Instituto de
Pesquisa em
Direito & Tecnologia
do Recife

NOTA TÉCNICA

TEXTO DO GOVERNO FEDERAL SOBRE O PL 2630

INTRODUÇÃO

O Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec, entidade sem fins lucrativos que atua na defesa de direitos humanos no ambiente digital, acompanha com atenção o debate de regulação de plataformas, materializado no PL 2630/2020, desde a primeira versão do projeto e vem, através da presente nota técnica, contribuir para o debate legislativo, realizando uma análise de pontos principais da proposta de texto do Governo Federal enviado para a Câmara dos Deputados para debate.

O texto do projeto de lei, aprovado em 2022 no Grupo de Trabalho da Câmara dos Deputados, avançou em relação àquele aprovado no Senado, mas teve sua urgência rejeitada no plenário da Câmara e desde então se encontra sem movimentação.

A discussão desta matéria é importante porque trata-se de uma oportunidade para estabelecer uma regulação de plataformas digitais compatível com os direitos fundamentais, além de fornecer ferramentas legais para lidar com fenômenos do tempo atual como a desinformação e o discurso de ódio, dentre outras práticas nocivas.

Nesse sentido, faz-se necessário o estabelecimento de parâmetros para que as empresas tenham a transparência como regra de suas ações e, ao mesmo tempo, respeitem direitos como privacidade e liberdade de expressão, coibindo condutas abusivas e nocivas ao debate público. Por outro lado, a tentativa regulatória deve levar em conta, como pressuposto, o rigor técnico-jurídico e os indicativos científicos interdisciplinares, de modo a criar novo diploma legal capaz de ter eficácia na garantia de direitos e não na redução das conquistas sociais protegidas constitucionalmente.

A proposta, analisada parcialmente nesta nota técnica, é apresentada pelo Governo Federal como contribuição ao debate legislativo. Permeada por um contexto político delicado, que se materializou nos ataques de 8 de janeiro de 2023 aos prédios-sede dos poderes da República em Brasília, busca dar respostas a discursos extremistas e anti democráticos como os que incentivaram os atos ocorridos na Capital Federal, que se utilizaram das redes sociais e plataformas de mensageria privada para amplificar sua abrangência.

Entretanto, como restará demonstrado na presente nota, não se trata da melhor resposta regulatória, considerando a complexidade da Internet e das operações das plataformas digitais, bem como suas especificidades. Além disso, nota-se um descompasso entre esta proposta legislativa e outros diplomas legais vigentes, como o Código Penal, o Marco Civil da Internet (MCI), a Lei Geral de Proteção de Dados(LGPD), entre outros.

1 A INCIDÊNCIA DA LEI E A INCORREÇÃO NO MANEJO DOS CONCEITOS

Da leitura do art. 1º da proposta, observa-se que a norma proposta incide sobre **todos** os provedores de aplicação de Internet do tipo plataforma digital de conteúdo de terceiros que oferecem serviços ao público brasileiro e exerçam atividade de forma organizada, sendo que, algumas normas incidem, unicamente, sobre os de grande porte, definidos como os que possuem mais de 10 milhões de usuários (art. 2º, inc. XIII).

É importante notar ainda que a **não incidência da lei** sobre certos tipos de plataformas apresenta-se como um fator positivo do projeto, pois favorece a livre disseminação do conhecimento, a inovação tecnológica e o compartilhamento de softwares abertos (art. 1º, § 4º, inc. I).

Além dessas, outras plataformas digitais estão fora do contexto da lei, como as de reuniões virtuais por vídeo ou voz (art. 1º, § 4º, inc. II) e as de comércio eletrônico de produtos (art. 1º, § 4º, inc. III) que, pela natureza específica dos serviços ofertados, demandam regulamentações específicas como na área de direito tributário, por exemplo.

1.1 A DISCREPÂNCIA DOS CONCEITOS LEGAIS (art. 2º)

Um dos problemas verificados na redação da proposta governamental é a completa falta de padronização conceitual no que se refere às plataformas a quem a regulação é direcionada.

Não há uma conceituação do que seriam exatamente as “plataformas digitais de conteúdo de terceiros”, termo repetidamente utilizado no texto. Uma vez que o termo não é definido em outros instrumentos legais, como o Marco Civil da Internet (MCI) ou a Lei Geral de Proteção de Dados, e aparece cerca de 35 vezes no texto em análise, faz-se necessária a criação da categoria.

