INTERNET IMPACT BRIEF

Abril 2024

Propostas para regulamentar plataformas digitais no Brasil: potenciais impactos para a Internet

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

Internet Society
Capítulo Brasil

FICHA TÉCNICA

CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

CEPI FGV Direito SP

Coordenação

Alexandre Pacheco da Silva

Marina Feferbaum

Líder de projeto

Ana Paula Camelo

Pesquisadoras

Ana Carolina Rodrigues Dias Silveira

Ana Paula Camelo

Beatriz Yuriko Schimitt Katano

Saiba mais: http://bit.ly/cepidireitosp

INTERNET SOCIETY CAPÍTULO BRASIL

ISOC Brasil

Presidente

Flavio Rech Wagner

Vice-Presidente

Raquel Fortes Gatto

Diretor de Projetos

Pedro de Perdigão Lana

Saiba mais: https://isoc.org.br/

COMO CITAR

CAMELO, Ana Paula et al. *Internet Impact Brief.* Propostas para regulamentar plataformas digitais no Brasil: potenciais impactos para a internet. São Paulo: CEPI FGV DIREITO SP; ISOC Brasil, 2024.

Internet impact brief [recurso eletrônico] : propostas para regulamentar plataformas digitais no Brasil : potenciais impactos para a internet / Ana Paula Camelo ... [et al.]. - São Paulo : FGV Direito SP, 2024.
23 p.

Inclui bibliografia.
ISBN: 978-65-87355-56-6

1. Internet. 2. Plataformas digitais. 3. Direito regulatório. I. Camelo, Ana Paula. II. Silveira, Ana Carolina Rodrigues Dias. III. Katano, Beatriz Yuriko Schimitt. IV. Silva, Alexandre Pacheco da. V. Wagner, Flavio Rech. VI. Lana, Pedro de Perdigão. VII. Gatto, Raquel Fortes. VIII. Fundação Getulio Vargas.

CDU 004.738.5

Ficha catalográfica elaborada por: Cristiane de Oliveira CRB SP-008061/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

INTERNET IMPACT BRIEF

PROPOSTAS PARA REGULAMENTAR PLATAFORMAS DIGITAIS NO BRASIL: POTENCIAIS IMPACTOS PARA A INTERNET

AUTORES

Ana Carolina Rodrigues Dias Silveira; Ana Paula Camelo; Beatriz Yuriko Schimitt Katano (CEPI FGV Direito SP)

Flávio Rech Wagner; Pedro de Perdigão Lana; Raquel Fortes Gatto (ISOC Brasil)

Versão 1.0, 22 de abril de 2024.

RESUMO

Este *Internet Impact Brief* analisa o projeto de lei PL 2630/2020 sob a perspectiva da soberania digital utilizando o *Internet Impact Assessment Toolki*t e o framework do Modo Internet de Interconectividade ("*Internet Way of Networking*"), ambos da Internet Society, para examinar como esta proposta legislativa brasileira pode afetar a Internet em suas características e estruturas fundantes.

SUMÁRIO

I – APRESENTAÇÃO

Neste *Internet Impact Brief* (IIB) aprofunda-se a discussão sobre a regulação de plataformas no contexto brasileiro e possíveis impactos sobre a estrutura da Internet, a partir da perspectiva da soberania digital. Para tanto, analisa-se o Projeto de Lei nº 2630/2020 (PL 2630)[i] e os riscos que a proposta legal representa para uma Internet aberta, globalmente conectada, segura e confiável. A iniciativa deste *Impact Brief* visa contribuir com o debate público sobre os temas da soberania digital e da regulação de plataformas, que têm ocupado as agendas política, legislativa e acadêmica de modo crescente nos últimos anos no Brasil. Em complemento, objetiva-se fomentar o diálogo informado e contribuir para o desenho e a implementação de instrumentos eficientes e responsáveis no âmbito das políticas relacionadas à Internet. Os principais riscos da proposta de lei discutidos neste documento residem na fragmentação da experiência do usuário, no vigilantismo e em ameaças à governança colaborativa e multissetorial, entre outros.

II – METODOLOGIA

A análise dos potenciais impactos do PL 2630/2020 está fundamentada na aplicação do *framework* das propriedades críticas[ii] e outros elementos constitutivos da Internet, desenvolvido pela *Internet Society*, e integra um esforço acadêmico[1] maior de mapeamento e discussão das narrativas em torno do conceito de soberania digital no Brasil e seus desdobramentos, explorando suas dimensões sociotécnicas, políticas e legais no que tange à infraestrutura e ao funcionamento da Internet. Para tanto, utiliza-se o *Internet Impact Assessment Toolkit*[iii], para examinar como o referido projeto de lei pode afetar a Internet em suas características e estruturas fundantes.

[1] O projeto de pesquisa "Soberania digital: para quê e para quem? Análise conceitual e política do conceito a partir do contexto brasileiro" é fruto da parceria entre ISOC Brasil e Centro de Ensino e Pesquisa em Inovação (CEPI) – FGV Direito SP. Para saber mais, acesse o relatório completo da pesquisa clicando aqui https://bit.ly/cepisoberania. A presente pesquisa mapeou a produção legislativa brasileira, buscando identificar propostas que se conectassem com o debate sobre soberania digital. Observou-se que a maioria dos projetos legislativos não faz menção expressa ao tema, mas repercute aspectos relacionados a ele, tais como necessidade de desenvolvimento tecnológico próprio; regulação local e exercício do poder de jurisdição; proteção dos direitos dos usuários; proteção das instituições e do processo democrático, entre outros. Dentre os 36 projetos mapeados e analisados, a escolha pelo PL 2630/2020 se deu pela associação direta ao debate da soberania digital. No entanto, não se pode deixar de chamar a atenção também para o PL 2768/2022, que trata da regulação das plataformas digitais, um dos temas mais relevantes atualmente nas discussões sobre o exercício da soberania digital, tendo em vista o alcance e o poder econômico adquirido pelas *big techs*, em oposição ao poder estatal, e para o PL 4723/2020, que determina a preservação no país de dados pessoais e dá outras providências.

