Consulta sobre Regulação de Plataformas Digitais no Brasil promovida pelo Comitê Gestor da Internet do Brasil (CGI.br)

Durante o mês de julho de 2023, o Grupo de Trabalho de Responsabilidade de Intermediários (GT-RI) da ISOC Brasil contribuiu para a consulta sobre Regulação de Plataformas Digitais no Brasil, promovida pelo Comitê Gestor da Internet do Brasil (CGI.br).

Agradecimentos especiais aos membros do capítulo que se envolveram nesta iniciativa, nomeadamente Laura Pereira, Luís Acioly, Flávio Rech Wagner, Paula Bernardi, Milena Cramar, Terezinha Brito, Vitória Santos, Pedro Lana, Laurianne Marie Schippers, João Vitor Zaidan, Thobias Prado, Helena Farias, Laíse Barbosa, Sinuhe Cruz, José Arthur, Paulo Renná, Thais Aguiar, Márcia Florentino, Henrique Bazan e Danielle Novaes.

2. Quais são as dimensões relevantes para descrever os diferentes tipos de plataformas digitais?

Os vários marcos regulatórios que têm sido propostos ao redor do mundo representam diversas possibilidades em termos de definições conceituais, princípios legais e mecanismos legislativos que podem delimitar modelos de responsabilidade de intermediários e escopos diferenciados de aplicação das novas legislações ou regramentos. Na medida em que os debates sobre esse arcabouço conceitual relacionado às plataformas digitais frequentemente se restringem ao debate sobre quais plataformas deveriam estar sujeitas à legislação fundamentalmente com base no seu número de usuários, a ISOC Brasil reforça a relevância de que outros elementos também sejam levados em consideração na busca por marco regulatório adequado às especificidades da Internet e do ambiente legal e regulatório do país.

Em conformidade com a missão global da Internet Society e com base no Decálogo e Recomendações sobre o Modelo Brasileiro de Responsabilidade de Intermediários, ressaltamos que a Internet integra um complexo sistema de provedores de serviços. Nesse sentido, chamamos a atenção para i) os diferentes tipos de serviços e aplicações existentes e as suas consequentes diferenciações em relação ii) ao poder econômico, iii) status jurídico e iv) posicionamento de mercado e de funcionalidade em um complexo ecossistema digital. Tal conjunto relevante de assimetrias entre atores, com diferentes modelos de negócios e capacidades econômicas que conferem distintos alcances e características dos serviços oferecidos, deve também ser compatibilizado com os modelos de responsabilidade civil já estabelecidos no ordenamento jurídico, entre legislações específicas, como o Marco Civil da Internet, e regramentos que também podem ser mobilizados para a área, como o Código de Defesa do Consumidor.

Por essas razões, a ISOC Brasil considera que legislações que não levem esse conjunto de fatores em consideração e que não dialoguem com a terminologia já pacificada pelo Marco Civil da Internet, bem como retomem o debate da época, o modelo de construção e os princípios do MCI para avançar em um maior detalhamento e compreensão dos provedores de aplicação, tendem a se tornar obsoletas, inaplicáveis e excessivamente contestáveis pelos diferentes atores que podem ser afetados. Além disso, acreditamos que a estratégia adotada pelo Marco Civil é capaz de atender às demandas que justificam atualizações regulatórios ao mesmo tempo em que também atende à necessária compatibilidade não só com as propriedades críticas da Internet e o ordenamento jurídico já estabelecido, mas ao importante princípio de que a Internet deve ser preservada como uma rede de propósitos múltiplos. Nesse sentido, regulações demasiadamente específicas em relação a um modelo de negócio vigente contemporaneamente podem também ser suplantadas pela rápida emergência de novas tecnologias e novos modelos de negócios. As atividades da ISOC Brasil têm recorrentemente justificado a firme compreensão de que os princípiosjá incorporados no Marco Civil da Internet e os princípios defendidos pelo Decálogo e Recomendações sobre o Modelo Brasileiro de Responsabilidade de Intermediários são indispensáveis para o estabelecimento de marcos regulatórios duradouros.

16. Caso haja riscos relacionados à soberania digital e ao desenvolvimento tecnológico que não tenham sido mencionados, descreva a seguir. Indique as medidas de mitigação desses novos riscos.

SOBRE OS DIFERENTES CONCEITOS DE SOBERANIA DIGITAL

É importante que uma regulação que trate de alguma forma a temática da soberania digital tome o cuidado de não impor ou vincular o termo a uma definição única e estanque que prejudique a compreensão de outras ações/políticas que também podem fazer parte desse conceito “guarda-chuva”.

É possível atribuir diferentes significados ao termo “soberania digital”, cujas noções, por vezes, podem se interseccionar. Uma das primeiras concepções de soberania digital é aquela vinculada à noção de controle e poder do Estado sobre o digital como um todo, seja com relação às diferentes camadas que compõem esse ambiente (infraestrutura física, códigos, *softwares*, *hardwares*, protocolos de operação, entre outros), seja com relação à garantia de segurança nacional, ao fluxo de dados e de informação, e ao estabelecimento de normas para o meio digital (e às formas de garantir a aplicação dessas regras) [1].

Uma segunda perspectiva, também vinculada ao poder e políticas provenientes do Estado, é a que preza pelo desenvolvimento da indústria local de tecnologias, plataformas e serviços digitais diversos [2]. Sob tal prisma, visa-se reduzir a

dependência de serviços oferecidos por empresas estrangeiras e, consequentemente, prover maior autonomia econômica ao país e maior capacidade competitiva do mercado interno.

Por fim, também é possível tratar da soberania digital em termos da autonomia/autodeterminação de indivíduos, grupos e movimentos sociais. Sob esse guarda-chuva, o conceito refere-se à capacidade de um indivíduo, bem como de grupos, comunidades e movimentos sociais, de poderem atuar e tomar decisões sobre suas informações e fluxos de dados de maneira autônoma e independente, de acordo com seus próprios interesses, valores e cultura [3]. Também envolve o desenvolvimento de sistemas, tecnologias e infraestruturas próprias. Como exemplos, é possível mencionar as medidas buscadas com relação aos dados da população Maori na Nova Zelândia; e à definição de soberania digital apresentada pelo MTST no Brasil:

> “A third approach aligns digital sovereignty with individual and/or collective sovereignty. This is manifested in measures to enhance the rights of individuals and/or communities in relation to data about or created by them. In its data sovereignty guidance, the New Zealand government calls for institutions to choose cloud services that respect indigenous Māori data rights. It upholds the Māori Data Sovereignty Charter, which urges greater Māori access to, and ownership of, data collected about them by other entities, and empowers the Māori to govern their data according to their customs and priorities” [4].