A falta de uma padronização conceitual dos termos jurídicos e a quem eles se destinam tem uma dupla ordem de consequências negativas: a primeira, é a quebra da tendência de diminuição de complexidade temática, pelo legislador, com a criação de artigos iniciais que apontam rol de conceitos, como aconteceu no Marco Civil da Internet, na Lei Geral de Proteção de Dados e outras legislações; a segunda, está relacionada ao fato de que a ausência desta correta padronização, lógica e semanticamente ordenadas, compromete a aplicação da lei, tornando-a inócua. O fundamento está na disparidade cognitiva-informacional entre o regulador-aplicador e o objeto regulado.

Em boa técnica legislativa, poder-se-ia considerar seguir os padrões conceituais adotados no MCI e, caso houvesse a necessidade de tratar de novas tecnologias, com características peculiares não abordadas em leis anteriores, trazendo conceitos e/ou terminologias inéditas ao mundo jurídico.

Para o caso específico, seria considerar o termo “provedor de aplicação” do Marco Civil da Internet como gênero e criar as espécies a partir da nova regra, determinando, de forma específica, o seu campo semântico mínimo.

Não se pode afirmar que a proposta é feliz no ponto. Na verdade, analisado o texto, verifica-se uma grande confusão, em que se misturam termos diferentes como se sinônimos fossem, sem qualquer estrutura lógica de derivação conceitual, como sói ocorrer em legislações com potencial de eficácia regulatória.

Historicamente, a estrutura conceitual de abordagem dos “provedores” na Internet brasileira, no âmbito pré-Marco Civil da Internet, já foi mais granular. Entretanto, por opção do legislador e visando regular os aspectos importantes naquele momento histórico, a lei de

regulação base da Internet brasileira trouxe uma dicotomia fundamental: provedores são aqueles que fornecem a conexão e as aplicações.

Ao menos duas razões principais podem ser destacadas: do ponto de vista técnico, a rede mundial de computadores é explicada e implementada concretamente em ao menos dois modelos (TCP/IP e OSI). Ambos os modelos deixam evidente que existe uma dimensão infraestrutural, a ser protegida contra todo aspecto de discriminação de tráfego. Para todos os casos, o MCI trouxe regramento específico (neutralidade da rede), mas o corte categorial do "provimento de conexão". As demais camadas ficam classificadas como "provimento de aplicação", nelas não se destaca o aspecto infraestrutural, mas a superestrutura de conteúdos. O que está, portanto, acima do transporte, em ambas as classificações estruturais da rede, é o objeto principal das intenções regulatórias analisadas aqui[1].

As aplicações da Internet se diversificaram e ganharam, portanto, relevância superestrutural no contexto geopolítico mundial. A diversidade e diferença específica é clara: não se pode juntar, num mesmo balaio, grandes plataformas (de redes sociais e outros serviços) e enciclopédias online colaborativas. Entretanto, ressalta a atecnia jurídica e computacional do texto proposto.

Veja-se, por exemplo, com base no Relatório Amostral de Conceitos Relativos à Responsabilidade Civil, publicado pelo IP.rec[2], que a profusão de conceitos pode, sob o pretexto de granularizar o tratamento, transformar o sistema jurídico numa grande colcha de retalhos - no documento citado, concluímos que a Austrália se transformou numa complexa rede conceitual cuja eficácia, em comparativo anacrônico com um cenário futuro brasileiro, pode nos levar à paralisia e não à resolução de conflitos.

O equívoco de tratar grandes players como se fossem sinônimo exato da categoria reforça o quadro, pondo em risco a própria estrutura da Internet e não dando guarida às legítimas medidas regulatórias e comprometendo novas iniciativas que ampliam a cultura e os direitos sociais.

O ponto, portanto, merece um tratamento rigoroso do ponto de vista semântico, jurídico e técnico-computacional. A hipótese que se apresenta, a partir de nossos estudos, é que diversos termos foram transplantados de forma apressada de textos regulatórios como o *Digital Services Act Europeu*, criando um ruído entre os nomes (significantes) e os significados atrelados.

Por fim, do ponto de vista Judicial e Administrativo, na qual tais conceitos receberão sua concretude prática - tanto sob o aspecto fiscalizatório, como sob o aspecto

---

[1] Ainda como discrepância no âmbito conceitual, questionamos se existem ferramentas de busca que não se utilizam de aplicações que indexam conteúdos de terceiros. O tratamento conceitual dado pelo De acordo com o art. 2º, inc. IX, os indexadores de conteúdo não está congruente. Ademais, o conceito legal para "indexadores de conteúdos" afasta-se do padrão adotado no projeto, que deveria classificá-lo como "aplicação" e não como "provedor de aplicação", a exemplo dos conceitos de "ferramenta de busca de conteúdo de terceiros" (art. 2, inc. VIII), "rede social" (art. 2, inc. V) e "serviço de mensageria instantânea" (art. 2, inc. V).