Os habilitadores “Desenvolvimento colaborativo, gestão e governança”, “Acessibilidade irrestrita”, “Confidencialidade de dados de informações, dispositivos e aplicativos”, “Responsabilidade” (*accountability*) e “Privacidade” foram relacionados a dimensões de soberania e discutidos a partir de potenciais impactos prejudiciais a uma Internet aberta, globalmente conectada, segura e confiável.

III – CONTEXTO

PL 2630/2020

O PL 2630/2020 propõe a regulamentação de plataformas digitais no país, estabelecendo regras de moderação de conteúdo nas redes sociais e serviços de mensageria, e altera o regime de responsabilidade das plataformas.

De forma abrangente, tal proposta legislativa ganhou destaque em função de seu foco na moderação de conteúdo e na responsabilidade dos intermediários. Por meio dela, o Congresso brasileiro visa criar a “Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet”, com o intuito de fomentar um ambiente digital que proteja os cidadãos e assegure direitos. A ênfase em questões relacionadas ao combate à desinformação e aos discursos de ódio levou o PL 2630/2020 a ser conhecido como “PL das *fake news*”, sob o argumento de limitar o poder das plataformas digitais e empoderar a sociedade. Transparência e controle do usuário sobre a moderação de conteúdos realizados pelas plataformas se destacam como eixos orientadores do projeto de lei e situam o debate brasileiro em um contexto mais amplo de tentativas de regulamentação do ambiente digital, também localizado em outros países.

O projeto de lei pretende estabelecer normas e mecanismos de transparência para provedores de redes sociais, de ferramentas de busca e de mensageria instantânea, assim como diretrizes para seu uso. Também propõe a instituição de um “devido processo” em relação à moderação de conteúdo, dispondo sobre a garantia do direito à notificação, ao contraditório e à ampla defesa dos usuários. Já entre seus princípios, prevê a proteção aos direitos constitucionais de liberdade de expressão e de manifestação artística, intelectual e cultural.

A motivação do PL 2630/2020 materializa uma pressão regulatória que emerge como reflexo de uma crise de confiança nas redes, impulsionada pela difusão de discursos de ódio e de conteúdos desinformativos, vistos como ameaças a direitos e riscos à ordem democrática. Alegações de que as plataformas digitais operam de forma predatória e nociva se somam aos argumentos de necessidade de atuação a favor da soberania brasileira.

QUADRO 1 – Síntese de alguns dos principais aspectos em disputa em torno do PL 2630/2020	
Pontos de maior consenso	***Pontos mais controversos***
a) Obrigações de transparência (incluindo relatórios periódicos e abertura de informações para pesquisa); b) Termos e políticas em português e adequados à legislação brasileira; c) Direito ao contraditório e à ampla defesa diante da remoção de conteúdo e/ou outras medidas relacionadas à moderação do conteúdo; e d) Promoção da educação digital para o uso seguro, consciente e responsável da Internet.	a) Imunidade a agentes políticos, com disposições que inibem a ação dos provedores; b) Inclusão de disposições sobre remuneração de conteúdos jornalísticos e de direitos autorais, questões incorporadas de outros debates legislativos; c) Alteração do regime de responsabilidade das plataformas; d) Riscos à privacidade; e) Indefinição sobre os arranjos institucionais em torno da regulamentação, fiscalização e aplicação da lei.

Fonte: elaborado pelos autores.

Atualmente, o PL 2630/2020 encontra-se em tramitação na Câmara dos Deputados, onde o texto sofreu alterações significativas e importantes avanços em termos técnicos e jurídicos. Contudo, ainda remanescem aspectos controversos e que merecem atenção. Em abril de 2024, o Presidente da Câmara comunicou a criação de um grupo de trabalho para discutir a matéria, gerando incerteza sobre o futuro da pauta.

Soberania digital dentro e fora do Legislativo

A relação entre o conteúdo da proposta legislativa e o tema da soberania digital de maneira abrangente é explícita e central em alguns debates sobre o texto que ainda está em tramitação, enfatizando-se a "necessidade de termos uma legislação para definir parâmetros e obrigações bastante claros para a operação destas plataformas digitais no Brasil", e como forma de o país não depender ou ficar sujeito desproporcionalmente a regras estabelecidas por empresas privadas, de acordo com avaliação da coordenadora do CGI.br, Renata Mielli[iv]. A inexistência de uma regulação local, brasileira, sobre a matéria é vista como uma vulnerabilidade crítica, e o PL 2630/2020 se apresenta como um instrumento estratégico para tratar da matéria com base na realidade e nas necessidades do país, reforçando os poderes de autoridades locais no exercício desse controle regulatório.

É importante pontuar que esse debate não se dá a partir de um entendimento único e consensual de soberania. Diferentes abordagens e narrativas coexistem e se co-produzem no debate do projeto de lei. No contexto brasileiro foi possível identificar perspectivas que coexistem e propõem (às vezes de forma contraditória)[2]: (i) o aumento da autoridade por parte do Estado e de suas instituições; (ii) o fomento a um ambiente mais seguro e saudável; e/ou (iii) a capacidade de garantir e/ou ampliar direitos de cidadãos. Esses itens, que foram também identificados no PL 2630/2020 e/ou nas narrativas atreladas a ele, são detalhados no Quadro 2.