> “Nós, do Núcleo de Tecnologia do Movimento dos Trabalhadores Sem Teto (MTST), entendemos a soberania digital como a soberania tecnológica dos movimentos sociais. Entendemos essa soberania a partir do uso e desenvolvimento de tecnologias por e para quem faz as lutas sociais. Isto é, além de não ficar para trás na corrida do digital, poder apontar qual caminho é realmente emancipatório, mostrando como podemos promover a tecnologia para o fortalecimento da organização do poder popular”[5].

Dessa forma, nota-se que o conceito de soberania digital aparece com diferentes contornos, sendo importante que uma regulação que trate sobre a temática não imponha uma definição única e estanque, sob pena de prejudicar a compreensão de outras ações/políticas como também sendo parte desse conceito “guarda-chuva”. Sendo um conceito multifacetado, a definição escolhida para soberania digital e suas respectivas ações de implementação têm o potencial de impactar outros atores e elementos-chave da infraestrutura da Internet global, como a conectividade e a Neutralidade da rede.

SOBRE OS CONCEITOS DE FRAGMENTAÇÃO DA INTERNET E SEUS RISCOS

Em defesa da Internet aberta, globalmente conectada, segura e confiável, chama-se a atenção aos riscos não apenas decorrentes da operação de plataformas digitais

em contextos nacionais, tal como observado na Consulta, mas aos riscos de opções regulatórias que fragmentem indevidamente a experiência do cidadão brasileiro conectado à rede.

A proposta parte da expansão da conceituação clássica de Fragmentação da Internet. Uma das mais difundidas, em razão do extenso trabalho da organização nesse campo e na proteção de uma Internet aberta, conectada globalmente, segura e confiável, é o da Internet Society. O conceito é guiado pela preocupação com a preservação desses elementos fundamentais, sendo especialmente relevante aqui a conexão global, a abertura e a confiabilidade da tecnologia, que podem ser severamente afetadas em processos de fragmentação. Importante comentar que existem diferentes tipos de fragmentação, a depender do conceito utilizado. Alguns deles, quando sob o controle consciente e intencional do usuário final que controla a ponta da rede e recebe a informação, podem ser considerados positivos. Vide https://www.internetsociety.org/blog/2016/01/hey-someone-fragmented-my-internet-and-didnt-even-tell-me/

Afinal, para a Internet existir na forma que a conhecemos hoje, é necessária a combinação de cinco propriedades fundamentais críticas: (i) uma infraestrutura acessível com um protocolo comum, permitindo a colaboração global sem fronteiras nacionais; (ii) uma arquitetura aberta de blocos de construção interoperáveis e reutilizáveis, estimulando a inovação ao manter a Internet simples; (iii) gerenciamento descentralizado e um único sistema de roteamento distribuído, permitindo que a rede evolua de forma eficiente priorizando que a informação chegue ao seu destino; (iv) identificadores globais comuns, garantindo que as comunicações cheguem ao endereço correto da ponta da rede; e (v) uma rede tecnologicamente neutra e de uso geral, permitindo a inovação pela falta de propósitos específicos.

Assim, para a ISOC, a antítese da Internet é o que ela chama de “splinternet”, ou, em tradução livre, uma “rede fragmentada”, resultado de processos de fragmentação mais incisivos. Essa é a ideia de que a Internet aberta e globalmente conectada que todos nós usamos se fragmente em uma coleção de redes isoladas controladas por governos ou corporações, ainda que continuem compartilhando os mesmos protocolos e nomes da rede global que conhecemos hoje. Ou seja, interrompe-se o livre fluxo da informação, e o que você recebe como um usuário da ponta do sistema é profundamente controlado (ou mesmo bloqueado) por terceiros, que podem inclusive te direcionar para um endereço virtual que não é o originalmente desejado (vide: https://isoc.org.br/noticia/como-proteger-a-internet-de-se-tornar-a-splinternet).

Em outras palavras, a Internet, tão caracterizada por ser uma tecnologia transfronteiriça (ainda que sejam legítimas algumas variações de país para país) passa a ter fronteiras rígidas e que geram experiências radicalmente diferentes quando você passa de um lado ao outro. O exemplo da China (Great Firewall), ou

das tentativas no mesmo sentido da Rússia (RuNet), são regularmente mencionados (vide: https://www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/.). Porém, é importante notar que existem vários exemplos de processos fragmentantes no ocidente, com múltiplos exemplos na Europa, no Canadá e nos EUA (https://www.internetsociety.org/blog/2023/03/misguided-policies-the-world-over-are-slowly-killing-the-open-internet/).

Exemplos importantes de processos de fragmentação que levam a uma splinternet são desligamentos (shutdowns) da Internet, decisões politizadas sobre acesso à Internet e sua infraestrutura (especialmente quando afetam outros países) e políticas ou decisões de negócios que não levam em consideração, como um elemento prioritário, a proteção das funcionalidades da Internet.

Assim como apontado pela Internet Society, a PNIF (Rede de Políticas sobre Fragmentação da Internet), vinculada ao IGF (Internet Governance Forum), também conceitua as diferentes formas de fragmentação da Internet a partir dos riscos existentes para a operação global dessa rede de redes.