[2] Ver. Relatório Amostral Norte Sul Global de Conceitos Relativos à Responsabilidade Civil de Intermediários na Internet. Vol. 2. Disponível em: < https://ip.rec.br/publicacoes/relatorio-amostral-norte-sul-global-de-conceitos-relativos-a-responsabilidade-civil-de-intermediarios-na-internet-volume-2/ >

sancionatório -, as falhas apontadas irão gerar uma profusão de interpretações inautênticas e divergentes, abarrotando o Judiciário e criando uma tensão a ser resolvida pelos processos de uniformização de jurisprudência.

1.2 A AUSÊNCIA DE PRINCÍPIOS E FUNDAMENTOS

No texto proposto de alteração do projeto de lei, também não foram identificados **princípios**, como aqueles que norteiam o projeto da Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet e como há explicitamente no MCI (art. 3º) e na LGPD (art. 6º).

Os princípios da necessidade, proporcionalidade e não-discriminação são apenas citados para orientar a definição dos termos e políticas de uso das plataformas digitais de conteúdos de terceiros, quanto à moderação de conteúdo (art. 4º, parágrafo único) Sequer há referência de se considerar os princípios das leis pretéritas, através do método de interpretação sistemático.

O art. 3º enuncia os **fundamentos**, dentre os quais merece questionamento se o inciso VIII ("*a adequada identificação de publicidade de plataforma e impulsionamento, seus agentes, e o combate à publicidade e impulsionamento enganosos ou abusivos*") alude a objetivo a ser alcançado, e não a um fundamento que expressamente regula as normas jurídicas proposta.

Mais uma vez há uma tendência histórica no processo regulatório de tecnologia: ainda que não sejam manejados na melhor e relevante técnica jurídica, há um processo evidente do legislador de atrelar às leis específicas da área um rol de fundamentos (qual a base da lei?), um rol de objetivos (qual o programa para o qual a lei ruma, na sua pretensão regulatória?) e um rol de princípios (quais as balizas interpretativas a serem consideradas no subsistema que a lei se insere ou instaura?)

Nenhuma dessas considerações estão explicitadas no texto proposto pelo Governo Federal, o que compromete, sem dúvidas, a eficácia futura do texto que, tal qual no ponto anterior, estará à mercê de interpretações criativas e voluntarismo dos aplicadores. Tal cenário não se coaduna com uma regulação rígida, pró-democracia e cristalizadora de direitos.

2 A RESPONSABILIDADE DAS PLATAFORMAS DIGITAIS DE CONTEÚDOS DE TERCEIROS DE GRANDE PORTE - DEVER DE CUIDADO

No que diz respeito às plataformas de grande porte, isto é, plataformas de conteúdo de terceiros que, nos termos do texto, possuam mais de 10 milhões de usuários[3], o art. 12 determina que elas terão o dever de atuar de forma diligente e em "prazo hábil e suficiente". O artigo estabelece, dessa forma, um rol de conteúdos ilegais relativos aos crimes que as

[3] Sobre a quantidade de usuários que determina a categoria de "plataforma de grande porte", importa citar o relatório já citado e o volume 1 da mesma série. Disponível em: < https://ip.rec.br/areas/regulacao-de-provedores-da-internet/ >

plataformas têm o dever legal de combater dentro de seus serviços, de modo que a omissão em relação a esses conteúdos poderá gerar sua responsabilização. Importa destacar, de pronto, que, qualquer que seja o resultado desta disposição, um rol desta espécie, que aponta para aumento de restrições com bases em tipos penais é, e deve ser interpretado, como taxativo.

Dentre os crimes listados no artigo, estão aqueles contra o Estado Democrático de Direito; os de terrorismo; contra crianças e adolescentes; os resultantes de preconceito de raça ou de cor; contra a saúde pública; os de indução, instigação ou de auxílio a suicídio ou a automutilação; e os de violência de gênero, inclusive aquela definida na Lei 14.192/21. Trata-se de uma enorme quantidade de tipos penais, cerca de 66 condutas criminosas, que deverão ser analisados pelas plataformas para que, se considerados como ilegais, sejam prontamente removidos por elas, conforme dispõe o dispositivo legal.

De acordo com com o art. 13, as plataformas de grande porte poderão ser responsabilizadas subsidiariamente pelos danos causados por conteúdos gerados por terceiros que constituam prática ou incitação aos crimes previstos no art. 12 - isso quando verificado conhecimento prévio e o descumprimento de dever de cuidado pelas plataformas nos termos do §1° do art. 12.