QUADRO 2 – Perspectivas/objetivos de soberania digital mapeados no contexto brasileiro

Segurança nacional e capacidade de fazer cumprir as leis	***Autodeterminação econômica***
○ Combate a ameaças à segurança nacional (ciberataques estrangeiros e vulnerabilidades online); ○ Garantia do domínio digital dentro de fronteiras por meio da capacidade de estabelecer e fazer cumprir leis em seu território (desde infraestruturas críticas até o uso de tecnologias da Internet em processos políticos e mudanças); ○ Acesso legal à informação por parte de agências de aplicação da lei, autoridades de concorrência e outros reguladores; controle de dados localmente; ○ Influência no funcionamento e operação de serviços e softwares em seu território.	○ Fortalecimento do desenvolvimento da indústria local para competição em ambientes dominados por empresas de tecnologia estrangeiras; ○ Medidas protecionistas fortes que fomentem forças de mercado visando a um ambiente mais equilibrado.
Proteção de direitos e capacitação de cidadãos/usuários e comunidades	***Defesa de normas e valores sociais***
○ Fortalecimento da autonomia individual e coletiva em relação às plataformas tecnológicas;	○ Preservação e/ou incentivo a determinadas normas e tradições locais para a

[2] O detalhamento das narrativas locais em torno do conceito de soberania digital está disponível no relatório de pesquisa do projeto "Soberania digital: para quê e para quem? Análise conceitual e política do conceito a partir do contexto brasileiro" https://hdl.handle.net/10438/35312 (2024).

○ Empoderamento dos cidadãos e comunidades para adotar medidas e tomar decisões relacionadas aos seus dados e atividades digitais.	promoção de valores sociais, culturais e políticos de terceiros; ○ Política de localização de dados para afirmar os direitos dos cidadãos sobre seus dados e medidas de segurança e privacidade contra dados armazenados no exterior; ○ Política de localização de dados para subsidiar a atuação de atores de inteligência e agências de aplicação da lei.

Fonte: baseado em "*Navigating digital sovereignty and its impact on the Internet*" (ISOC, 2022)[v].

No Brasil, o debate sobre soberania digital ganhou projeção em diferentes espaços e contextos, para além da esfera governamental. Um exemplo disso é a crescente incidência do tema em fóruns multissetoriais sobre governança da Internet, como é o caso do Fórum da Internet no Brasil (FIB), onde diferentes vozes e perspectivas (governamentais, do terceiro setor, da comunidade acadêmica e empresarial) têm repercutido as oportunidades e desafios da soberania digital no país[3].

Deve-se destacar ainda a realização de uma Consulta Pública por parte do Comitê Gestor da Internet (CGI) em 2023 a respeito da regulação de plataformas digitais, cujo objetivo foi mapear diferentes tipologias de plataformas digitais, identificar riscos associados ao uso das plataformas, apontar medidas regulatórias capazes de amenizar tais riscos e também identificar os atores e caminhos possíveis para a regulação[vi] a partir de um debate multissetorial. Dentre os eixos norteadores da consulta, destaca-se o "Grupo de riscos – Riscos relacionados a ameaças à soberania digital e ao desenvolvimento tecnológico", que mobilizou debates e contribuições em torno da "capacidade de o país proteger e desenvolver sua infraestrutura digital autonomamente e garantir a proteção de dados pessoais e estratégicos de seus cidadãos" por meio (i) do controle do Estado em relação às diferentes camadas do ambiente digital e em relação à segurança nacional e fluxo de dados; (ii) do desenvolvimento de tecnologias locais, para reduzir a dependência relacionada a empresas estrangeiras; (iii)

[3] É possível localizar submissões de *workshops* dedicadas à soberania digital no Fórum da Internet no Brasil desde sua 11ª edição, o que indica um aumento importante na iniciativa multissetorial sobre o assunto, que até então se mostrava menos estruturada. No ano de 2023, o fórum contou com dois *workshops* sobre soberania digital, além de uma sessão principal e de um painel durante o Encontro Anual da ISOC Brasil, sem mencionar outros espaços informais de discussão dessa temática durante o evento. A edição de 2024 contará com três *workshops* dedicados exclusivamente ao tema.

da autonomia e autodeterminação de indivíduos, possibilitando às pessoas tomarem as próprias decisões sobre o que é feito com suas informações[vii].

No âmbito das atividades legislativas, foram realizadas audiências[viii] e debates públicos[ix] com especialistas que abordaram, dentre diversas questões, a "dificuldade do exercício da soberania devido à natureza global da internet", tal qual mencionada no parecer proferido em plenário ao PL 2630/2020 em 27 de abril de 2023.

Não menos importante, destaca-se também a Carta Soberania Digital[x], endereçada a Luiz Inácio Lula da Silva, então candidato à Presidência da República, e assinada por pesquisadores, professores e ativistas de todo o país. No cerne desse documento estava a crítica ao modelo de concentração de mercado representado pelas *big techs* e a demanda pelo desenvolvimento de uma infraestrutura tecnológica nacional.

O debate em torno da soberania digital também está presente no Judiciário, onde têm sido discutidas muitas matérias relacionadas ao funcionamento da Internet e das tecnologias digitais (e.g., responsabilização das plataformas, transferência internacional de dados etc.), que acabam afetando o poder de jurisdição nacional. No Supremo Tribunal Federal (STF), chama a atenção a Ação Declaratória de Constitucionalidade (ADC) nº 51[xi], que declarou a constitucionalidade do Acordo de Assistência Judiciária em Matéria Penal (MLAT, na sigla em inglês) para solicitação de informações diretamente às plataformas e provedores de Internet estrangeiros com sede ou representação no Brasil (já transitada em julgado). Outros destaques são os recursos extraordinários[4] que discutem a constitucionalidade do art. 19[5] do Marco Civil da Internet (Lei nº 12.965/2014[xii]) e a necessidade de intervenção do Poder Judiciário como requisito para a responsabilização de provedores de aplicações por conteúdo gerado pelos usuários (ainda em julgamento).