A PNIF conceitua a fragmentação a partir de três dimensões principais: (i) da experiência do usuário; (ii) da camada técnica da Internet; e, (iii) da governança e coordenação da Internet. A primeira, fragmentação da experiência do usuário, se baseia principalmente no acesso aos conteúdos, serviços e aplicações disponíveis na Internet, tratando das distintas possibilidades de experimentação do usuário nesse meio, resultante da ausência de acesso efetivo à infraestrutura ou do controle do fluxo de informações operada por intervenções estatais ou de corporações. Nesse cenário, a estrutura de Direitos Humanos e a necessidade de manter um fluxo livre de dados serviriam como referências para avaliar quais medidas afetam a experiência do usuário e como evitar aquelas que a afetam negativamente. O aumento da censura e bloqueios da Internet em épocas de eleições e/ou protestos são exemplos de formas de fragmentação que ferem os direitos humanos (conhecidos como Internet shutdowns). Neste contexto, o capítulo brasileiro da ISOC Brasil acredita que incluir esta chave conceitual no debate sobre marcos regulatórios é estratégia frutífera para prevenir riscos indesejados que possam decorrer de iniciativas nacionais.

A segunda dimensão destacada pela PNIF é baseada na fragmentação da camada técnica da Internet, referindo-se, assim, às medidas que causam potenciais riscos à interoperabilidade da infraestrutura e do funcionamento da Internet global. São citadas, como causas possíveis desses riscos, interferência no núcleo público da Internet, criação de “internets nacionais” limitadas por fronteiras geográficas e roteamento do tráfego de Internet via infraestrutura privada por grandes empresas de tecnologia.

A terceira dimensão é a de fragmentação da governança e coordenação da Internet, podendo se manifestar através de mudanças no compromisso de gestão multissetorial da Internet ou da ausência de um compromisso global e multissetorial para abordar questões de políticas globais de Internet, a partir de uma perspectiva de direitos humanos e livre fluxo de dados. O compromisso multissetorial com o desenvolvimento de políticas e regulamentos é destacado como um ponto de crucial relevância, tendo por certo que, caso um dos setores interessados deseje fazer interesses próprios se sobreporem em detrimento do interesse dos demais, é colocada em risco a camada técnica e, consequentemente, também a experiência dos usuários.

Vale ressaltar, ainda, que se reconhece a existência de alguns níveis de fragmentação que podem ser condizentes com o desenvolvimento da Internet. No entanto, há preocupações de que o fenômeno esteja piorando e possa impactar o cenário global de interoperabilidade da Internet, o que reforça a necessidade de atenção de legisladores e de toda a comunidade brasileira de Governança na Internet na contínua construção do ambiente legal e regulatório que é aplicado à Internet no Brasil.

Nessa conjuntura, o espaço multissetorial de Governança da Internet, por agregar ao debate diversas partes interessadas, está intrinsecamente ligado com os diálogos necessários para que possa evitar a fragmentação. Nesse sentido, a partir da discussão entre variados atores, algumas premissas básicas foram estipuladas: a Internet aberta deve ser globalmente conectada, disponível para todos e baseada nos direitos humanos; a transparência e a proteção da privacidade são fundamentais, incluindo a possibilidade de controle da própria experiência online; a concorrência, escolha e inovação devem ser protegidas; e o debate sobre moderação de conteúdo deve ser aprofundado.

Com efeito, compreende-se que, no que diz respeito à experiência do usuário, as discussões sobre a fragmentação e o futuro da Internet devem abandonar a perspectiva individualista e passar para um paradigma coletivo; e, em relação à Governança da Internet, passar de um modelo de apenas cooperação entre os atores para um modelo que vise também o empoderamento mútuo destes.

Por fim, no contexto nebuloso de busca pela definição da fragmentação da Internet, é necessário ter uma compreensão nítida do que não se enquadra como fragmentação ou uma consequência dela, ao mesmo tempo que a definição e o discurso em torno da fragmentação não devem ser modulados para excluir exemplos de fragmentação que são aceitos, como, por exemplo, certas ações de aplicação da lei contra conteúdo nocivo e/ou regulamentação excessiva.

PRÁTICAS REGULATÓRIAS QUE PODEM FRAGMENTAR A INTERNET: O caso do Sending Party Network Pays (SPNP) na Coreia do Sul

Um exemplo de como práticas regulatórias podem impactar a Internet é o caso do Sending Party Network Pays (SPNP) na Coreia do Sul. O Internet Impact Brief (relatório elaborado com o objetivo de analisar como diferentes políticas ou novas tecnologias podem impactar nas propriedades críticas que garantem o funcionamento e o desenvolvimento da Internet. Saiba mais em: https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/) elaborado pela Internet Society analisa as novas regras de interconexão entre provedores de serviços de internet (ISPs) e provedores de serviços de valor agregado às telecomunicações (VSPs) na Coreia do Sul. Essas regras incluem taxas pelo uso de redes e requisitos de qualidade de serviço. O Ministério da Ciência, TIC e Planejamento de Futuro da Coreia do Sul implementou os Padrões de Interconexão para Instalações de Telecomunicações em 2016, exigindo que os ISPs cobrem pelo tráfego recebido uns dos outros. Essa prática é conhecida como Sending Party Network Pays (SPNP) e impõe custos adicionais aos provedores de conteúdo. A política SPNP foi reforçada por alterações no Telecommunications Business Act, exigindo que os provedores de conteúdo atendam a certos requisitos e firmando contratos com ISPs locais.

Essas regras afetam as propriedades críticas da Internet. Elas interferem na autonomia da Internet como uma rede gerenciada descentralizada, impondo acordos de negócios entre os agentes para o uso das redes e restringindo a flexibilidade das redes. A política SPNP também limita a escalabilidade na entrega de conteúdo interativo e streaming devido à infraestrutura de conectividade e troca de tráfego inadequada que ela impõe. Além disso, essas regras violam o princípio da neutralidade da rede e fragmentam a Internet, limitando o acesso dos usuários a serviços online que não têm contrato com ISPs locais.

A política SPNP impõe ônus aos provedores de conteúdo para manter a qualidade do serviço, podendo resultar em downgrade ou suspensão de seus serviços. Isso pode ser usado pelos ISPs locais para favorecer um provedor de conteúdo em detrimento de outros, prejudicando a experiência do usuário e ameaçando a ideia de uma Internet global e de propósito geral. No Brasil, a Agência Nacional de Telecomunicações (Anatel) propõe uma política regulatória semelhante (https://apps.anatel.gov.br/ParticipaAnatel/VisualizarTextoConsulta.aspx?TelaDeOrigem=2&ConsultaId=10120), que poderia transferir custos e impor restrições aos provedores de conteúdo, criando dificuldades de acesso e segregação virtual de usuários.