Para análise do **conhecimento prévio**, será avaliada a existência de notificações sobre a presença de conteúdos ilegais feitas a partir dos mecanismos de denúncia que as plataformas devem criar, conforme determina o art. 14. O §3º deste artigo deixa claro que se presume o conhecimento pela plataforma sobre seu conteúdo ilícito a partir da existência de notificações em seus canais de denúncia, o que exigirá uma atuação diligente dela em resposta a isso.

Em relação ao **dever de cuidado**, conforme dispõe o § 1º, serão levadas em consideração questões como a atuação da plataforma digital em relação aos deveres previstos no caput; a avaliação dos relatórios periódicos previstos; o cumprimento da obrigação de adaptação dos sistemas e o cumprimento das obrigações de adaptação de processos para atender o previsto no projeto de lei, não cabendo, de acordo com o § 2° do art. 12, uma avaliação sobre o tratamento individual de conteúdos, apenas de aspectos gerais conforme estabelecido no §1°.

O § 6 do art. 14 ainda estabelece que as plataformas deverão criar um canal de comunicação direto com o poder público para facilitar o intercâmbio de informações que, supostamente, facilitariam a prevenção e identificação da autoria e da materialidade dos crimes previstos no art. 12 desta Lei.

Da forma como está posto, todo esse sistema traduzido pelos arts. 12, 13 e 14 propõe, na verdade, que as plataformas realizem um julgamento prévio sobre o teor do conteúdo que circula em seus serviços para determinar se ele se enquadra ou não no suporte fático das normas incriminadoras listadas no artigo 12. Acontece que, de acordo com a Constituição Federal, a função de interpretar e aplicar a lei é exclusiva do Poder Judiciário (ainda mais quando se trata de matéria penal), de modo que delegar essa função para as plataformas viola frontalmente princípios constitucionais como o devido processo legal (art. 5°, inciso LIV, da CF/88) e a presunção de inocência (art. 5°, inciso LVII, da CF/88), além de usurpar a reserva legal de jurisdição do Poder Público. Neste sentido, é

bem provável que este artigo, da forma como está estruturado, tenha sua constitucionalidade questionada nos foros pertinentes.

É importante notar, também, que isso aumentaria ainda mais o poder das plataformas, já que, além de controlar grande parte do fluxo informacional na Internet, elas também poderiam decidir sobre, expressamente, indícios de autoria e materialidade de conteúdos publicados por usuários brasileiro na Internet. Há um patente contrassenso, considerando que um dos objetivos de regulação dos modelos de negócio dessas plataformas é justamente tentar reduzir o poder e a assimetria informacional dessas empresas.

Além disso, partindo do pressuposto que grande parte da moderação de conteúdo é automatizada, não é possível garantir que os algoritmos utilizados possuam a capacidade técnica suficiente para distinguir, com segurança, o material ilegal daquele que é legal. O tema é técnico, mas, também, jurídico: a linguagem jurídica possui sentidos que não são corriqueiros e essa semântica ainda não é apreendida com devida acurácia pelos modelos utilizados. Os melhores e mais eficazes, por outro lado, envolvem altíssimo custo de operação.

Diante disso, o mais provável a ocorrer é a retirada massiva de todo conteúdo que represente, minimamente, um risco para as empresas, de modo que conteúdos legítimos possivelmente serão perdidos nessa atuação "diligente" das plataformas. Consequentemente, criar-se-ia um o chamado *chilling effect*, ou efeito inibidor, que impactaria diretamente o exercício do direito à liberdade de expressão nessas plataformas de grande porte. Somado ao estado da arte e custo de operação de modelos automatizados, teríamos uma redução da esfera de direitos garantidos sem a segurança, sequer, de uma compensação em termos de redução de danos relativos à desinformação ou discurso de ódio e criminoso.

Outro ponto que chama atenção é a contradição entre o art. 13, que estabelece os requisitos para responsabilização das plataformas de grande porte, e o § 2° do art. 12, que prevê a avaliação do conjunto de medidas adotadas para determinar o descumprimento de um dever de cuidado. Isso porque, mesmo sem levar em consideração questões pontuais, a simples notificação de um usuário nos canais de denúncia configura-se como conhecimento prévio da plataforma sobre conteúdo ilícito. A ciência sobre isso gera a exigência de atuação diligente por parte do provedor de aplicação para "apurar a ilegalidade da publicação". Caso não o faça, será responsabilizada.

Há ainda um problema operacional nessa determinação: em plataformas nas quais não existem grupos ou comunidades, como é o caso do TikTok, do Instagram e do Twitter, a moderação de conteúdos ocorrerá no próprio perfil do usuário e no *feed*, referenciando a conta que teve a publicação indisponibilizada. Dessa forma, o monitoramento coletivo acaba sendo também, em última instância, um monitoramento individual.

