos serviços e sistemas judiciais. O *ransomware* utilizado foi uma variação do grupo de malware conhecido como "Conti," que é famoso por suas operações agressivas e pela demanda de resgates elevados.

Em Maio de 2021 o TJRS sofreu um ataque hacker que paralisou as atividades de forma total, num prejuízo mais grave do que a própria pandemia e o trabalho remoto frente a pandemia trouxe, com efeitos que mais de 3 meses depois continuam reverberando para todas as partes envolvidas, seja advocacia, serventuários, cidadãos.

Em Julho de 2021 a polícia apreendeu computadores na casa de um servidor do Tribunal ligado ao setor de informática e afirmam terem localizado indícios de que na casa de uma juíza haveria também a possibilidade de que as invasões ao TJRS tivessem sido originárias destes locais. (Rocha, 2021, p. 01)

O impacto do ataque foi extenso e multifacetado: O TJRS enfrentou uma paralisação significativa de seus serviços digitais, incluindo o sistema de processos judiciais, consultas públicas e outras funções essenciais. Isso gerou atrasos em processos legais e causou transtornos para advogados, partes envolvidas e o público em geral. Embora não tenha sido confirmado que dados sensíveis foram diretamente acessados ou divulgados, a criptografia de arquivos e o bloqueio de sistemas levantaram preocupações sobre a possível exposição de informações pessoais e confidenciais de cidadãos e funcionários.

A recuperação do ataque demandou consideráveis recursos financeiros e humanos. O TJRS precisou investir em serviços de cibersegurança para restaurar seus sistemas e garantir a integridade dos dados, além de revisar e fortalecer suas medidas de segurança. O ataque também afetou a reputação do tribunal, minando a confiança pública na capacidade da instituição de proteger informações sensíveis e garantir a continuidade dos serviços.

Cumprе ressaltar que o incidente com o TJRS sublinha várias questões críticas sobre a proteção de dados pessoais e a segurança online: A ocorrência destaca a importância de investir em medidas de segurança cibernética robustas e atualizadas, incluindo sistemas de defesa contra *ransomware*, criptografia de dados e práticas de segurança contínuas. Também mostrou ser essencial promover a conscientização sobre cibersegurança entre funcionários e usuários. Treinamentos regulares sobre *phishing* e outras ameaças podem ajudar a prevenir ataques. Razão pela qual as instituições precisam desenvolver planos de resposta a incidentes eficazes para minimizar o impacto de ataques e garantir a rápida recuperação dos serviços.

Esse ataque reforça a necessidade de conformidade com leis e regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, que impõe responsabilidades sobre o tratamento e segurança das informações pessoais. E, por outro lado, aponta para a necessidade da colaboração entre organizações e o compartilhamento de informações sobre ameaças que podem melhorar a detecção e a resposta a incidentes cibernéticos.

O ataque ao Tribunal de Justiça do Rio Grande do Sul em 2021 serve como um lembrete contundente da crescente ameaça cibernética enfrentada por instituições públicas e privadas. A proteção de dados pessoais e a segurança online devem ser priorizadas para assegurar a integridade das informações e a continuidade dos serviços essenciais. A experiência adquirida com o incidente oferece lições valiosas para fortalecer a resiliência e a segurança em um ambiente digital cada vez mais complexo e desafiador.

Após 10 anos de sua vigência, a lei tem enfrentado diversos desafios em sua aplicação, gerando debates sobre a necessidade de uma atualização. Um exemplo disso pode-se perceber no que diz respeito ao fato de apesar da evidente clareza do dispositivo do art. 3º, anteriormente referido no presente estudo, persiste a argumentação de que as plataformas digitais apenas seriam responsáveis conforme o disposto no art. 19, que aborda a responsabilidade em relação ao conteúdo publicado pelos usuários. Em outras palavras, observa-se uma negligência na interpretação sistemática das leis, resultando na omissão da aplicação da responsabilidade das plataformas em relação às suas atividades de moderação de conteúdos, como impulsionamento, recomendação, e restrição de alcance de conteúdos e contas. Essa postura tem sido benéfica para essas empresas, mas extremamente prejudicial para a sociedade brasileira em larga escala.