O Tribunal Superior Eleitoral (TSE) também tem se inserido nesse debate, por meio de medidas que buscam proteger o processo eleitoral das ameaças oferecidas pelo mau uso das redes, questão central no debate acerca da regulação das plataformas digitais no Brasil. Enquanto o STF discute a constitucionalidade do atual regime de responsabilidade dos intermediários e o Congresso não chega a um consenso sobre

[4] A saber, o Recurso Extraordinário nº 1037396/SP e o Recurso Extraordinário nº 1057258/MG.

[5] O art. 19 do MCI determina que “o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário”, visando assegurar a liberdade de expressão e impedir a censura em função da norma.

as balizas regulatórias, o TSE já responsabiliza os provedores por conteúdos desinformativos em período eleitoral por meio da Resolução nº 23.610/2019. Em março de 2024, o Tribunal promoveu alterações na Resolução, incluindo a regulamentação de conteúdos produzidos por meio de Inteligência Artificial.

IV – ANÁLISE DO IMPACTO DO PL 2630/2020 SOBRE AS PROPRIEDADES FUNDAMENTAIS DA INTERNET SOB A PERSPECTIVA DA SOBERANIA DIGITAL

Nesta seção analisa-se o projeto legislativo objeto deste relatório com vistas a compreender de que maneira ele poderia impactar as propriedades e demais elementos constitutivos do Modo Internet de Interconectividade, do inglês "*Internet Way of Networking*" (IWN), sob a lente da soberania digital.

O IWN é um modelo proposto pela *Internet Society* para descrever o que torna a Internet "a Internet"[xiii], não apenas como uma rede complexa, diversa e dinâmica, mas também uma rede aberta, globalmente conectada, segura e confiável. Esse modelo é definido por um conjunto de "propriedades críticas" e "elementos habilitadores" que sustentam o crescimento e a adaptabilidade da "rede das redes"[xiv].

A análise baseada nas versões públicas mais recentes do PL 2630/2020, pela lente da soberania digital, identificou possíveis impactos sobre as propriedades críticas e sobre alguns elementos habilitadores, conforme descrito a seguir.

Propriedades críticas

De acordo com o *framework* do IWN, o modo de rede da Internet é constituído a partir de cinco propriedades críticas necessárias para a estrutura e o funcionamento da Internet. São elas: (1) uma infraestrutura acessível com um protocolo comum; (2) uma arquitetura aberta de blocos de construção interoperáveis e reutilizáveis; (3) gestão descentralizada e um único sistema de roteamento distribuído; (4) identificadores globais comuns; e (5) uma rede tecnologicamente neutra e de uso geral.

Para fins deste *Impact Brief*, não foram identificados impactos nas propriedades críticas a partir do recorte desta análise. Dedicou-se especial atenção aos impactos sobre os habilitadores ("*enablers"*) que dão suporte a uma Internet aberta, globalmente conectada, segura e confiável.

Habilitadores de uma Internet aberta, globalmente conectada, segura e confiável

Os habilitadores[xv] podem funcionar como ferramentas de análise dos efeitos potenciais que determinadas mudanças legislativas podem implicar, afetando em última instância os objetivos almejados.

Para fins deste *Impact Brief*, identificaram-se potenciais impactos do PL 2630/2020 aos habilitadores descritos no Quadro 3 e detalhados na sequência.

QUADRO 3 – Síntese analítica: PL 2630/2020, habilitadores e perspectivas de soberania

Objetivo	***Habilitador***	***Perspectivas de soberania***	***Impactos***
Internet aberta	Desenvolvimento colaborativo, gestão e governança	Segurança nacional e capacidade de fazer cumprir as leis: governos que desejam controlar como as operações e recursos da Internet são executados (i.e., poder de regulação).	- Estrutura institucional de regulação, controle e fiscalização - Centralização da governança - Ameaça ao modelo de governança multissetorial
Internet globalmente conectada	Acessibilidade irrestrita	Segurança nacional e capacidade de fazer cumprir as leis: governos que desejam controlar como as operações e recursos da Internet são executados (i.e., poder de regulação/jurisdição).	- Regulação local (regras específicas de moderação de conteúdo e outras obrigações) - Risco de fragmentação da “experiência do usuário”
Internet segura	Confidencialidade de dados de informações, dispositivos e aplicativos	Segurança nacional e capacidade de fazer cumprir as leis: (i) governos que desejam controlar como as operações e recursos da Internet são executados; (ii) aumentar o poder do Estado e o acesso aos dados (i.e., poder de jurisdição).	- Soberania estatal x soberania individual (soberania informacional + autodeterminação de dados) - Segurança
Internet confiável	Responsabilidade	Proteção de direitos e capacitação de cidadãos/usuários e comunidades: autonomia dos	- Autonomia na tomada de decisões - Direitos humanos digitais

		cidadãos sobre suas interações com dispositivos, plataformas e o modo como gerenciam seus dados.	- Liberdade de expressão no espaço digital, especialmente em relação ao controle de seus dados
	Privacidade	Proteção de direitos e capacitação de cidadãos/usuários e comunidades: autonomia dos cidadãos sobre suas interações com dispositivos, plataformas e o modo como gerenciam seus dados.	- Autonomia na tomada de decisões - Controle de dados - Direitos humanos no mundo digital - Privacidade - Liberdade de expressão no espaço digital, especialmente em relação ao controle de seus dados

Fonte: baseado em: "Contribuição do capítulo brasileiro da *Internet Society* ao processo de desenvolvimento de política "habilitadores de uma Internet aberta, globalmente conectada, segura e confiável" (ISOC Brasil)[6]

Apoio a uma Internet aberta: Colaboratividade no desenvolvimento, na gestão e na governança

A análise do desenvolvimento, gestão e governança da Internet sob uma perspectiva colaborativa, características essenciais de suporte a uma Internet aberta, permite identificar no PL 2630/2020 uma das dimensões da soberania digital, qual seja: a capacidade de o Estado fazer cumprir suas próprias leis, que se relaciona diretamente com a questão da jurisdição. O debate em torno da estrutura institucional responsável pelo *enforcement* da lei pode vir a ter um significativo impacto sobre o modelo de governança da Internet no Brasil.