Por fim, é importante notar ainda que o PL não revoga expressamente o art.19 do Marco Civil da Internet, de modo que não está claro como essas novas exigências, especialmente relacionadas ao dever de cuidado e do conhecimento prévio das plataformas, serão compatibilizadas com as normas já em vigor. Há, portanto, cenário de

vulnerabilização de direitos e de problemas práticos e jurídicos de conformação das sugestões ao ordenamento brasileiro.

3 ANÁLISE E ATENUAÇÃO DE RISCOS (ARTS. 30 E 31)

Da análise efetuada, consideramos positivo o art. 30 da proposta em comento, que diz respeito às necessidades de plataformas digitais identificarem, analisarem e avaliarem riscos sistêmicos decorrentes da concepção e funcionamento de seus serviços e sistemas relacionados. Também vemos como proveitosa a exigência de auditoria externa e independente para os critérios expostos no art. 31.

De forma geral, o capítulo X, sobre análise e atenuação de risco, aponta para uma problemática acerca do design das plataformas - sem necessariamente restringir práticas de inovação e construção de produtos. Os artigos dispostos no texto direcionam o olhar para formas através das quais os serviços podem afetar os usuários em diversos campos - seja, por exemplo, por meio de deceptive patterns ou através de recomendações algorítmicas**.**

Pode-se citar de forma ilustrativa sobre como a ausência de análise e atenuação de riscos pode impactar a vida dos usuários através do caso *Lemmon v Snapchat* nos Estados Unidos, originado pelo falecimento de dois garotos que dirigiam em alta velocidade utilizando o filtro do aplicativo capaz de registrar velocidade. No caso, argumentou-se que o Snapchat, por meio do filtro, incentivava direção perigosa em alta velocidade e, por isso, a Nona Corte afastou a imunidade da plataforma concedida pela Seção 230 do *Communications Decency Act*, visto que não se tratava de um conteúdo de terceiro, mas sim questão de design de própria plataforma social.

A criação e distribuição de um conjunto de obrigações novas aos atores, recortados o seu tamanho de mercado, é uma medida já incorporada por outros países. O resultado costuma envolver a diminuição da disparidade informacional sobre o funcionamento destas empresas e a criação de um estado de dever - em âmbito individual e coletivo - orientado ao aumento da simetria destes agentes, no contexto político de cada país. Estas medidas, associadas a um processo de transparência e *compliance*, permitem avançar no escrutínio público e na adequação destes negócios à sua função social, conforme comando expresso da Constituição Federal.

4 REMUNERAÇÃO DE CONTEÚDO PROTEGIDO POR DIREITO AUTORAL

O art. 54 da versão proposta pelo Governo Federal informa que os conteúdos protegidos por direitos autorais ensejarão remuneração aos titulares, por meio das plataformas e provedores. Essa remuneração deverá ser realizada de acordo com regulamentação posterior, do órgão competente, o qual não é indicado no texto - e nem poderia sê-lo, sob pena de vício de iniciativa.

Os conteúdos abarcados pelo art. 54 do texto sugerido para o PL incluem conteúdo musical, audiovisual e jornalístico. Não fica claro de que forma os titulares dos conteúdos protegidos por direito autoral serão remunerados.

Os titulares dos conteúdos protegidos exercerão seus direitos por meio de associações de gestão coletiva de direitos autorais, que irão negociar com os provedores os valores a serem praticados, o modelo e prazo da remuneração, nos termos da regulamentação, observado o disposto no §15 do art. 98, da Lei 9.610, de 19 de fevereiro de 1998. Hoje, a gestão coletiva de direitos autorais,disciplinada pelas leis nº 12.853/2013 e nº 9.610/1998, é realizada pelo Ecad (Escritório Central de Arrecadação e Distribuição), sendo administrada por sete associações de música. Nesse contexto, questiona-se: como se dará a distribuição e o gerenciamento de remuneração por conteúdo jornalístico e audiovisual? Seguirão o mesmo modelo de gestão coletiva da música?

O artigo 54 ainda menciona que o processo de definição da remuneração irá considerar conteúdos produzidos por cidadãos brasileiros ou consumidos no Brasil.

Já o art. 20 do texto analisado trata dos relatórios de transparência produzidos pelas plataformas. Neste artigo, há a previsão legal de que as plataformas deverão disponibilizar a descrição dos sistemas algoritmos utilizados para a recomendação e exibição dos conteúdos aos usuários. Esta disposição se aproxima de certa forma com o que encontramos em nosso relatório recém publicado na análise sobre a proposta da *Bill C-11*, do Canadá.