Essa regulação brasileira tem o potencial de reduzir a inovação na Internet, impor barreiras ao desenvolvimento de tecnologias e criar fragmentação na experiência do usuário. Transferir custos de infraestrutura para os provedores de conteúdo pode limitar o alcance e o acesso a determinados conteúdos. Portanto, uma regulação de plataformas com objetivos semelhantes corre o risco de afetar negativamente as propriedades críticas da Internet.

SOBERANIA, REGULAÇÃO E PRINCÍPIOS DA INTERNET

Ao se pensar regulação sob o prisma da soberania digital, é imperativo ponderar um equilíbrio entre as necessidades e direitos dos Estados e a preservação dos princípios universais da Internet, garantindo sua natureza global, aberta e acessível. Deve-se ter em conta que essa natureza principiológica impacta significativamente a direção futura de seu desenvolvimento.

A regulação da Internet deve ser sempre orientada por um compromisso com o bem comum global, buscando proteger sua integridade e universalidade. Dessa forma, a regulação requer um forte compromisso com os princípios fundamentais da Internet, entre os quais podemos citar:

1) UNIVERSALIDADE E IGUALDADE: A Internet deve ser acessível a todos, independentemente de sua localização, raça, gênero, idade ou status econômico. A igualdade de acesso é essencial para garantir que todos possam se beneficiar das oportunidades oferecidas pela Internet.

2) ABERTURA: A natureza aberta da Internet tem sido fundamental para o seu crescimento e sucesso. As normas devem promover a abertura e a transparência, permitindo que todos contribuam para o seu desenvolvimento e evolução e que novos serviços e tecnologias sejam incorporados facilmente.

3) SEGURANÇA: A segurança é um aspecto crítico da Internet. A regulação deve se concentrar na garantia de que os sistemas sejam robustos e resilientes a uma variedade de ameaças.

4) INTEROPERABILIDADE: As normas devem promover a interoperabilidade entre redes e dispositivos, garantindo que eles possam funcionar juntos de forma eficaz.

5) NEUTRALIDADE DA REDE: Este princípio assegura que todos os dados na Internet sejam tratados de forma igual, sem discriminação ou preferência.

6) DESCENTRALIZAÇÃO: Este é um princípio fundamental da Internet, que não tem um controle centralizado, e permite a todos a oportunidade de criar, inovar e compartilhar informação de maneira equitativa.

7) MODELO DE PARTICIPAÇÃO MULTISSETORIAL: A criação e implementação de normas deve ser um processo inclusivo e participativo, que permita a contribuição de todas as partes interessadas.

A complexidade da tarefa regulatória reside na necessidade de equilibrar a preservação desses princípios fundadores da Internet com objetivos multifacetados da regulação, que incluem a manutenção da segurança, a proteção dos direitos dos

usuários, a promoção da concorrência justa, a garantia da privacidade, a mitigação da disseminação de conteúdo desinformativo, a proteção dos direitos humanos, dentre outros. Ao se pensar regulação sob o prisma da soberania digital, é imperativo ponderar um equilíbrio entre as necessidades e direitos dos Estados e a preservação dos princípios universais da Internet, garantindo sua natureza global, aberta e acessível. Essa tarefa demanda uma abordagem cooperativa e multissetorial, que não comprometa a essência interconectada e descentralizada da Internet.

REFERÊNCIAS

[1] INTERNET SOCIETY. Navigating Digital Sovereignty and its Impact on the Internet. 2022. Disponível em: https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf; FALKNER, G. et al. Digital Sovereignty – Rhetoric and Reality. Framework Paper for the Online Conference 28-29 April 2022. Disponível em: https://eif.univie.ac.at/downloads/veranstaltungen/2022/2022%20Falkner%20et%20al.%20Digital%20Sovereignty%20Framework%20Paper.pdf; CHANDER, A.; SUN, H. Sovereignty 2.0. Georgetown University Law Center, 2021. Disponível em: https://scholarship.law.georgetown.edu/facpub/2404/; POHLE, J.; THIEL, T. Digital Sovereignty. In: HERLO, B. et al (Eds.). Practicing Sovereignty: Digital Involvement in Times of Crises. Bielefeld: transcript Verlag, 2021.

[2] INTERNET SOCIETY. Op. cit.; POHLE, J.; THIEL, T. Op. cit.

[3] INTERNET SOCIETY. Op. cit.; COUTURE, S.; TOUPIN, S. What does the notion of “sovereignty” mean when referring to the digital? New Media & Society v. 21, Issue 10, 2019. Disponível em: https://journals.sagepub.com/doi/10.1177/1461444819865984; POHLE, J.; THIEL, T. Op. cit.

[4] INTERNET SOCIETY. Op. cit. p. 18-19.

[5] NÚCLEO DE TECNOLOGIA DO MTST. A soberania digital a partir dos movimentos sociais. Blog Boitempo, 2022. Disponível em: https://blogdaboitempo.com.br/2022/11/11/a-soberania-digital-a-partir-dos-movimentos-sociais/

27. Você concorda que a lista de temas elencados a seguir, relacionada a ameaças à democracia e aos direitos humanos, são riscos que devem ser considerados para regulação de plataformas digitais? Comente cada risco se julgar adequado.

i Riscos associados a infodemias, como desinformação, extremismos, discurso de ódio, incitação ao terrorismo, entre outros;

ii Riscos associados a ameaças a processos eleitorais e inibição de mecanismos de participação política e de engajamento cívico;

iii Riscos associados aos efeitos da falta de transparência dos critérios e mecanismos associados ao uso de dados pessoais, à moderação e monetização de conteúdos e à publicidade direcionada feitas por plataformas digitais sobre temas de interesse público;

iv Riscos relacionados a impactos negativos das atividades e modelos de negócio das plataformas sobre o jornalismo;

v Riscos associados à privacidade e à proteção de dados pessoais;

vi Riscos associados ao uso de plataformas digitais por crianças e adolescentes, considerando as necessidades especiais de proteção de seus interesses.