3.1 A questão da neutralidade na rede

Barbosa recorda que a neutralidade de rede foi um dos temas divergentes que dificultou a aprovação da matéria. "Na época, [a neutralidade] foi o tema que gerou maior discordância entre empresas e sociedade civil e pesquisadores naquele momento, porque o Brasil vinha avançando para um modelo de comercialização de serviços de acesso à Internet que poderia chegar num estágio em que você teria pacotes mais baratos, em que o usuário só acessaria, por exemplo, e-mail e redes sociais. Outros pacotes mais caros em que você poderia assistir vídeos", disse a jornalista, que atualmente integra a organização Direito à Comunicação e Democracia (Dira-Com) e é uma das representantes da sociedade civil no Comitê Gestor da Internet no Brasil (CGI.br). (Urupá. 2024, p. 01)

Aqui exsurge com destaque o que prevê o art. 9º do Marco Civil, qual seja o denominado princípio da neutralidade da rede, o qual assegura que os provedores de internet tratem todos os pacotes de dados de forma igualitária, sem distinção por conteúdo, origem, destino, serviço, terminal ou aplicação. O caput do artigo referido assim dispõe: "Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação." Ou seja,

o artigo estabelece que todos os pacotes de dados que transitam pela rede devem receber tratamento isonômico. Isso significa, tecnicamente, que os bits que trafegam pela rede mundial não devem ser discriminados com base em sua origem, destino, conteúdo, terminal ou aplicação, tornando vedadas tais práticas discriminatórias.

Além disso, revela-se pertinente trazer à lume o que está disposto no conteúdo dos incisos I, II, III e IV do parágrafo 2º e 3º do art. 9º, que estabelecem disposições referentes à responsabilidade por práticas de discriminação ou degradação no tráfego da web, a saber:

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no caput deve:

I – abster-se de causar dano aos usuários, na forma do art. 927[1] da Lei no 10.406, de 10 de janeiro de 2002 – Código Civil;

II – agir com proporcionalidade, transparência e isonomia;

III – informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV – oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Em conformidade com o disposto no inciso I do § 2º do art. 9º, que remete ao artigo 927 do Código Civil – Lei 10.406/02, a responsabilidade pela reparação de danos decorrentes de atos ilícitos (arts. 186 e 187) é atribuída àqueles que os causarem. Assim, os dispositivos legais mencionados impedem que os provedores de conexão restrinjam o acesso dos usuários a determinados serviços e garantem que todos os provedores e operadoras de serviços de internet ofereçam pacotes que não discriminem os usuários, especialmente no que se refere ao acesso a sites específicos.

Em termos mais claros, as entidades responsáveis pela prestação de serviços de rede estão proibidas de discriminar os serviços oferecidos aos usuários ou de estabelecer restrições diferenciadas no acesso individual dos usuários. Ou seja, todos os usuários devem gozar de direitos iguais. Assim é possível referir-se à neutralidade da rede como proibição de modificações na velocidade e na qualidade do serviço pelos provedores em relação a conteúdos, destinos de acesso ou ao uso de produtos de concorrentes. Um exemplo disso é a prática de reduzir a velocidade de conexão para programas de Voz sobre IP (VOIP), como o SKYPE. A neutralidade da rede tornou-se uma norma, e qualquer provedor que a viole deverá justificar suas ações.

A neutralidade da rede foi um tema amplamente debatido durante a discussão e aprovação da Lei nº 12.965/14, pois a sua implementação contrariou interesses de grandes organizações nacionais fornecedoras de serviços de Internet. A referida lei legalizou e, consequentemente, burocratizou a prestação desses serviços, mas ao mesmo tempo, assegurou direitos e proteção aos usuários da rede.

