Nota Técnica sobre PL 1429/2020 e PLS 1358/2020, que instituem a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet

14 de maio de 2020

O **Instituto de Pesquisa em Direito e Tecnologia do Recife**[1] e a **Coding Rights**[2], entidades membras da Coalizão Direitos na Rede e atuantes no campo de direitos humanos e tecnologia, apresentam comentários aos Projetos de Lei n. 1429/2020 e 1358/2020, de autoria dos Deputados Tabata Amaral e Felipe Rigoni, e do Senador Alessandro Vieira.

Os Projetos de Lei em questão visam introduzir no Brasil uma Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, por meio de dispositivos relativos a pontos como (a) novas regras a respeito da responsabilização de intermediários na Internet; (b) medidas a serem adotadas por plataformas de redes sociais que proporcionem o combate à disseminação de desinformação e notícias falsas; (c) recomendações de transparência; e, por fim, (d) sanções aplicáveis a disseminação de informações falsas e tipificação da conduta de disseminação por agentes públicos como crime de responsabilidade.

De uma maneira geral, entendemos a preocupação com mecanismos capazes de combater a disseminação das notícias falsas online, ao passo que determinadas práticas online têm se mostrado cada vez mais nocivas contra a garantia do direito de acesso à informação e uma Internet segura. No entanto, é importante ressaltar a importância da preservação do modelo de responsabilização de intermediários introduzido pelo Marco Civil da Internet, ao passo que a lei se preocupou em salvaguardar os direitos dos usuários, promover uma inferência mínima na Internet e garantir o exercício de liberdades e direitos fundamentais como a Liberdade de Expressão.

Em função disso, o presente posicionamento traz alguns pontos sobre os Projetos de Lei em questão, bem como os possíveis riscos apresentados por alguns dispositivos. Para tal, será dividido nas seguintes sessões:

1) Conceitos e vedações do artigo 5º;
2) Modelo de responsabilidade civil de plataformas criado pelo projeto de lei;
3) Transparência das plataformas;
4) Confusão entre conteúdo patrocinado e impulsionamento;

[1] Site do Instituto de Pesquisa em Direito e Tecnologia do Recife: https://ip.rec.br/
[2] Site da Coding Rights: https://www.codingrights.org/

5) Criptografia como ferramenta de garantia de direitos; e
6) Considerações finais.

A presente manifestação usou como base o texto do PL 1429/2020 disponível para consulta pública no site e-Democracia[3].

1. Conceitos e vedações do artigo 5º

O PL traz alguns conceitos que merecem aprimoramento para que não resultem em eventuais limitações impostas à liberdade de expressão ou de outros comportamentos online, como o anonimato, ferramenta necessária para proteger usuários do capitalismo de plataformas e até mesmo para garantir o direito de acesso à informação. De uma maneira geral, temos preocupações com as seguintes definições: (a) desinformação; (b) Conta inautêntica; e (c) disseminadores artificiais.

Iniciando pelo conceito de desinformação do PL, entendemos que o objetivo geral da proposta foi combater o fenômeno, bem como a criação de informações falsas e a sua posterior disseminação. No entanto, ao passo que a definição entende como desinformação o conteúdo "inequivocamente falso ou enganoso, passível de verificação, colocado fora de contexto, manipulado ou forjado, com potencial de causar danos individuais ou coletivos", preocupam-nos os critérios que serão adotados para determinar postagens como tal e, consequentemente, com o fato da proposta em questão deixar a avaliação destes conteúdos para as plataformas de redes sociais, cujas políticas são conhecidamente definidas de uma maneira global e com pouca sensibilidade para questões e práticas regionais.

Em um segundo momento, gostaríamos de apontar os riscos da definição de "conta inautêntica" para um eventual cerceamento de liberdades e identidades online. A proposta identifica como conta inautêntica aquelas criadas com o propósito de disseminação de informação falsa ou assumir a identidade de terceira pessoa para enganar o público. Apesar do PL mencionar que as vedações impostas ao conceito em questão não implicará em restrições ao livre desenvolvimento da personalidade individual, é importante considerar que essa definição e a vedação imposta à ela no artigo 5º podem acabar resultando restrições à Liberdade de expressão, bem como do direito à privacidade.