Historicamente, o Brasil adotou um modelo multissetorial de governança da Internet. Assim como em muitos outros países, houve uma separação entre a regulação das operadoras de telecomunicações e a regulação da Internet (cf. Norma 04/95 da ANATEL e art. 61 da Lei Geral de Telecomunicações – Lei nº 9.472/97). Também o Comitê Gestor da Internet no Brasil (CGI.br) foi criado nesse contexto, contando com representantes de diferentes setores em sua composição (setor público, setor empre-

sarial, terceiro setor e comunidade científica e tecnológica). Tem vigorado, desde então, uma lógica que privilegia as ideias de "*permissionless innovation*"[7] e autorregulação[8]. Contudo, tem havido uma crescente pressão pela regulação dos provedores de aplicação, diante das externalidades negativas causadas especialmente pelas redes sociais (tais como a disseminação de desinformação e de discursos de ódio).

A regulação é uma forma de os países exercerem a soberania digital. Muitos governos enfrentam dificuldades para exercer autoridade sobre ativos e serviços digitais que operam ou são disponibilizados localmente – muitas vezes por meio de empresas multinacionais estrangeiras – e querem reafirmar sua capacidade de definir e aplicar leis em seu território[xvi]. Com as propostas de regulação, surge também a discussão em torno da criação de uma arquitetura institucional que desempenhe o papel de controle e fiscalização.

O PL 2630/2020 ainda carece de uma definição em relação à estrutura institucional para promover a regulamentação (i.e., o estabelecimento de diretrizes, normas, padrões técnicos etc.) e a supervisão do *enforcement* da norma. Às vésperas da votação, em abril de 2023, o relator removeu da proposta legislativa a figura da chamada "Entidade Autônoma de Supervisão". Essa indefinição causa insegurança jurídica, inclusive porque há vários dispositivos do projeto de lei que dependerão de regulamentação posterior e, a depender de como for feita, pode haver ou não impactos negativos na estrutura da Internet. Em última instância, essas omissões legislativas poderão ser judicializadas, restando aos juízes decidirem discricionariamente, um risco que se amplifica diante do enorme volume de conteúdos sujeitos à moderação diariamente.

Uma das propostas para preencher a lacuna institucional mencionada seria delegar esses poderes a uma autoridade central estatal, a exemplo da Agência Nacional de Telecomunicações (ANATEL), o que já foi incorporado a outros projetos de lei. A ANATEL é a autarquia federal brasileira responsável por regular e fiscalizar o setor de telecomunicações no país. Alguns modelos têm sido discutidos nesse sentido, paralelamente à tramitação do PL 2630/2020. É o caso, por exemplo, do PL 2768/2022,

[7] O princípio da "*permissionless innovation*" (i.e., "inovação sem barreiras – tradução livre") tem sido uma das bases do desenvolvimento de uma Internet aberta. Ele pressupõe a capacidade de criar coisas novas sem prévia autorização ou licença, o que permitiu uma rápida evolução das aplicações da Internet ao longo das últimas décadas, por meio de uma grande variedade de modelos de negócio.

[8] Na esteira do princípio da "*permissionless innovation*", por muito tempo vigorou o entendimento de que a "autorregulação" das empresas do setor, por meio de suas estruturas de governança corporativa, seria suficiente para o bom desenvolvimento e uso da Internet. Contudo, a regulação estatal tem se tornado cada vez mais presente, considerando os potenciais impactos sobre a sociedade, a necessidade de desenvolvimento de políticas públicas para gerir esses impactos e os conflitos de interesses entre o público (social) e o privado (corporativo). O desafio é compreender quais devem ser os limites dessa regulação e quais podem ser os efeitos indesejados.

que propõe uma abordagem regulatória focada em aspectos econômicos, esvaziando o debate em torno da moderação de conteúdo.

O PL 2768/2022[xvii] atribui também à ANATEL poderes para atuação em assuntos de natureza concorrencial. Atualmente, esse papel é exclusivamente do Conselho Administrativo de Defesa Econômica (CADE), que tem mantido um entendimento de prevalência do bem-estar do consumidor, evitando agir contra a concentração de mercado.

A eventual delegação de poderes regulatórios a uma autoridade central, vinculada ao Estado, requer alguns cuidados. Entre os pontos de atenção, destacam-se: (i) o desafio de gerir conflitos de interesses entre diferentes atores e *players* do mercado; (ii) a preservação do modelo de governança multissetorial, por meio da participação de representantes dos diferentes setores envolvidos na tomada de decisões; e (iii) a competência técnica interdisciplinar, sobretudo considerando o desafio de regulamentar e fiscalizar a moderação do conteúdo, questão central do PL 2630/2020 e do debate regulatório em torno da responsabilidade das plataformas no país[9].

Apoio a uma Internet globalmente conectada: Alcance irrestrito

O PL 2630/2020 pode gerar impactos na acessibilidade irrestrita, indispensável para que se atinja o objetivo da Internet globalmente conectada, em termos de dois desdobramentos possíveis do conceito de soberania digital: (i) o poder de fazer cumprir suas leis e (ii) a questão da soberania relacionada à jurisdição. Ambos os aspectos dizem respeito à noção de soberania digital relacionada ao ponto de vista do Estado.

A exemplo da legislação europeia, o PL 2630/2020 estabelece regramentos muito específicos aos provedores de aplicações digitais que desejam realizar suas atividades no Brasil. O objetivo de tais mecanismos é a defesa dos interesses brasileiros, via meios de proteção e empoderamento das normas e instituições locais, assim reforçando seu poder de regulação. No entanto, não se pode deixar de considerar que o excesso de instrumentos normativos locais pode gerar um obstáculo ao funcionamento da Internet globalmente conectada.