Atualmente, considerando a importância da internet na vida cotidiana, a ausência de um Marco Civil da Internet, que estabelecesse os princípios jurídicos fundamentais para o uso da rede, resultaria na falta do princípio da neutralidade da rede e, certamente, tal ausência poderia ter consequências negativas significativas, expondo os usuários a diversos riscos associados à internet. Entre os quais podem ser citados, a título exemplar, ainda que sem a pretensão de esgotar a temática:

- a) Discriminação de Conteúdos: Provedores de serviços poderiam priorizar ou penalizar determinados conteúdos com base em acordos comerciais ou interesses próprios, prejudicando a liberdade de acesso e a diversidade de informações.
- b) Distorção da Competição: Empresas de maior porte poderiam pagar para garantir maior velocidade e visibilidade para seus serviços, desfavorecendo startups e concorrentes menores que não possuem recursos financeiros para competir em termos de velocidade e acesso.
- c) Restrição ao Acesso a Serviços: Usuários poderiam enfrentar limitações no acesso a serviços específicos, como plataformas de comunicação e ferramentas de colaboração, caso tais serviços sejam favorecidos ou prejudicados pelos provedores.
- d) Aumento dos Custos para Usuários: A introdução de diferentes pacotes e tarifas para acessar diferentes tipos de conteúdo e serviços poderia elevar os custos para os usuários, afetando negativamente o acesso à informação e a inclusão digital.
- e) Impacto na Liberdade de Expressão: A possibilidade de provedores limitarem ou priorizarem certos conteúdos pode afetar a liberdade de expressão, limitando a capacidade dos indivíduos de compartilhar e acessar informações de forma equitativa.
- f) Redução da Inovação: A falta de neutralidade pode desencorajar a inovação tecnológica, pois novos serviços e aplicativos podem enfrentar barreiras artificiais impostas por provedores que favorecem concorrentes estabelecidos.
- g) Prejuízo à Privacidade: Provedores poderiam monitorar e manipular o tráfego de dados de acordo com interesses comerciais, comprometendo a privacidade dos usuários e a segurança das informações pessoais.

De todo modo, e apesar dos avanços significativos, é importante demarcar que a implementação da neutralidade da rede no Brasil enfrenta diversos desafios. Um dos principais é a fiscalização eficaz deste princípio. A Agência Nacional de Telecomunicações (Anatel) é a responsável por regulamentar e fiscalizar os ISPs, mas enfrenta dificuldades técnicas e orçamentárias para realizar essa tarefa de forma plena. A complexidade técnica da gestão de tráfego de dados e a falta de recursos adequados dificultam a identificação e punição de práticas que violam a neutralidade da rede.

Um dos principais desafios é a aplicação efetiva da neutralidade da rede. Segundo Rodrigues (2018, p. 60), "a fiscalização e a garantia da neutralidade da rede são tarefas complexas, que exigem uma coordenação eficaz entre diferentes órgãos reguladores e a participação ativa da sociedade civil".

Outro desafio significativo é a proteção da privacidade e dos dados pessoais. Embora o Marco Civil estabeleça diretrizes claras, a implementação prática dessas medidas enfrenta obstáculos, como a falta de recursos e a necessidade de aprimoramento das capacidades técnicas dos órgãos responsáveis pela fiscalização. Além disso, a crescente incidência de crimes cibernéticos e vazamentos de dados exige uma atualização constante das políticas de segurança e proteção de dados.

Há que ser apontado um importante desafio a ser enfrentado consubstanciado pela pressão das grandes empresas de telecomunicações. Esses conglomerados possuem recursos significativos e frequentemente exercem influência política para tentar flexibilizar as regras de neutralidade, alegando que a capacidade de gerenciar o tráfego de dados é essencial para a manutenção de um serviço de alta qualidade. Segundo estudos, em diversos momentos houve tentativas de

lobby para alterar a legislação em favor desses interesses, o que poderia comprometer a igualdade de acesso à internet.