A referida proposta canadense é um projeto de legislação que abarca regras sobre a moderação de conteúdo pelas plataformas, mas principalmente versa sobre a disponibilização e priorização de conteúdos feitos no Canadá (por produtores canadenses) nas plataformas. A Bill C-11 é um projeto de lei que surgiu após a Bill C-10, que defendia que as plataformas de streaming de conteúdo, como o YouTube, concedessem parte de sua publicidade para conteúdos produzidos no Canadá, de forma a incentivar a produção e o consumo de conteúdo local. A Bill C-11 surgiu em 2022 como uma emenda ao Broadcasting Act canadense, que, dentre outras regulamentações, dá poder ao CRTC (*Canadian Radio-Television and Telecommunications Comission*), uma autoridade para regular o sistema de compartilhamento de conteúdo no país.

A seção "*Regulations – Canadian Programs*" do Projeto de Lei C-11 dispõe sobre a quantidade de conteúdos nas plataformas que deverão ser produzidos no Canadá, ou seja, conteúdos canadenses, de forma a incentivar o consumo de conteúdos produzidos no país. Ainda, a seção dispõe que pessoas que produzem conteúdos canadenses nas plataformas deverão disponibilizar parte de seus lucros para o sistema de transmissão canadense, o já citado CRTC. O propósito desta disposição foi amplamente discutido como uma tentativa do governo de fomentar o setor cultural canadense (o CRTC é uma entidade pública criada pelo Broadcasting Act, em 1876). Com a Bill C-11, o CRTC passaria a regular também conteúdos na Internet[4].

[4] Importa notar que muitos produtores de conteúdo canadenses, como streamers independentes e influencers, são contra o projeto de Lei, pois ele impactaria o lucro que esses streamers, youtubers e influencers ganham sobre o seu conteúdo consumido por usuários. As plataformas grandes de streaming, como a Netflix, Amazon e Spotify, serão sujeitas ao CRTC caso a Lei seja aprovada – o que também não seria bom para as plataformas de streaming, já que elas precisariam se adequar a

A medida se coaduna, portanto, com outros princípios relativos ao fomento do setor no Brasil, entretanto dois pontos merecem ser ressaltados: (a) o fato de que a matéria não é preferencial no tratamento da presente lei, desviando o seu objeto final e criando uma espécie de "jabuti" temático; (b) o Brasil não iniciou um processo, que merece amadurecimento devido, de revisão da sua legislação de direitos autorais, há, no ponto, um descompasso e uma postura reativa do legislador, que não deve ser chancelada pelos demais setores, no processo de regulação de tecnologias e das legislações que apresentam atravessamento por tecnologias.

5 IMUNIDADE PARLAMENTAR

A proposta ora comentada, no art. 18, estende a imunidade parlamentar constitucional para as redes sociais, criando um perigoso mecanismo através do qual as contas indicadas como institucionais pelas entidades da Administração Pública e as contas de cidadãos eleitos para cargos no Executivo e no Legislativo nas esferas federal e estadual tenham uma proteção diferente das contas de usuários ditos comuns.

Segundo o texto, as plataformas podem moderar conteúdos destas contas, mas não podem suspender ou bloquear estes perfis, mesmo em caso de as contas serem "contumazes violadoras dos termos e políticas de uso ou disseminadores de discursos de ódio, conteúdos ilícitos ou com potencial de provocar dano iminente ou de difícil reparação". Para estes casos, a maior sanção que pode ser aplicada pela plataforma é uma suspensão por 7 (sete) dias.

Trata-se, portanto, de uma autorização para que pessoas que foram eleitas disseminem qualquer tipo de desinformação ou discurso de ódio, já que o dispositivo não impõe consequências mais duras, que desincentivem a prática de tais atos. Surpreende que agentes públicos, cuja atuação é protegida para ensejar processos democráticos, tenham uma sinalização de impunidade, quando a tendência deveria ser a criação de ônus (ou seja, de obrigações impostas pela própria autoridade ao se candidatar no pleito eleitoral).

Nos últimos anos, pudemos perceber inclusive que grande parte da desinformação presente nas redes sociais tinha como grandes disseminadores justamente ocupantes de cargos públicos, como deputados federais e estaduais, senadores, ministros de Estado e o próprio ex-presidente da República, cujas contas tinham um grande alcance e uma enorme quantidade de seguidores. Em 2020, por exemplo, o Twitter retirou do ar algumas publicações do ex-presidente da República e de seus ministros por violarem seus termos de uso, divulgando informações sem comprovação científica sobre a Covid-19, colocando em risco a vida de milhares de brasileiros que seguiam e acompanhavam os perfis dessas pessoas.