Legislações como a proposta pelo PL 2630/2020 suscitam questionamentos sobre riscos de fragmentação da Internet, especialmente o da “fragmentação da experiência do usuário”, tendo em vista o conflito de regras entre diferentes jurisdições. Isso

[9] Essa tarefa, idealmente, deveria ser compartilhada com diferentes órgãos, tal como ocorre com o controle exercido sobre outras mídias. Esse modelo traz mais segurança em relação à proteção à liberdade de expressão.

ocorre porque especificidades na legislação que regula determinado tema podem levar a uma dissonância entre as leis do país no qual a empresa é sediada, geralmente Estados do Norte Global, e as leis nacionais, o que por sua vez pode resultar na impossibilidade de realização de determinadas operações, gerando prejuízos e insegurança aos usuários.

Estabelecer padrões para a atuação de empresas estrangeiras em solo nacional pode ser um desses objetos de conflitos relacionados à ideia de jurisdição e ao poder de regular sobre temas já tratados pela legislação brasileira, a exemplo do exposto no art. 3º, XIII (adequação a diplomas legislativos brasileiros), no art. 11 (rol exaustivo de condutas ilícitas sujeitas à moderação) e no art. 41 (imposição de regras de funcionamento operacional aos serviços de mensageria instantânea). Além disso, podem estar sendo criadas barreiras de entrada para outras partes interessadas, o que pode concentrar as atividades do nicho em um pequeno número de *players* já consolidados no setor.

Apoio a uma Internet segura: Confidencialidade de dados de informações, dispositivos e aplicativos

A respeito da dimensão da confidencialidade, requisito essencial para a Internet segura, é possível identificar que o PL 2630/2020 pode gerar impactos quanto a três desdobramentos da soberania digital: (i) a questão da segurança nacional; (ii) a capacidade de o Estado fazer cumprir suas próprias leis, que se relaciona diretamente com a questão da jurisdição; e (iii) o direito à autodeterminação de dados dos usuários, esfera da soberania digital focada no aspecto do indivíduo. É de suma importância considerar o item (iii), que passa a, em certa medida, competir com os itens (i) e (ii), focados na soberania digital relacionada aos interesses do Estado, ao passo que o terceiro item prioriza a proteção dos direitos dos cidadãos.

O art. 45 do PL 2630/2020 obriga as plataformas a comunicarem às autoridades suspeitas que ocorreu ou pode ocorrer um crime contra a vida. Já o art. 46 as obriga a guardar, pelo prazo de seis meses, conteúdos removidos ou desativados – em função do cumprimento das regras de moderação trazidas pela lei –, assim como dados e metadados relacionados a esses conteúdos. Não há qualquer ponderação sobre eventuais limites técnicos ao cumprimento dessas obrigações, por exemplo, no caso

dos serviços de mensageria baseados em criptografia[10]. Isso gera grande insegurança aos usuários.

É importante notar que há, nesse caso, um conflito entre o poder de regular do Estado, que visa sobrepor sua jurisdição às empresas estrangeiras que pretendem atuar no Brasil, e o direito individual dos usuários do serviço. Os cidadãos, ao fazerem uso das aplicações digitais, desejam que os serviços sejam seguros e que possam enviar mensagens sem correr o risco de que estas sejam acessadas por sujeitos externos ao assunto. É importante destacar que, embora exista semelhança entre os temas da confidencialidade e da privacidade, trata-se de conceitos diferentes. Enquanto a privacidade se relaciona muito mais com a proteção de dados dos usuários e com sua capacidade de decidir como eles serão tratados, a confidencialidade se refere à possibilidade de os usuários enviarem mensagens com mecanismos de segurança, como a criptografia, de modo que terceiros não possam ter acesso ao conteúdo ou a quem o está enviando[xviii]. Cabe ressaltar que ambos (privacidade e confidencialidade – "ou sigilo das comunicações") são assegurados pelo MCI (cf. art. 11). Entende-se que a possibilidade de monitoramento do conteúdo por terceiros representa um dos principais riscos à confidencialidade, além de riscos à segurança dos usuários, e deve ser estudada com cautela para que seja possível definir limites à aplicação desse dispositivo, sob pena de gerar um vigilantismo excessivo que diminua a liberdade dos cidadãos.

O art. 46, por sua vez, mostra-se problemático por estipular que o conteúdo retirado das plataformas digitais seja mantido a fim de que possa ser utilizado em análises futuras. Isso contraria a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que defende a guarda mínima de dados. Manter o registro do conteúdo por mais tempo do que o necessário aumenta os riscos de violação da confidencialidade, de modo que também aumenta os riscos de exposição indevida do conteúdo a terceiros.

Apoio a uma Internet confiável: Responsabilidade (*accountability*)

No que tange à dimensão de apoio a uma Internet segura a partir do quesito responsabilidade (*accountability*), duas dimensões do debate sobre soberania são identificadas: (i) exercício do poder de regulação e jurisdição no que diz respeito à aderência a leis locais e (ii) garantia do exercício e proteção a direitos.

[10] Há duas ações em curso no STF (a ADPF 403 e a ADI 5527) que analisam a criptografia de ponta a ponta e suas implicações sob a perspectiva legal. Os relatores de ambas as ações já se manifestaram no sentido de que a criptografia é uma ferramenta necessária à proteção de direitos fundamentais.

A ênfase na transparência das práticas de moderação de conteúdos postados por terceiros em redes sociais e na adoção de mecanismos e ferramentas de informação sobre conteúdos disponibilizados para o usuário, por sua vez, está baseada na proteção do usuário final e de seus direitos, de acordo com o ordenamento jurídico brasileiro e o devido processo legal.