No limite que o Projeto de Lei visa coibir a criação de perfis que assumam identidade de terceiras pessoas ele, ao mesmo tempo, limita o uso de pseudônimos ou o pseudo anonimato na Internet[4]. Iniciativas legislativas que promovem uma identificação massiva de usuários ou até um cerceamento do anonimato acabam limitando a gestão de identidades, prática importante para garantir a segurança e privacidade de todos nós, dado que navegamos em um ambiente online que tem como modelo de negócios predominante o extrativismo massivo de nossos dados pessoas que, por sua vez, são

[3] Link para a Consulta Pública: https://edemocracia.camara.leg.br/wikilegis/p/12-lei-brasileira-de-liberdade-responsabilidade-e-transparencia-na-internet/

[4] Sobre a questão do anonimato na Internet, Bruce Schneier, acadêmico americano e pesquisador em temas de segurança, traça algumas considerações em um post de 2010: https://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html

utilizados para venda de perfis de cidadãos. Poder dissociar nossos perfis é uma prática saudável e segura, até mesmo em caso de vazamento de informações. Além disso, por vezes, o livre acesso à informação é também dependente de que se possa fazer uso de pseudônimos e perfis anônimos, por exemplo, entre muitos outros casos, jovens ou adolescentes que estejam buscando informações sobre educação sexual ou diversidade de gênero podem se sentir constrangidos se não puderem utilizar a pseudonímia.

O dispositivo ainda passa uma presunção equivocada de que apenas contas que adotem pseudônimos são propagadoras de informações falsas. Esse cenário, ante a polarização política enfrentada no contexto brasileiro e somada à ausência de salvaguardas no processo de identificação de um determinado conteúdo como desinformação, pode acabar resultando na remoção indevida de contas de usuários determinado espectro político que utilizem pseudônimos - por exemplo.

Adicionalmente à discussão de anonimato, o PL também pode vir a cercear o registro de contas em redes sociais que possuam identidades de gênero diferentes das registradas em documentos oficiais e limitar a utilização de nomes sociais, tão relevantes para a identidade de gênero de muitos indivíduos.

Sobre a definição e vedação de contas inautênticas, uma possível leitura é a de que o PL pode ser permissivos para a propagação de informações falsas, desde que elas venham de uma conta identificada e cuja identidade corresponde a do real autor do conteúdo. Aqui, a identificação de usuários e autoria dos posts pode conferir uma falsa noção de que (a) a disseminação está correndo apenas por estes meios e (b) que os autores identificados são os disseminadores exclusivos. Entretanto, o contexto brasileiro deixa bastante claro que dados pessoais de indivíduos podem ser utilizados desautorizadamente para o registro de contas em redes sociais e compras de chips de telefonia móvel - em ambos os casos pode se tratar de um disseminador que se assemelha a uma pessoa real.

A respeito do conceito de disseminadores artificiais, entendemos que a definição pode acabar abarcando bots e contas automatizadas que não sejam utilizados para a disseminação ou impulsionamento de conteúdo falso. Entendemos a intenção da proposta em coibir a utilização maliciosa de automação; no entanto, é importante ressaltar que também existem uso de bots em redes sociais que são utilizadas de uma maneira positiva e em processos que podem conferir mais transparência às instituições públicas ou promover acesso à informação e participação popular. Por exemplo, a Rosie, bot do twitter que analisa e identifica suspeitas em gastos de deputados federais em exercício de sua função, ou a Beta, bot do facebook que traz informações sobre temas de gênero que são discutidos no Congresso Nacional. Para não limitar o surgimento desse tipo de inovações cívicas, é importante que a lei seja focada em uma conduta bem específica e não amplamente em uma tecnologia (ex. uso de bots).

Essa definição, somada à vedação de disseminadores artificiais não rotulados presente no artigo 5º, pode vir a promover um escrutínio de ferramentas que utilizem automação e resultará em um processo massivo de identificação das situações onde a tecnologia é aplicada. Aqui, ao invés de focar no disseminador artificial não comunicado ao provedor de aplicação, a proposta de lei deveria se dedicar a

aperfeiçoar a proibição daqueles utilizados para a disseminação de desinformação de uma maneira que não resulte em um cerceamento de liberdades individuais.

2. Modelo de responsabilidade civil de plataformas criado pelo projeto de lei

A Lei 12.965/2014, conhecida como Marco Civil da Internet, foi responsável por introduzir um modelo de responsabilidade aplicável aos provedores de aplicações de Internet - incluindo as redes sociais - em casos de danos decorrentes de conteúdo gerado por terceiros. À época da redação da Lei em questão, a preocupação foi encontrar um modelo de responsabilidade que não onerasse tanto as plataformas por conteúdo gerado por terceiros ao mesmo tempo que previa algumas ações a serem tomadas ante a emissão de uma ordem judicial[5].