Somos cautelosos com a regulação de plataformas e da Internet que tem como premissa o combate à conteúdos prejudiciais nas redes. Verifica-se uma tendência preocupante de governos em usar tecnologia e controle da Internet para suprimir a dissidência e fortalecer seu poder. Isso pode tomar várias formas, desde a censura e o bloqueio de sites até a vigilância massiva e a coleta de dados pessoais.

De acordo com a Access Now, o ano de 2022 mostrou uma perturbadora tendência de apagões de Internet em 12 países africanos, com 19 incidentes, frequentemente justificados por pretextos de segurança nacional. Estes foram especialmente observados durante os processos eleitorais, sob a suposta premissa de combater a propagação de discurso de ódio e desinformação (vide Garay, Vladimir. "Los apagones de internet atentan contra los derechos humanos." Derechos Digitales, 10 de junho de 2023. https://www.derechosdigitales.org/20673/los-apagones-de-internet-atentan-contra-los-derechos-humanos/).

Considerando que a Internet se tornou um instrumento indispensável para o exercício de direitos fundamentais, tais interrupções vão além de simples

inconveniências - elas acarretam danos a direitos civis e têm o potencial de afetar diversas esferas da vida cotidiana dos cidadãos.

Situação semelhante é observada na América Latina, onde relatos de interrupções parciais da Internet durante protestos políticos têm sido alarmantes. Incidentes significativos ocorreram na Nicarágua em 2018 e na Colômbia em 2019 e 2021. Na mesma linha, existem exemplos notáveis em lugares como a Rússia. A implementação de filtros na Rússia segue uma longa história de restrições de conteúdo no país baseadas em táticas mais sutis e difíceis de documentar. O Kremlin exerce uma influência cada vez maior sobre o discurso público online, com atores do Estado participando ativamente de debates e discussões em plataformas tradicionalmente usadas por pioneiros não estatais. A censura nas mídias sociais também está aumentando, com provedores de conteúdo da Internet migrando cada vez mais para as plataformas de mídia social (Zittrain, Jonathan L., et al. "The Shifting Landscape of Global Internet Censorship." *SSRN Electronic Journal* (2017). https://doi.org/10.2139/ssrn.2993485. p.17.).

Conforme o relatório "Freedom on the Net Report" da Freedom House (https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf.), a censura a plataformas de mídias sociais e aplicativos de comunicação atingiu um recorde global em 2022, com um número cada vez maior de governos visando plataformas de mídia social e aplicativos de mensagens como WhatsApp e Telegram para controlar o fluxo digital de informações. Estes exemplos reforçam a necessidade crítica de garantir que o acesso à Internet - e, por extensão, os direitos fundamentais - não sejam arbitrariamente comprometidos.

No Brasil, cabe mencionar os casos dos bloqueios do WhatsApp entre 2015 e 2016, além do do bloqueio do Telegram em 2023, suspenso por uma decisão judicial pela falha em entregar informações sobre usuários em grupos de conversa acusados de disseminar discursos de ódio. (https://agenciabrasil.ebc.com.br/justica/noticia/2022-03/ministro-do-stf-determina-bloqueio-do-telegram-no-brasil). Apesar da medida ser fundamentada em preocupações válidas de segurança e combate ao discurso de ódio, levantou-se uma série de questões críticas acerca do delicado equilíbrio entre segurança e privacidade na Internet.

28. Caso haja riscos relacionados a ameaças à democracia e aos direitos humanos que não tenham sido mencionados, descreva a seguir. Indique as medidas de mitigação deste(s) novos riscos.

Os riscos acima mencionados compreendem parte importante, embora não exaustiva, dos elementos a serem considerados na construção de novos elementos que componham o marco regulatório sobre Internet do país. Eles representam problemas fundamentais que têm sido sistematicamente afirmados como relevantes

e urgentes dentro do lugar que plataformas digitais, em especial as de mídias sociais e de mensageria, têm assumido na contemporaneidade.

Nesses termos, o Grupo de Trabalho de Responsabilidade de Intermediários do capítulo brasileiro da ISOC Brasil considera que o modelo de responsabilidade já existente no Marco Civil da Internet é plenamente adequado para atender às demandas que vêm sendo colocadas. É importante avaliar que o Marco Civil não foi construído e não tem operado como forma de desresponsabilização generalizada ou criação de um ambiente isento de leis. Como um modelo específico e brasileiro de responsabilidade civil aplicada à Internet, mundialmente respeitado, o Marco prevê mecanismos de responsabilização para conteúdos de terceiros, como detalhado na Seção III da Lei 12.965/2014 que têm sido operados pelo Direito brasileiro. Além disso, o faz tendo por base princípios e valores balizados por meio de amplo debate público, e alinhados às propriedades críticas da estruturação e do funcionamento da Internet.

O prudente respeito ao ordenamento jurídico existente há quase uma década no país não é impeditivo ao possível aprimoramento da legislação, mas consideramos, também, que processos afins devem ser balizados no reconhecimento e continuidade dos fundamentos, princípios e objetivos nele estabelecidos. O Marco Civil, além disso, expressa igualmente os resultados benéficos e inigualáveis de processos legislativos feitos com abertura e centralidade para a participação social, multissetorial e democrática, de atores interessados, o que também integra a tradição legislativa por ele representada e o valor de que novas iniciativas atenham-se também à necessidade e proporcionalidade em relação aos problemas a serem enfrentados.

Nesses temas, o enfrentamento dos riscos acima dispostos pode ter por base não o descarte do acúmulo representado pelo Marco Civil, mas a sua completa efetivação e possíveis aprimoramentos compatíveis ao corpo da Lei, com atenção à crescente relevância de mecanismos de transparência e respeito ao devido processo legal, dentro e fora do ambiente imediato das plataformas.

35. Considerando os riscos associados a atividades e modelos de negócio das plataformas sobre o jornalismo, indique possíveis medidas de mitigação.

O recente caso da legislação canadense para a remuneração de conteúdo jornalístico no país é um exemplo de um arranjo regulatórios que pode restringir a experiência que o usuário possui da rede aberta, globalmente conectada, segura e confiável. Aprovada em junho de 2023, a proposta do Online News Act (Bill C-18) foi previamente analisada pela Internet Society (Disponível em: https://www.internetsociety.org/resources/doc/2023/internet-impact-brief-how-canadas-online-news-act-will-harm-the-internet-restricting-innovation-security-and-growth-of-the-digital-economy/) identificando que o projeto, cujo objetivo era fortalecer os

produtores nacionais de conteúdo jornalístico por meio da criação de novas obrigações de remuneração para as plataformas digitais, iria, dentre outras consequências negativas, restringir o livre acesso de cidadãos canadenses a conteúdos globais, diferenciando a experiência da sociedade canadense na Internet, se comparada aos demais países.