O PL 2630/2020 estabelece uma série de obrigações que podem gerar impactos sobre esse habilitador, que contemplam: (i) regras e obrigações de transparência, que incluem a disponibilização de relatórios semestrais contendo informações qualitativas e quantitativas acerca dos procedimentos de moderação de conteúdo previstos na lei; (ii) a adoção de termos de uso e políticas em português e aderentes à legislação/realidade local; (iii) a instituição de um "devido processo" (direito à notificação, contestação e defesa); e (iv) a realização de auditorias externas anuais.

O projeto de lei também prevê algumas informações obrigatórias, tais como faixa etária indicativa, conteúdos proibidos, regras de moderação e formas de notificação sobre possíveis irregularidades. O usuário que tiver seu conteúdo e/ou conta removidos, por exemplo, deverá ser notificado sobre a natureza da medida adotada e seu território de aplicação e o fundamento da decisão com base na indicação dos termos de uso infringidos, oportunizando-se a ele o direito de contestação e defesa, para reversão da medida.

A obrigatoriedade de auditorias externas, por sua vez, deve igualmente abarcar alguns aspectos previstos em lei, tais como eficiência na adoção das medidas e identificação de riscos sistêmicos; aferição de tratamento discriminatório e/ou enviesamento das decisões durante a moderação de conteúdos/contas; impacto dos algoritmos sobre a distribuição do conteúdo etc.

No entanto, é possível identificar, atrelados a essas medidas, riscos à liberdade de expressão e aos direitos humanos dos usuários que extrapolam a dimensão da transparência e que fazem interseção, por sua vez, com as discussões e impactos no que tange à segurança, proteção da privacidade e da confidencialidade.

Nesse sentido, identifica-se uma interseção entre ideias de "soberania estatal" e de "soberania individual" no que diz respeito ao poder de decisão e autoridade. De um lado se encontram regras em favor da coletividade e da necessidade de se obter/garantir segurança, justiça, paz, e bem-estar aos cidadãos; do outro, a autonomia dos indivíduos para se responsabilizar por suas próprias decisões e vida, que seria possível por meio dos instrumentos de notificação e empoderamento linguístico em relação aos termos de uso e políticas das plataformas.

Apoio a uma Internet confiável: Privacidade

Em termos de privacidade, que dá suporte a uma Internet confiável, pode-se identificar três desdobramentos do conceito de soberania digital que impactam a discussão: (i) exercício do poder de jurisdição; (ii) soberania informacional; e (iii) autodeterminação de dados. Destaca-se que o item (i) está focado na noção de soberania relacionada ao Estado, ao passo que o (ii) e o (iii) priorizam a esfera dos interesses dos usuários.

As obrigações trazidas pelos arts. 42, 45 e 46 do PL 2630/2020, ao trazer um risco à confidencialidade dos dados (conforme mencionado em tópico anterior), também põem em xeque a privacidade dos usuários, tanto pelo monitoramento do conteúdo compartilhado – inclusive em mensagens privadas criptografadas – quanto pelo armazenamento de um imenso volume de dados pessoais, incluindo dados possivelmente sensíveis. Um eventual vazamento desses dados comprometeria a privacidade dos usuários.

Essas obrigações servem ao propósito de facilitar o exercício do poder de jurisdição local (novamente, uma forma de manifestação da soberania digital), por meio do fornecimento de dados que possam auxiliar investigações. Contudo, identifica-se aqui mais uma vez o conflito entre a noção de "soberania estatal" (i.e., poder de jurisdição) e a noção de uma "soberania individual", que envolve a soberania informacional dos usuários e a autodeterminação de seus dados. Essa perspectiva de direitos individuais encontra guarida na Lei Geral de Proteção de Dados, que institui o princípio da "necessidade", segundo o qual o tratamento de dados pessoais (que inclui coleta e armazenamento, dentre outras operações) deve se restringir ao "mínimo necessário" para a realização das finalidades do serviço, "com abrangência dos dados pertinentes, proporcionais e não excessivos" (cf. art. 6º, III, da LGPD). Além disso, o MCI prevê o sigilo das comunicações entre os usuários (cf. art. 11), ressalvando a guarda obrigatória, para fins legais, tão somente dos dados de conexão.

Embora o PL 2630/2020 traga como um de seus princípios a privacidade e a proteção dos dados pessoais dos usuários, fazendo diversas remissões à LGPD[xix], os dispositivos mencionados acima representam pontos de alerta importantes.

Cabe ressaltar que as questões relacionadas à privacidade estão intimamente ligadas às análises de outros tópicos deste IIB. Não é possível conceber um modelo de *accountability* e governança que não proteja a privacidade dos usuários e o sigilo de suas comunicações na Internet.

V – CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

Em julho de 2020, o Brasil passou a discutir norma s e mecanismos de transparência para provedores de redes sociais, ferramentas de busca e mensageria instantânea, assim como diretrizes para seu uso, a partir da apresentação da proposta legislativa da "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet" (PL 2630/2020). Um dos principais objetivos do projeto de lei é regular deveres e responsabilidades dos intermediários no contexto brasileiro.

Este relatório utilizou *Internet Impact Assessment Toolkit* para avaliar como o referido projeto de lei pode afetar a Internet global pelas lentes do debate sobre soberania digital. Para tanto, foi considerada a última versão do PL 2630/2020 (apresentada no plenário da Câmara dos Deputados em 27/04/2023) disponível até a finalização deste documento.

A partir desta análise, não foram identificados impactos diretos e imediatos às propriedades críticas que sustentam a infraestrutura da Internet. No entanto, discute-se como o PL 2630/2020 pode afetar habilitadores que possibilitam à Internet funcionar e prosperar como um recurso aberto, globalmente conectado, seguro e confiável para todos. A discussão foi estabelecida com base em argumentos e dimensões de soberania digital que podem causar prejuízos ou reduzir: (i) o desenvolvimento e a governança colaborativos; (ii) a acessibilidade irrestrita; (iii) a confidencialidade de informações, dispositivos e aplicativos; (iv) a responsabilização; e (v) a privacidade.