Por fim, a garantia da liberdade de expressão na internet também enfrenta desafios. A disseminação de desinformação e discurso de ódio nas plataformas digitais representa uma ameaça à integridade do ambiente digital. Conforme observa Gagliardi (2020), "é necessário encontrar um equilíbrio entre a proteção da liberdade de expressão e a prevenção de abusos que possam comprometer a harmonia social e a democracia".

Para enfrentar esses desafios, é crucial que o Brasil desenvolva políticas públicas robustas e eficazes. A participação ativa da sociedade civil e de organizações não governamentais é fundamental para garantir que a implementação do Marco Civil continue a proteger os direitos dos usuários. Campanhas de conscientização e educação digital podem ajudar os cidadãos a entenderem seus direitos e a identificarem violações, pressionando por uma internet mais justa e equitativa.

4 A IMPORTÂNCIA DAS POLÍTICAS PÚBLICAS NA REGULAÇÃO DIGITAL

É essencial que o governo e as agências reguladoras invistam em capacidades técnicas e recursos para a fiscalização. A cooperação internacional também pode ser uma ferramenta valiosa, permitindo a troca de experiências e melhores práticas com outros países que enfrentam desafios semelhantes na regulação da neutralidade da rede.

Além do Marco Civil da Internet, diversas outras políticas públicas têm sido desenvolvidas para aprimorar a regulação digital no Brasil. Entre essas iniciativas, destaca-se a Lei Geral de Proteção de Dados (LGPD), que foi sancionada em 2018 e representa um marco significativo na legislação brasileira sobre a proteção de dados pessoais. A LGPD, inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, tem como objetivo central estabelecer normas rigorosas para o tratamento e a proteção de dados pessoais, refletindo uma preocupação crescente com a privacidade dos indivíduos na era digital.

A LGPD cria um conjunto de diretrizes e princípios que regulamentam a coleta, o armazenamento, o processamento e a utilização de dados pessoais. Essas diretrizes visam assegurar que os dados dos cidadãos sejam tratados de forma ética e transparente, garantindo que os indivíduos tenham controle sobre suas próprias informações. A lei exige que as organizações obtenham o consentimento explícito dos titulares de dados antes de processar suas informações, e estabelece a obrigatoriedade de informar claramente sobre a finalidade do uso desses dados.

Além disso, a LGPD institui direitos específicos para os titulares de dados, como o direito à confirmação da existência de tratamento, o direito de acesso às informações, e o direito de correção de dados incompletos, inexatos ou desatualizados. A lei também prevê mecanismos para que os indivíduos possam revogar seu consentimento a qualquer momento e solicitar a exclusão de seus dados pessoais.

Outro aspecto importante da LGPD é a criação da Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e assegurar o cumprimento da legislação. A ANPD tem a competência para aplicar sanções e multas às organizações que não aderirem às normas estabelecidas, além de promover orientações e esclarecimentos sobre a aplicação da lei.

Portanto, a LGPD representa um avanço significativo na proteção dos dados pessoais no Brasil, alinhando-se às melhores práticas internacionais e reforçando o compromisso com a privacidade e a segurança das informações dos cidadãos. Essa legislação complementa e fortalece o Marco Civil da Internet, oferecendo um framework mais robusto para enfrentar os desafios da era digital e garantir a proteção dos direitos dos usuários.

A LGPD impõe obrigações rigorosas às empresas e organizações que coletam e processam dados pessoais, exigindo medidas de segurança adequadas e a obtenção de consentimento claro dos usuários. Bioni (2016) destaca que "a proteção de dados pessoais no Brasil representa um passo crucial para a consolidação de um ambiente digital seguro e confiável" (p. 50).