---

lei e gastar recursos investindo nos criadores de conteúdo canadense e em uma mudança nos algoritmos de exibição de conteúdo somente para o país do Canadá. Outro ponto criticado na Lei é o impacto na liberdade de expressão e acesso a informação, já que uma das previsões da Lei é que conteúdos produzidos por canadenses tenham destaque no sistema de algoritmos da plataforma, de forma que sejam exibidos em destaque, com prioridade, em detrimento dos conteúdos produzidos fora do país.

Aprovar o presente artigo, mais do que deixar impune quem se utiliza de um cargo público e de toda a sua estrutura para realizar campanhas de desinformação, causando inúmeros danos à coletividade, é sinalizar, de forma equivocada e contraditória, acerca do papel social destes agentes e dos objetivos da própria lei proposta

O tema da imunidade parlamentar é antigo no direito brasileiro, aparece já na Constituição do Império. É regra, sob suas variadas formas e desdobramentos, de garantia do regime democrático. Entretanto, sua incidência tem limite definido. Pontes de Miranda, por exemplo, destaca que "*é punível o que o deputado ou senador disse ou escreveu fora da câmara e da função, e. g., em banquetes pra que não foi por ela designado, em meetings, jornais, ou livros*"[5] - o mesmo se diga da eventual responsabilidade civil de parlamentar que se manifesta por tecnologia de comunicação e informação *fora das funções*.

O tema, portanto, além de contar com amplo histórico de produção doutrinária, que se coaduna ao comando do atual art. 53, da Constituição Federal, também tem sua semântica e incidência delimitadas desde o início da experiência constitucional brasileira. Não se pode, portanto, por falha de inação dos aplicadores da lei, criar um quadro contraditório de irresponsabilidade de agentes públicos.

6 MENSAGERIA INSTANTÂNEA - arts. 32 E 33

Outro motivo de preocupação está nos artigos 32 e 33, que se referem aos serviços de mensageria instantânea. Em nosso ponto de vista, a redação do artigo 32 é extremamente confusa, podendo abrir novamente margem para criação de uma obrigação de rastreabilidade, que já esteve presente no texto do PL 2630/2020 aprovado pelo Senado.

Trata-se de uma estratégia considerada extremamente problemática por comunidade técnica e acadêmica, assim como pela sociedade civil engajada na proteção do direito à privacidade e pelo setor privado. O artigo em comento determina que os "serviços de mensageria instantânea preservem e disponibilizem informações suficientes para identificar a primeira conta denunciada por outros usuários quando em causa do envio de conteúdos ilícitos" a partir de ordem judicial.

A interpretação que parece fazer mais sentido aqui é que o conteúdo denunciado deve ser rastreável até a conta de origem - isto é, rastreabilidade. Hoje, sabe-se, que para o caso de serviços de mensageria como WhatsApp, principal fornecedor no Brasil de tal aplicação, ao usuário denunciar alguma conta e/ou conteúdo, os moderadores de conteúdo têm acesso às 5 mensagens mais recentes, além de metadados e informações sobre o usuário.

Isso, entretanto, não possibilita com que, através do usuário denunciado, o serviço seja capaz de chegar ao originador da mensagem. Além do mais, não podemos considerar que essa seja uma prática de outros serviços de mensageria com criptografia ponta-a-ponta. Respectivamente, para a adequação dos serviços às demandas legais, tal

[5] PONTES DE MIRANDA, Francisco Cavalcanti. Comentários à Constituição de 1967. Editora Revista dos Tribunais, 1970.

fato se daria pelo enfraquecimento da segurança e da privacidade desses serviços que empregam criptografia ponta-a-ponta, o que não se mostra benéfico, tanto para usuários quanto para as próprias empresas. Além do mais, vale notar que pequenos ajustes nos produtos, modificações ou outras estratégias simples adotadas pelos próprios usuários podem ser capazes de driblar a rastreabilidade de compartilhamento.

O conteúdo só pode ser considerado ilícito após algum nível de análise. Logo, para que seja possível obter essas informações para identificação da conta original, pode-se entender que seria necessário a existência de rastreabilidade em massa para recuperar a conta original, num movimento a posteriori, que iria requerer uma rastreabilidade em massa. Tal proposta já havia sido descartada pelo Grupo de Trabalho do Projeto de Lei 2630, em prol de uma alternativa mais alinhada às evidências sobre moderação de conteúdo em ambientes criptografados, isto é, unir a denúncia pelos usuários à análise de metadados. Essa alternativa consta no art. 13, do PL 2630, de relatoria do Deputado Orlando Silva.