Em debates onde se busca uma maior responsabilização de indivíduos e plataformas por conteúdos de terceiros, como é o caso do Projeto de Lei em questão, é importante ressaltar a necessidade de conciliação da obrigação de garantia de liberdade de expressão com a coibição de eventuais práticas que resultem em censura na Internet. Nesse sentido, apesar de compreendermos os riscos apresentados pela desinformação - inclusive relativos ao livre exercício de direitos fundamentais tal qual o direito à saúde, que assume uma relevância ainda maior no cenário da pandemia -, atentamos para o papel fundamental do Poder Judiciário neste processo e pela posição adotada pelo MCI referente à responsabilidade subjetiva de tais provedores. As plataformas somente se tornam responsáveis quando descumprem uma ordem judicial. Isso é necessário para que não sejam elas as detentoras de um poder de decisão sobre os conteúdos que circulam na rede.

Nesse sentido, seria importante que eventuais novas legislações aprovadas no Brasil a respeito do tema das Fake News e Desinformação não sejam responsáveis por conferir às plataformas alto grau de responsabilidade (objetiva) e amplo poder de regulação, correndo o risco de transferir aos provedores de aplicação a capacidade de decidir o que deve e o que não deve ser veiculado nas redes. Inclusive porque o Poder Judiciário, ao decidir sobre a responsabilidade das plataformas em relação a conteúdo gerado por terceiro, faz a ponderação e o juízo de valor sobre o conteúdo veiculado e os direitos por ele atingidos, primando pela garantia do devido processo legal, sendo este, portanto, o procedimento mais adequado para esses casos.

Por fim, em seu artigo 28, o Projeto de Lei traz algumas sanções aplicáveis aos provedores de aplicações de Internet. Aqui cumpre destacar que (a) a imposição de sanções nas esferas civil, criminal e administrativa; bem como (b) a ausência de entidade responsável, no âmbito da Administração Pública, podem gerar insegurança jurídica para a atuação das empresas em questão. De maneira geral, o temor é que se incentive uma prática massiva de remoção de conteúdo para evitar responsabilização. Justamente algo que o Marco Civil da Internet tentou evitar.

---

[5] O artigo 19 da mencionada Lei é redigido da seguinte forma: *"Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário."*

Além disso, cabe ressaltar que estudos apontam que nem sempre a remoção de conteúdo que dissemina desinformação é o método mais eficiente de lidar com as chamadas fake news. Em alguns casos, sinalizar na próprio post que o conteúdo traz desinformação tem mais alcance do que deletar e postar conteúdo que contradiz, mas não tem os elementos de choque, surpresa, escândalo, etc que chamam a atenção, tão característicos dos posts de desinformação. Nesse sentido, o algoritmo das plataformas também acaba sendo uma questão na disseminação de tais postagens.

3. Transparência das plataformas

Embora o Marco Civil estabeleça uma salvaguarda na responsabilização das plataformas, por si mesmas, elas optam por remover conteúdos. Muitas vezes, esbarrando na liberdade de expressão de seus consumidores, e outras, deixando disponíveis conteúdos que na legislação brasileira são considerados crime, como é o caso de conteúdos racistas. Nesse sentido, é importante e tem sido recomendação[6] recorrente de várias organizações da sociedade civil que essas plataformas sejam transparentes, publicando relatórios sobre essas práticas de moderação de conteúdo, para além dos relatórios de transparência que apresentam informações de remoções por ordem judicial.

Nesse sentido, a princípio, é bem visto que o Projeto de Lei em questão traga dois pontos importantes sobre transparência das plataformas: a Seção II do Capítulo II, que fala sobre o dever de transparência dos provedores de aplicação, e o Capítulo III, que regula os deveres de transparência em relação a conteúdos patrocinados.

O primeiro ponto diz respeito, em síntese, à publicação de relatórios de transparência por parte dos provedores de aplicação, fazendo constar algumas informações que os referidos relatórios devem conter. Tais medidas são importantes para que os usuários tomem conhecimento de como essas plataformas se comportam em relação à moderação de conteúdos.

Entretanto, como destacado acima, o conceito equivocado de "disseminadores artificiais" continua presente, trazendo insegurança sobre o que se enquadra neste termo e, por consequência, o que é exigido dos provedores de aplicação quando se refere ao "número total de disseminadores artificiais, redes de disseminação artificial e conteúdos patrocinados destacados, removidos ou suspensos".