Para enfrentar os desafios complexos da regulação digital, é essencial que as políticas públicas sejam elaboradas de forma participativa e transparente. Este processo deve envolver ativamente diversos stakeholders, incluindo a sociedade civil, organizações não governamentais (ONGs) e o setor privado, para assegurar que as políticas reflitam as necessidades e preocupações de todos os envolvidos.

A participação ativa da sociedade civil é crucial para a criação de políticas que realmente atendam às demandas da população. Por exemplo, a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil resultou de um processo de consulta pública extensivo, no qual foram coletadas contribuições de cidadãos, especialistas e empresas. Essa abordagem ajudou a moldar uma legislação que equilibrasse a proteção da privacidade com a necessidade de inovação e crescimento econômico. A participação de ONGs, como a Data Privacy Brasil, foi fundamental para garantir que a lei atendesse às preocupações sobre a coleta e o uso de dados pessoais.

Além do mais, o envolvimento do setor privado também é importante para garantir a viabilidade e a aplicabilidade das políticas. Empresas de tecnologia, por exemplo, podem fornecer insights valiosos sobre a implementação prática de regulamentações e colaborar na criação de soluções técnicas que atendam aos requisitos legais. Um exemplo disso é o trabalho conjunto entre plataformas de redes sociais e reguladores para implementar medidas de combate à desinformação e proteger a integridade das eleições. Plataformas como o Facebook e o Twitter têm colaborado com entidades reguladoras para desenvolver e aprimorar políticas que abordem a disseminação de informações falsas e o impacto na opinião pública.

Campanhas de conscientização e educação digital são ferramentas eficazes para empoderar os cidadãos e promover uma internet mais justa e equitativa. Essas campanhas ajudam os usuários a entenderem seus direitos e a reconhecerem possíveis violações, além de fornecerem informações sobre como agir em casos de abuso. Por exemplo, iniciativas como o "Safer Internet Day" promovem a educação sobre segurança online e proteção de dados pessoais, incentivando o engajamento dos usuários em práticas seguras e responsáveis na internet.

Essas ações coletivas são essenciais para a construção de um ambiente digital que respeite os direitos dos indivíduos e promova a justiça social. A formulação de políticas públicas eficazes depende de uma colaboração contínua e transparente entre todos os stakeholders, garantindo que as regulamentações sejam justas, aplicáveis e adaptadas às necessidades reais da sociedade.

A cooperação internacional é essencial para aprimorar as políticas de regulação digital, e a troca de experiências e melhores práticas entre países desempenha um papel fundamental nesse processo. Ao colaborar com organismos internacionais e adotar padrões globais, o Brasil pode fortalecer a proteção dos direitos dos usuários e criar um ambiente digital mais seguro e eficiente.

Um exemplo notável dessa cooperação é a participação do Brasil no Grupo de Trabalho sobre Governança da Internet da OCDE. Através desse grupo, o Brasil tem acesso a diretrizes e práticas recomendadas por países que lideram a regulação digital, como os membros da União

Europeia e os Estados Unidos. A troca de experiências com essas nações permite que o Brasil adote abordagens comprovadas para questões como a proteção de dados pessoais e a segurança cibernética. Por exemplo, a experiência da União Europeia com o Regulamento Geral sobre a Proteção de Dados (GDPR) tem sido uma referência crucial para a Lei Geral de Proteção de Dados (LGPD) do Brasil, que incorporou muitos dos princípios e práticas do GDPR para assegurar um padrão elevado de proteção de dados.

Outro exemplo é a colaboração do Brasil com a Comissão Internacional de Proteção de Dados (ICDP) e a Rede Internacional de Autoridades de Proteção de Dados e Privacidade (IDP). Essas organizações oferecem um fórum para discutir desafios globais e compartilhar soluções em matéria de proteção de dados. Através dessa rede, o Brasil tem participado de debates sobre a implementação de mecanismos de conformidade e fiscalização, beneficiando-se das experiências de outros países que já enfrentaram desafios semelhantes (ANPD, 2022).