Nesses termos, a avaliação feita do projeto a partir dos parâmetros fundamentais que constituem a Internet interconectada e interoperável (Ver https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/) mostrou que a solução proposta para um problema legítimo poderia, em realidade, levar a novas e complexas questões. A aprovação do Online News Act é recente, mas já tem suscitado uma primeira onda de reações mercadológicas associadas à interrupção de exibição e acesso a notícias em plataformas da Meta e da Google, dentre outros debates relevantes nessa área (Mais informações em: https://oglobo.globo.com/economia/noticia/2023/06/canada-aprova-lei-que-obriga-a-meta-e-a-alphabet-a-pagar-os-editores-de-noticias.ghtml).

A busca por soluções legislativas para fenômenos e problemas relacionados à Internet tem afetado todos os países e demais atores da comunidade de governança da Internet. Em particular, o próprio tema da remuneração de conteúdo jornalístico não está distante do contexto brasileiro, tendo sido recentemente esmiuçado pela Câmara de Conteúdos e Bens Culturais do Comitê Gestor da Internet em estudo publicado em maio de 2023 (https://www.cgi.br/publicacao/remuneracao-do-jornalismo-pelas-plataformas-digitais/). Nesses termos, questões tais como aquelas colocadas no âmbito da legislação canadense e, anteriormente, no caso australiano, e mesmo presentes em propostas existentes no Brasil, não podem ser avaliadas como riscos distantes ou menores perante à legítima preocupação e urgência de pautas em que dimensões presentes nos usos contemporâneos da Internet estão sob questionamento. Nesse sentido, a ISOC Brasil acredita que a consideração dos impactos de um marco regulatório nacional a nível da fragmentação da experiência digital de usuários brasileiros é imperativa e intrínseca ao objetivo de constituir regramentos que não inviabilizem as propriedades críticas da Internet como nós a conhecemos.

43. Como devem ser implementadas medidas de reparação e sancionamento no caso de violação das obrigações definidas na regulação de plataformas digitais?

Ainda comuns em diversos países e com um preocupante histórico de tentativas no Brasil, os bloqueios de aplicativos de mensageria instantânea são lembretes e ameaças constantes dos alertas que organizações como a Internet Society e a

Policy Network for Internet Fragmentation têm feito sobre a fragmentação da Internet. Estudos da área têm mostrado que bloqueios de conteúdos, de aplicações e mesmo do acesso local à Internet (https://www.internetsociety.org/blog/2019/12/from-content-blocking-to-national-shutdowns-understanding-internet-disruptions/) ocorrem globalmente sob a justificativa de atendimento a demandas situadas no campo investigação criminal ou, em geral, à necessidade de exercício de pressão judicial e estatal às empresas privadas. No entanto, as diferentes técnicas e escopos de bloqueio (https://www.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview_PT_.pdf) frequentemente negligenciam os custos de possíveis danos colaterais infligidos à sociedade, bem como a potencial ineficácia frente aos problemas a serem enfrentados.

Nesses termos, bloqueios locais de aplicações móveis por meio de determinações jurídicas e regulatórias integram conjunto de medidas que podem restringir o acesso aos conteúdos, serviços e aplicações disponíveis na Internet, fragmentando a experiência que populações inteiras têm da conexão em rede em suas várias facetas. Assim, o capítulo brasileiro da Internet Society traz pontos de atenção aos riscos de se estabelecer um marco regulatório nacional que falhe em adequadamente integrar a gravidade do tema, deixando assim de estabelecer freios e contrapesos que coíbam práticas dessa natureza. Na perspectiva da organização, é deletério que a crescente e legítima demanda nacional por uma experiência digital positiva resulte na aproximação do país a exemplos negativos de prejuízo às propriedades de uma Internet aberta, globalmente conectada, segura e confiável, incorrendo em contrasensos entre intenções e resultados. Nesses termos, preza-se pela antecipação de problemas por vezes inerentes a opções regulatórias pouco amadurecidas e desconectadas do necessário resgate e consideração do que toma parte da operação da Internet como tal.

Os riscos apontados se tornam ainda mais latentes quando o contexto do Brasil é levado em consideração, já que a indevida aposta na determinação de bloqueios aplicáveis genericamente aos cidadãos brasileiros como solução a problemas complexos não é inédita ou rara no país, estando presente em discursos e práticas. A situação pode ser ilustrada pelo histórico do país ao tratar do WhatsApp e do Telegram, os dois mensageiros mais utilizados no país.

CASO DO WHATSAPP

O WhatsApp, que surgiu em 2009 como uma alternativa ao SMS, é um aplicativo de mensagens instantâneas amplamente difundido no cotidiano brasileiro. Contando com mais de dois bilhões de pessoas em mais de 180 países ao redor do mundo, o aplicativo se tornou essencial na vida de diversas pessoas, conectando diferentes gerações e facilitando a comunicação de maneira prática e gratuita.

O Brasil é o segundo país com mais usuários, tendo aproximadamente 147 milhões de pessoas conectadas em 2022. Ainda, o aplicativo está no topo do ranking como a plataforma de mídia social mais usada no país e presente em cerca de 99% dos smartphones.

Para além da comunicação direta entre indivíduos, nos últimos anos se tornou o canal de comunicação oficial de diversas marcas, empresas, instituições financeiras e até setores do judiciário (com inclusive a possibilidade de que oficiais de justiça intimem via whatsapp).

Contudo, a despeito do amplo uso no país, desde 2015, diversas decisões judiciais determinando o bloqueio do aplicativo em todo o território nacional repercutiram e geraram controvérsias. A problemática se inicia com a investigação de organizações criminosas que estariam utilizando o Whatsapp para atividades ilegais, o que levou o judiciário a solicitar a quebra dos dados criptografados da plataforma.