Apesar dos significativos avanços técnicos e jurídicos da proposta em relação à versão aprovada no Senado, foram identificados alguns pontos de atenção, que podem ter consequências para a inovação, para a resiliência e para a fragmentação da Internet, evidenciando a relevância do debate.

Recomenda-se atenção a esses possíveis impactos, com vistas a uma legislação que seja adequada ao enfrentamento dos desafios gerados pelo mau uso das redes sociais e pelas externalidades negativas dos modelos de negócio adotados pelas plataformas, mas que também seja capaz de acompanhar o dinamismo das transformações geradas pela evolução tecnológica.

REFERÊNCIAS

[i] BRASIL. *Projeto de Lei nº 2.630/2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/propostas-legislativas/2256735. Acesso em: 6 abr. 2024.

[ii] ISOC BRASIL. *O Modo Internet de Interconectividade*: um fundamento para o sucesso. [S.d.]. Disponível em: https://www.isoc.org.br/files/IWN_introducao_traducao%20(1).pdf. Acesso em: 6 abr. 2024.

[iii] INTERNET SOCIETY. *Internet Impact Assessment Toolkit*. [S.d.]. Disponível em: https://www.Internetsociety.org/issues/Internet-way-of-networking/Internet-impact-assessment-toolkit/. Acesso em: 6 abr. 2024.

[iv] TOCH, Lucas. "Regulação promove Internet mais saudável para a democracia", diz Renata Mielli (2023). *NIC.br*, 2 jan. 2024. Disponível em: https://www.nic.br/noticia/na-midia/regulacao-promove-Internet-mais-saudavel-para-a-democracia-diz-renata-mielli/. Acesso em: 6 abr. 2024.

INTERNET SOCIETY. *Navigating digital sovereignty and its impact on the Internet*. December 2022. Disponível em: https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf. Acesso em: 6 abr. 2024.

[vi] NIC.br. Grupo de Trabalho sobre Regulação de Plataformas do CGI.br. *Sistematização das contribuições à consulta sobre regulação de plataformas digitais.* São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2023. p. 22. Disponível em: https://cgi.br/media/docs/publicacoes/1/20240227162808/sistematizacao_consulta_regulacao_plataformas.pdf. Acesso em: 6 abr. 2024.

[vii] NIC.br. Grupo de Trabalho sobre Regulação de Plataformas do CGI.br. *Sistematização das contribuições à consulta sobre regulação de plataformas digitais.* São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2023. p. 16. Disponível em: https://cgi.br/media/docs/publicacoes/1/20240227162808/sistematizacao_consulta_regulacao_plataformas.pdf Acesso em: 6 abr. 2024.

[viii] APERFEIÇOAMENTO LEGISLAÇÃO BRASILEIRA – Internet – Tecnologia e soberania nacional, 31/08/2021 (1h43min). Publicado pelo canal Câmara dos Deputados. Disponível em: https://www.youtube.com/watch?v=_L_F1xYbNRc. Acesso em: 6 abr. 2024.

[ix] CICLO DE DEBATES PÚBLICOS: Lei de Combate às Fake News (PL 2630/20), 29/07/2020 (2h12min). Publicado pelo canal Câmara dos Deputados. Disponível em: https://www.youtube.com/watch?v=iWB97_-GYu4. Acesso em: 6 abr. 2024.

[x] CARTA SOBERANIA DIGITAL. [S.d.]. Disponível em: https://cartasoberaniadigital.lablivre.wiki.br/carta/. Acesso em: 6 abr. 2024.

[xi] STF. *Autoridades nacionais podem requisitar dados diretamente a provedores no exterior, decide STF.* 23 de fevereiro de 2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=502922&ori=1. Acesso em: 6 abr. 2024.

[xii] BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 23 abr. 2014. Disponível em:

http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 6 abr. 2024.

[xiii] ISOC BRASIL. *O Modo Internet de Interconectividade*: um fundamento para o sucesso. [S.d.]. Disponível em: https://www.isoc.org.br/files/IWN_introducao_traducao%20(1).pdf. Acesso em: 6 abr. 2024.

[xiv] ISOC. *How to conduct an Internet Impact Brief*. Internet Impact Assessment Toolkit, 2021. p. 3. Disponível em: https://www.Internetsociety.org/resources/doc/2021/how-to-conduct-an-Internet-impact-brief/. Acesso em: 6 abr. 2024.

[xv] ISOC Brasil. *Contribuição do Capítulo Brasileiro da Internet Society ao processo de desenvolvimento de política "Habilitadores de uma Internet aberta, globalmente conectada, segura e confiável".* [202-]. Disponível em: https://isoc.org.br//files/Contribui%C3%A7%C3%A3o%20do%20Cap%C3%ADtulo%20Brasileiro%20da%20Internet%20Society%20ao%20Processo%20de%20Desenvolvimento%20de%20Pol%C3%ADtica%20%E2%80%9CHabilitadores%20De%20Uma%20Internet%20Aberta,%20Globalmente%20Conectada,%20Segura%20E%20Confi%C3%A1vel%E2%80%9D.pdf. Acesso em: 6 abr. 2024.

[xvi] INTERNET SOCIETY. *Navigating digital sovereignty and its impact on the Internet*. December 2022. p. 12. Disponível em: https://www.Internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf. Acesso em: 6 abr. 2024.

[xvii] BRASIL. *Projeto de Lei nº 2.768/2022*. Dispõe sobre a organização, o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro e dá outras providências. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2337417. Acesso em: 6 abr. 2024.

[xviii] INTERNET SOCIETY. *Navigating digital sovereignty and its impact on the Internet*. December 2022. p. 33. Disponível em: https://www.Internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf. Acesso em: 6 abr. 2024.

[xix] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 abr. 2024.

FGV DIREITO SP
CENTRO DE ENSINO
E PESQUISA EM INOVAÇÃO

Internet Society
Capítulo Brasil