Além disso, a cooperação internacional também é evidenciada pelo envolvimento do Brasil em iniciativas globais contra a desinformação e o discurso de ódio online. A participação em fóruns internacionais, como o Fórum Global sobre Segurança Cibernética e o Fórum de Governança da Internet da ONU, permite ao Brasil colaborar com outras nações para desenvolver estratégias eficazes de combate a ameaças digitais. Por exemplo, a colaboração com países da União Europeia na criação de diretrizes para o combate à desinformação ajudou o Brasil a desenvolver políticas mais robustas e alinhadas com padrões globais.

Essas experiências demonstram que a cooperação internacional não apenas facilita o acesso a melhores práticas e soluções inovadoras, mas também contribui para a criação de um ambiente digital mais seguro e justo. Através do intercâmbio de conhecimentos e da adoção de padrões globais, o Brasil pode aprimorar suas políticas de regulação digital e proteger efetivamente os direitos dos usuários.

CONCLUSÃO

Caminha-se para a conclusão do presente ensaio no qual buscou-se demonstrar em que medida o Marco Civil da Internet no Brasil representa um marco significativo na regulação digital, especialmente no que se refere à neutralidade da rede. Ao longo do texto foi possível perceber que essa normativa, sancionada em 2014, estabelece princípios fundamentais para a utilização da internet, como a liberdade de expressão, a privacidade dos usuários e a neutralidade da rede, que garante que todos os dados trafeguem pela mesma rede sem discriminação. No entanto, a implementação e a efetividade desses princípios enfrentam desafios consideráveis que exigem uma atuação contínua e integrada de diversos setores da sociedade.

O avanço promovido pelo Marco Civil da Internet é evidente, mas não é isento de dificuldades. A sua implementação bem-sucedida depende da coordenação entre políticas públicas eficazes, uma fiscalização rigorosa e a participação ativa dos cidadãos. Sem esses elementos, a promessa de uma internet livre, aberta e inclusiva pode ser comprometida. Para garantir que a internet continue a ser um espaço de igualdade de acesso e inovação, é crucial que o Brasil mantenha um compromisso sólido com a regulação digital.

A importância das políticas públicas na regulação digital é inegável. O Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, representam avanços significativos na proteção dos direitos dos usuários e na promoção de um ambiente digital justo e democrático. A LGPD, inspirada pelo Regulamento Geral sobre a Proteção de Dados (GDPR)

da União Europeia, estabelece diretrizes rigorosas para o tratamento e proteção de dados pessoais. Essas leis são essenciais para proteger a privacidade dos usuários e garantir que suas informações sejam utilizadas de forma transparente e ética.

Por outro lado, a implementação dessas políticas enfrenta vários desafios. Por exemplo, o Marco Civil da Internet enfrenta dificuldades na aplicação efetiva de princípios como a neutralidade da rede e a proteção de dados pessoais, especialmente com a rápida evolução da tecnologia e a crescente complexidade das plataformas digitais. A fiscalização das práticas de coleta e uso de dados, bem como a proteção contra abusos e a promoção da transparência, requerem esforços contínuos e atualizações regulares das diretrizes.

A participação social desempenha um papel crucial na regulação digital. A colaboração ativa de cidadãos, organizações não governamentais e do setor privado é essencial para garantir que as políticas atendam às necessidades e preocupações de todos os stakeholders. Campanhas de conscientização e educação digital ajudam a empoderar os cidadãos, permitindo-lhes compreender seus direitos e identificar possíveis violações. Por exemplo, a iniciativa "*Safer Internet Day*" promove a educação sobre segurança online e proteção de dados pessoais, incentivando práticas responsáveis e seguras entre os usuários da internet.