Em resposta, o Facebook - já dono do Whatsapp à época - respondeu que, por conta de inviabilidades tanto técnicas quanto legais, não seria capaz de cumprir a requisição. A situação se repetiu ao longo dos anos de 2015 e 2016 por diversos motivos, levando ao bloqueio do aplicativo de algumas horas a até o dia todo. Em suma, a determinação de bloqueio se dava após o descumprimento de exigências que visavam o fornecimento de dados à justiça, sendo adotada como forma de coação à plataforma para que colaborasse.

Nesse sentido, vale ressaltar que o período em destaque se passa no cenário pré-LGPD (Lei 13.709/2018) e, portanto, não havia lei específica para proteção de dados pessoais. Dessa forma, recorria-se à Lei nº 12.965/2014, Marco Civil da Internet, que assegura a inviolabilidade da privacidade do cidadão e o direito ao sigilo de suas comunicações pela internet e comunicações privadas armazenadas (art. 7º). Ainda, protege os dados pessoais, não permitindo o fornecimento sem consentimento a terceiros.

Entretanto, compreendendo a relevância do aplicativo no país, milhares de usuários ficaram impossibilitados de se comunicar da forma que estavam acostumados durante o período de suspensão. Em manifestação à época, o Comitê Gestor da Internet no Brasil (CGI.br) pontuou a desproporcionalidade da medida adotada pelo Poder Judiciário.

Dentre as questões apontadas pela entidade, uma das principais preocupações se dá em relação ao bloqueio total e indiscriminado de um aplicativo em função do uso deturpado por alguns usuários, o que leva à punição não apenas dos diretamente culpados, mas sim de todos os usuários e, inclusive, da própria plataforma. Nesses termos, resta evidente os riscos que tal medida representa para a unidade da Internet, podendo levar a casos de fragmentação da rede.

Nesse cenário, vê-se o substancial desencontro entre as decisões judiciais e os meios de aplicá-las na prática. São diversas as decisões que não levam em consideração os obstáculos e problemas técnicos - como neste caso, em que se solicitou o fornecimento de dados criptografados.

CASO DO TELEGRAM

De modo semelhante ao que ocorreu ao Whatsapp, o aplicativo de mensageria Telegram passou a ser alvo de suspensões judiciais no Brasil. É importante observar que o Telegram é a principal alternativa ao Whatsapp no contexto nacional. Nesse sentido, portanto, os principais aplicativos de comunicação privada no país têm sido alvos de bloqueios. Importa, ademais, diferenciar que o Telegram foi suspenso em razão de decisões que foram validadas pela alta Corte do país, o Supremo Tribunal Federal (STF), o que torna a questão ainda mais sensível.

No caso Telegram, a primeira suspensão da plataforma ocorreu em 17/03/22, por decisão do STF, após a inércia do aplicativo em excluir a conta do usuário Allan dos Santos, figura pública vinculada a grupos da extrema direita no Brasil. À época, a plataforma ficou mais de dois dias suspensa.

Mais recentemente, após decisões anteriores que previam a suspensão do aplicativo como sanção em caso de descumprimento de requisições judiciais, no dia 26/04/2023, o Telegram acabou por ser suspenso judicialmente, por decisão da Justiça Federal do Espírito Santo. Nesse episódio, a suspensão se deu em razão da negativa da plataforma ao fornecimento de informações que possibilitassem a identificação de usuários neonazistas que atuam no aplicativo.

Tal sanção reacendeu o debate sobre o impacto social e econômico do bloqueio de plataformas digitais, ainda que em razão de decisões que, em tese, buscam garantir direitos humanos fundamentais. Nesse período, a proposta do marco regulatório brasileiro das plataformas digitais também já estava sob discussão (PL 2630/20), de modo que o bloqueio do Telegram respingou nas preocupações sobre as questões de liberdade de expressão, privacidade, autoritarismo e fragmentação da rede.

Ainda em 2022, na primeira suspensão, a organização Artigo 19 já havia alertado que o bloqueio de uma plataforma digital de uso comum e massivo pela população é uma medida desproporcional, ainda que seja realizada a fim de resguardar direitos fundamentais. Isso porque implica em restrição ao exercício de direitos fundamentais de milhões de brasileiros que não concorreram para as ilegalidades que geraram a decisão judicial.

Sobre a suspensão determinada em 2023, o próprio Poder Judiciário reconheceu em 2ª instância, por meio de decisão do Tribunal Regional Federal da 2ª Região, que a determinação sancionatória de bloqueio do Telegram “não guarda razoabilidade, considerando a afetação ampla em todo território nacional da

liberdade de comunicação de milhares de pessoas absolutamente estranhas aos fatos sob apuração".

A CONTRIBUIÇÃO DO BLOQUEIO DE PLATAFORMAS DIGITAIS PARA A FRAGMENTAÇÃO DA INTERNET

O bloqueio de aplicativos em território nacional materializa a fragmentação da rede. Ainda que não o faça em extensão global, a suspensão de um aplicativo imprime uma limitação territorial aos usuários da rede. Isso porque medidas desse tipo impedem que os usuários no Brasil compartilhem informações com usuários em outras regiões no mundo e vice-versa, criando, assim, pontos de rompimento na conexão da rede.

Esses pontos de rompimento, especialmente quando gerados por decisões judiciais ou governamentais, ameaçam a Internet aberta, globalmente conectada e segura, além de resultar em riscos significativos para o Estado Democrático de Direito. Veja-se que o bloqueio de uma plataforma digital de uso comum, e por vezes massivo, pelos usuários brasileiros, afeta o exercício de direitos fundamentais, sobretudo os direitos humanos digitais, tais como o direito ao acesso à Internet, a liberdade de expressão e a livre iniciativa.

A gravidade e desproporcionalidade de decisões de bloqueio de plataformas se torna ainda mais patente ao analisar os impactos extraterritoriais. A exemplo, em decorrência de fatores técnicos, o bloqueio do Whatsapp em território brasileiro provocou consequências em países vizinhos, principalmente Argentina, Uruguai e Chile. Isso ocorre por conta do uso de cabos submarinos e terrestres que transferem a conexão. Assim, além de uma decisão proferida por um Tribunal específico afetar o Brasil como um todo, os prejuízos foram refletidos em territórios internacionais.