Por fim, quando se fala do fomento à transparência das plataformas, é importante discutir a necessidade de políticas e justificativas mais claras de remoções de conteúdo, bem como da presença de mecanismos de apelação capazes de garantir o contraditório e o devido processo legal para os usuários. Conforme disposto acima, o PL deixa a remoção de conteúdos e contas, bem como a delimitação de critérios a cargo das plataformas em questão e, dessa maneira, acaba por reproduzir o cenário atual onde os usuários ficam a cargo das políticas internas das empresas, que pouco se

[6] Recommendations on technology-related Violence Against Women (VAW) for the UN. Disponível em : https://medium.com/codingrights/recommendations-on-technology-related-violence-against-women-vaw-for-the-un-75d8c885c0a0

atentam para questões mais específicas de conteúdos e que, no limite, podem vir a incidir em censura do livre discurso.

Sobre a remoção de conteúdos com base em políticas de comunidade de termos de uso, em 2018, a Coding Rights teve um post removido dos stories de sua conta no instagram por uma alegada violação das políticas da comunidade[7]. O post em questão eram um gif de uma sapinha dançando, em comemoração ao Dia da Visibilidade Lésbica cuja justificativa de remoção foi baseada na possibilidade do post propagar discurso de ódio. Aqui, mais uma vez, vale ressaltar a importância da participação dos mais diferentes grupos e setores da sociedade na concepção de políticas de moderação de conteúdo a fim de evitar que elas acabem silenciando grupos minoritários.

4. Confusão entre conteúdo patrocinado e impulsionamento

Há ainda, na nossa avaliação, uma confusão primordial no Projeto de Lei, quando ele se refere a conteúdo patrocinado. O conceito apresentado no art. 4º, VIII, expressa "qualquer conteúdo criado, postado, compartilhado ou oferecido como comentário por indivíduos em troca de pagamento pecuniário ou valor estimável em dinheiro".

Ocorre que o referido conceito engloba algumas práticas comuns atualmente e que em nada se relacionam com a disseminação de notícias falsas na Rede, como por exemplo os conteúdos patrocinados veiculados por influenciadores digitais. Por este conceito, portanto, os influenciadores digitais, que firmam contratos com empresas para promover seus produtos e, com isso, auferir renda, serão obrigados a informar à plataforma que estão veiculando postagens patrocinadas (art. 5º, IV) e os provedores de aplicação serão obrigados a tornar públicas as informações referentes a estes contratos, como o pagador do conteúdo, incluindo intermediários, bem como as suas informações de contato (art. 20, I, II e III), o que, conforme já exposto, é uma infração à LGPD.

A respeito da requerida transparência em relação a conteúdos patrocinados, o PL acerta na exigência de identificação do conteúdo pago ou promovido (art. 20, I), mas comete alguns equívocos quando exige a divulgação do responsável pelo pagamento, incluindo intermediários, com a divulgação, inclusive, de informações de contato (art. 20, II e III). Trata-se de incompatibilidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), ferindo a privacidade do usuário, razão pela qual entendemos que essas exigências não podem ser feitas e recomendamos a supressão desses dispositivos.

Além disso, a provisão de identificação de anunciante - com a listagem de nome e informações de contato pode vir a ser um pouco abusiva ao passo que promove a divulgação de dados pessoais desproporcionalmente. Aqui, a aplicação do princípio da publicidade faria sentido se o PL estivesse se referindo a anúncios públicos e impulsionamentos contratados pela Administração Pública, fomentando mais transparência para a publicidade digital contratada com dinheiro público.

---

[7] Postagem no instagram da Coding Rights a respeito da remoção de stories sobre o Dia da Visibilidade Lésbica - https://www.instagram.com/p/B17E4olJ7A0/?igshid=1vu18r4k7jxg8

O que se percebe, portanto, é que o PL almeja a fiscalização de conteúdos falsos impulsionados ou disseminados em massa, com a contratação de agências específicas para este fim, mas acerta em práticas legítimas de publicidade online, as quais já têm sua regulação e consequente fiscalização definida e realizada pelo CONAR, de forma que não se faz necessária, por enquanto, uma modificação desse sistema.

5. Criptografia como ferramenta de garantia de direitos

O PL se debruça também sobre a disseminação de notícias falsas em plataformas de mensageria privada. O texto disponível para comentários no E-democracia da Câmara dos Deputados expressa no art. 16 que os "os provedores de aplicação que prestarem serviços de mensageria privada devem utilizar todos os meios ao seu alcance para limitar a difusão e assinalar aos seus usuários a presença de conteúdo desinformativo". Entretanto, os autores não levam em consideração a utilização de criptografia ponta-a-ponta de que fazem uso, em maior ou menor medida, os principais e mais populares serviços dessa natureza.