Além da participação nacional, a cooperação internacional é vital para aprimorar as políticas de regulação digital. A troca de experiências e melhores práticas com outros países pode fornecer insights valiosos e ajudar o Brasil a adotar abordagens mais eficazes. A participação em fóruns internacionais, como o Fórum Global sobre Segurança Cibernética e o Fórum de Governança da Internet da ONU, permite ao Brasil colaborar com outras nações para desenvolver estratégias globais de proteção de dados e combate à desinformação. A experiência internacional, como a implementação do GDPR na União Europeia, oferece lições importantes que podem ser adaptadas às necessidades brasileiras.

A atualização constante das diretrizes e a melhoria das capacidades técnicas e de fiscalização são fundamentais para enfrentar os desafios emergentes. As rápidas inovações tecnológicas e o surgimento de novas ameaças digitais exigem que as políticas de regulação digital sejam adaptáveis e responsivas. O aprimoramento contínuo das práticas de fiscalização, bem como a integração de novas tecnologias e metodologias, é essencial para garantir que a proteção dos direitos digitais seja eficaz e abrangente.

Finalmente, para assegurar uma internet que seja livre, aberta e inclusiva, é essencial fortalecer as políticas públicas e promover a cooperação entre governo, sociedade civil e setor privado. A integração dessas partes interessadas, aliada à atualização constante das diretrizes e à melhoria das capacidades de fiscalização, permitirá ao Brasil enfrentar os desafios emergentes e garantir a proteção dos direitos digitais de forma justa e eficaz. Com esses esforços coordenados, o Brasil pode continuar a servir como um exemplo global de regulação digital justa e democrática.

REFERÊNCIAS

ANPD. **Participação da ANPD no cenário internacional e a regulamentação de transferências internacionais de dados pessoais**. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/asuntos/semana-da-protexao-de-dados-2022/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais>. Acesso em 30 jun. 2024.

BIONI, B. Proteção de Dados Pessoais: A Função e os Limites do Consentimento. In: **Revista Brasileira de Direito das Telecomunicações**, 8(2), 45-67. 2016

BRASIL. **Marco Civil da Internet**. Lei 12.965 de 23 de abril de 2014. Diário Oficial da União. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em 11 de abril de 2024.

BRASIL. **Lei nº 11.419**, de 19 de dezembro de 2006. Código Civil. Diário Oficial da União. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/111419.htm>. Acesso em 29 junho de 2024.

DONEDA, D. O Marco Civil da Internet e a Proteção dos Dados Pessoais. In: **Revista de Direito Constitucional e Internacional**, 22(88), 2014, 120-140.

GAGLIARDI, A. Desinformação e Discurso de Ódio na Internet: Desafios para a Regulação Digital. In: **Revista Brasileira de Estudos Políticos**, 15(1), 2020, pp.90-112.

POLIDO, F., & DONEDA, D. O Processo de Construção do Marco Civil da Internet: Participação Cidadã e Transparência. In: **Revista Direito GV**, 11(2), 2015, pp. 385-406.

RAMOS, Rahellen. **O que é o Marco Civil da Internet?** 2021, Disponível em: <https://www.politize.com.br/marco-civil-da-internet/>. Acesso em: 20 jun 2024;

RODRIGUES, C. Neutralidade da Rede no Brasil: Avanços e Desafios na Implementação do Marco Civil da Internet. In: **Revista de Direito e Tecnologia**, 9(1), 2018, 55-78.

ROCHA, Gustavo. **Ataque hacker ao Tribunal de Justiça do Rio Grande do Sul – TJRS: Efeitos eternos?** Disponível em: usbrasil.com.br/artigos/ataque-hacker-ao-tribunal-de-justica-do-rio-grande-do-sul-tjrs-efeitos-eternos/1268417383. Acesso em 10 jul 2024.

URUPÁ, Marcos. **Dez anos depois, Marco Civil da Internet ainda enfrenta desafios para ser cumprido**. 2024. Disponível em: <https://teletime.com.br/23/04/2024/depois-anos-depois-marco-civil-da-internet-ainda-passa-por-desafios-para-ser-cumprido/>. Acesso em 30 jun. 2024.