Logo, as distorções geradas em razão de bloqueios ainda que parciais da rede afetam liberdades individuais, negócios e até mesmo a defesa da democracia. A esse respeito, há que se destacar que, ao determinar a suspensão de aplicativos, o Brasil se aproxima de realidades políticas autoritárias ao redor do mundo que vêm controlando o acesso à Internet de maneira arbitrária. Sobre isso, os bloqueios da Internet (*shutdows*), que podem ser parciais, completos, temporários ou permanentes, são comuns dentre atos voltados ao controle da opinião pública e à supressão da cidadania.

A campanha KeepItOn da organização AccesNow aponta para o aumento de medidas de bloqueio da rede em países como a Índia, Cuba, Irã, Ucrânia e inclusive Brasil. Ademais, mais recentemente, após as ondas de protestos na França em julho de 2023, o presidente Emmanuel Macron passou a defender a possibilidade de bloqueio das redes sociais no país para controlar os protestos em curso.

Portanto, é necessário ter em conta que assegurar que a Internet permaneça como uma rede aberta, global e livre, conversa diretamente com a proteção de direitos humanos fundamentais. Desse modo, prevenir a possibilidade de bloqueios de plataformas significa evitar bloqueios da própria rede, inclusive a fim de limitar medidas autoritárias por parte do Estado.

APONTAMENTOS SOBRE O USO DO BLOQUEIO DE PLATAFORMAS DIGITAIS COMO SANÇÃO JURÍDICA

O cerne da discussão sobre as decisões judiciais que determinaram medidas de bloqueio de plataformas reside na ausência de proporcionalidade, isto é no sentido de adequação, necessidade e proporcionalidade da decisão para o caso concreto (http://repositorio.ufla.br/bitstream/1/30751/1/Thaís%20Bernardes%20Carvalho%20-%20TCC.pdf), bem como na contestável legitimidade (https://www.conjur.com.br/2021-mar-14/opiniao-legitimidade-decisao-processo-democratico) do uso da medida de bloqueio como sanção em casos de ilegalidades cometidas por usuários.

Nesse sentido, não se busca esgotar o tema, que também encontra relação com a discussão sobre o modelo regulatório da responsabilização de terceiros. Contudo, propõe-se alguns apontamentos para a construção de diretrizes quanto ao bloqueio de plataformas como sanção jurídica.

De início, há que se destacar a necessidade de observância do princípio da legalidade, pois o bloqueio de plataformas como medida sancionatória precisa estar de acordo com o ordenamento jurídico. Contudo, para que isso ocorra, é necessário que a legislação aborde de maneira mais detalhada as hipóteses nas quais o bloqueio poderia ser utilizado ou não como sanção jurídica.

Atualmente, o Marco Civil da Internet (art.12, III) e a Lei Geral de Proteção de Dados (art. 52, X) prevêem a possibilidade da suspensão temporária de plataformas em casos de irregularidades recorrentes no tratamento de dados. Porém, o MCI foi utilizado como base jurídica para fundamentar as decisões de bloqueio de aplicativos, como no caso do Telegram, ainda que tais situações tratem de moderação de conteúdo online e não estritamente de questões referentes ao tratamento de dados.

Outro ponto é que o bloqueio de tais aplicativos, apesar de serem plataformas de uso massivo e diário, costuma surpreender os usuários, que só tomam conhecimento do bloqueio quando este já foi concretizado. Isso agrava os prejuízos econômicos decorrente das suspensões e, ainda que tenham sido previstas em decisões judiciais públicas, tais medidas são pouco transparentes da perspectiva do usuário.

Ademais, há que se observar as peculiaridades do uso da Internet no Brasil. Os casos de bloqueios de plataforma no país tiveram por objeto aplicativos de mensageria, Whatsapp e Telegram especificamente. O brasileiro raramente faz uso de SMS, sendo grande parte da comunicação online feita por meio do Whatsapp. O uso desse tipo de aplicativo é tão difundido no país que as operadoras que fornecem conexão à Internet incluem tais plataformas em suas práticas de *zero-rating*, tornando seu uso mais barato aos usuários. Nesse cenário, o bloqueio sancionatório de plataformas precisa ser estabelecido como medida extrema, a última a ser adotada em caso de necessidade.

Por fim, não se defende que haja desresponsabilização da plataforma digital em favor da integridade da rede. A esse respeito, não se ignora que o Telegram foi um dos aplicativos de mensageria que mais cresceu no Brasil após a implementação de medidas de combate à desinformação por parte do Whatsapp. À época, grupos inteiros de usuários migraram para o Telegram em razão de políticas mais brandas ou inexistentes sobre o compartilhamento de conteúdo falso e/ou legal nessa plataforma.

Logo, medidas para o combate às ilegalidades online precisam ser adotadas em conjunto com esforços das empresas, mas isso não pode resultar em violação dos direitos fundamentais dos usuários não envolvidos em eventuais ilegalidades, preservando também a livre iniciativa.

Assim, a ISOC Brasil ressalta a importância de:

1. Atenção aos riscos de se estabelecer um marco regulatório nacional que falhe em adequadamente considerar a gravidade do tema de bloqueios locais de aplicações móveis por meio de determinações jurídicas e regulatórias, deixando assim de estabelecer freios e contrapesos que coíbam práticas dessa natureza.Instituir princípios sobre a aplicação do bloqueio de plataformas digitais como sanção jurídica, definindo-o como medida extrema, levando em consideração o impacto profundo da suspensão do serviço sobre os usuários e sobre a própria empresa, sob orientação do princípio da proporcionalidade e dos princípios para o uso e governança da internet.

2. Conceber um escopo regulatório robusto e específico sobre o bloqueio de plataformas digitais, a fim de definir diretrizes detalhadas sobre as hipóteses de bloqueio e estabelecer critérios de aplicabilidade, abordando a restrição de seu uso como ferramenta de controle da opinião pública.

3. Estabelecer medidas de maior transparência e publicização quando o bloqueio de plataformas digitais for determinado, com exposição de período de suspensão e razões que a fundamentam, a fim de informar com antecedência acerca da indisponibilidade do serviço para mitigar os impactos econômicos e sociais que serão suportados pelos usuários.