A criptografia ponta-a-ponta é um protocolo que garante o sigilo, a integridade e a autenticação de mensagens trocadas entre duas ou mais pessoas. O protocolo garante que um terceiro, estranho à comunicação, incluindo a própria aplicação, não tenha acesso ao texto puro das mensagens por ela trocadas. Mesmo que as chaves de encriptação de um usuário sejam fisicamente comprometidas, elas não poderão ser utilizadas para decriptar mensagens passadas, garantindo, portanto, o sigilo da comunicação.

Nesse sentido, o art. 16 do PL em comento põe às plataformas de mensagem instantânea uma obrigação que elas não podem cumprir por uma limitação técnica da aplicação, já que elas não têm acesso ao conteúdo das mensagens trocadas e não conseguirão, por conseguinte, assinalar que o conteúdo é desinformativo.

Todavia, a utilização de criptografia ponta-a-ponta jamais pode ser encarada como um empecilho para a regulação das plataformas. Organismos internacionais de defesa dos direitos humanos, como a UNESCO[8] e a Anistia Internacional[9], assim como especialistas em criptografia, argumentam que o uso de técnicas criptográficas ajuda a proteger e a viabilizar o exercício de direitos humanos, tais como direito à privacidade e à liberdade de expressão. Adicionalmente, o Conselho de Direitos Humanos da ONU reconheceu, em resolução recente sobre a Promoção e proteção de todos os direitos humanos, civis, direitos políticos, econômicos, sociais e culturais, incluindo o direito ao desenvolvimento[10], a "necessidade de implementação de soluções técnicas para proteger a confidencialidade das comunicações digitais, incluindo medidas de criptografia e anonimato" e a sua importância para o exercício dos direitos humanos - em particular os direitos à privacidade, à liberdade de expressão e à liberdade de reunião e associação pacífica.

---

[8] Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000246527
[9] DIsponível em: https://www.amnestyusa.org/reports/encryption-a-matter-of-human-rights/
[10] Resolução do Conselho de Direitos Humanos da Organização das Nações Unidas - A/HRC/38/L.10/Rev.1 - https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1

Por fim, com relação à incorporação de medidas de transparência em conteúdos patrocinados ou disseminação de fake news no whatsapp/chats de mensageria encriptados, talvez seja interessante explorar soluções técnicas de identificação aplicadas àqueles conteúdos reconhecidamente falsos sempre que uma mensagem é enviada ou recebida. Uma solução conhecida é a utilização de hashes encriptadas[11] adotada para impedir a propagação de conteúdos como os relativos a abuso ou exploração infantil, e que teve como meta não violar a privacidade do usuário.

6. Considerações finais

Os Projetos de Lei que se propõem a ser a "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet" se perdem nesses três propósitos ao (1) limitar a liberdade dos usuários de usar pseudônimos ou contas automatizadas em aplicativos de mensageria ou em redes sociais, para qualquer finalidade não relacionada à disseminação de notícias falsas, ou seja, para usos completamente legítimos e inofensivos; (2) ampliar a responsabilidade das plataformas para além do previsto no Marco Civil da Internet, desrespeitando o regime robusto de responsabilidade civil por ele construído; e (3) exigir, sob o manto da transparência, a divulgação de dados pessoais dos responsáveis pelo conteúdo patrocinado, ferindo o disposto na Lei Geral de Proteção de Dados.

Adicionalmente, ao tentar combater práticas de disseminação de conteúdos falsos na rede, a proposta em questão coloca em risco o anonimato, a autodeterminação de identidades e a Liberdade de expressão, princípios fundamentais para uma Internet aberta e livre.

Ainda, os PLs não conseguem atingir o objetivo de combater o maior problema quando se trata de desinformação, que é sua disseminação em massa. Ao contrário, os PLs regulam contas falsas (inautênticas) ao invés do conteúdo falso, além de colocar entraves à propaganda, que já tem regulação originada do CONAR, sob a moldura de conteúdo patrocinado.

Por isso, é opinião do Instituto de Pesquisa em Direito e Tecnologia do Recife e da Coding Rights que, embora trate de temas relevantes, os presentes Projetos de Lei apresentam falhas técnicas importantes e que, por isso, necessita de muitos aprimoramentos e uma ampla discussão com todos os setores interessados, para além do breve prazo de 10 dias propostos na consulta pública, a fim de que não resulte em um texto final que restrinja direitos e liberdades individuais.

IP.REC
https://ip.rec.br/
contato@ip.rec.br

CODING RIGHTS
www.codingrights.org
contact@codingrights.org

[11]Um Hash é um valor atribuído, uma espécie de assinatura digital eletrônica de um grande conjunto de dados, adotada por plataformas como o Whatapp - https://gizmodo.uol.com.br/whatsapp-criptografia-analise/