Neste artigo, sob autorização judicial, os serviços de mensageria instantânea deveriam disponibilizar registros de interações de usuários, “vedados pedidos genéricos ou fora do âmbito e dos limites técnicos do seu serviço”. No primeiro parágrafo, há a definição da natureza da informação: “dados de envio e recebimento de mensagens e chamadas de áudio por sua conta e devem incluir data e hora de sua ocorrência, sendo vedada a associação desses registros ao conteúdo das comunicações”. Este artigo, de um lado, protege a criptografia, considerando a impossibilidade dos serviços acessarem o conteúdo dado o ‘limite técnico’ imposta pela criptografia ponta a ponta. Por outro lado, tem a vantagem de coibir a violação do sigilo do conteúdo das comunicações privadas. É visto, portanto, como ponto positivo.

Assim, manifestamos a importância de retomar esta proposta do relatório do GT em detrimento da substitutivo originado no Governo Federal, dado que a primeira está mais alinhada com as evidências empíricas e com a preservação do sigilo das comunicações, da criptografia forte e do direito à privacidade, reconhecido desde 2022 como direito fundamental em nossa Constituição.

Outro ponto crítico é o artigo 33, no qual certos dispositivos parecem ter sido pensados para serviços específicos, agindo assim para formatar a arquitetura dos serviços.

Em nossa concepção, **a lei não deve ser redigida considerando nomenclatura de um ou outro serviço privado, mas sim ter abstração para organizar e orientar as arquiteturas em geral, sob pena de, eventualmente, tornar-se obsoleta**. O fundamento regulatório segue a mesma regra, especialmente quando da tentativa de restrição de direitos individuais e coletivos.

Em certo momento, ao tratar de listas de transmissão, o inciso I do art. 33 parece pressupor o serviço de mensageria do Whatsapp e do Telegram - utilizando os próprios termos de tais serviços. Por outro lado, o parágrafo primeiro deste mesmo artigo parece ter sido desenhado com objetivo de incidir sobre os canais públicos do serviço de mensageria instantânea Telegram, muito usados por políticos.

Entendemos que a regulação é importante, mas deve ter a capacidade de ir além de um ou outro serviço específico existente atualmente, assim como deve ter elementos que permitam sua aplicação para inovações tecnológicas, como é frequente nos serviços de

mensageria instantânea. O papel de separação de atuações individuais, dentro da burocracia estatal, cabe às agências regulatórias, em processo administrativo individual. A proposta acaba por desmoronar importantes estruturas jurídicas de funcionamento básico do Estado Contemporâneo.

Um texto de regulação de serviços de mensageria instantânea deve, primeiramente, definir conceitos de maneira sólida e com certo grau de generalidade, evitando assim sua obsolescência, tendo em vista o intenso ritmo de transformações dos serviços digitais, assim como mecanismos de evasão legal, como por exemplo, alteração no nome da funcionalidade.

No mesmo artigo, parágrafo terceiro, ao exigir que contas comerciais em serviços de mensageria sejam capazes de identificar o remetente e viabilize acesso a identificação por meio de documento de registro nacional, identificamos uma falta de precisão no que significaria tal exigência. Não fica claro se a necessidade de identificar o remetente da mensagem, assim como acesso a algum documento de registro nacional, seria para o serviço de mensageria ou para o usuário que se comunica com a empresa.

Em caso da primeira hipótese, isso representaria uma necessidade de alteração na infraestrutura de serviços de mensageria, podendo minar a privacidade e segurança dos usuários.

7 RETENÇÃO DE DADOS PARA FINS INVESTIGATIVOS - arts. 36 e 57

Outro tema que suscita grande preocupação é o capítulo que determina a coleta de dados para investigações criminais. O art. 36 do texto em comento expressa que as empresas devem guardar, pelo prazo de um ano a partir da remoção ou desativação, dados ou informações “que possam constituir” material probatório. Mas esta determinação, da forma como está redigida, é extremamente ampla, considerando que qualquer coisa tem o potencial de constituir prova em investigações.

O referido artigo modifica, sem colocar isso expressamente, o regime de guarda e disponibilização de dados para investigações disposto nos arts. 13 e 15 do Marco Civil da Internet. Segundo o art. 13 do MCI, aplicável aos provedores de conexão, a guarda dos dados será requerida cautelarmente pela autoridade policial ou administrativa ou pelo Ministério Público, se por prazo maior que 6 (seis) meses. Feito isso, a autoridade requerente tem prazo de 60 (sessenta dias) para ingressar com pedido de autorização judicial para acesso aos dados resguardados pelo provedor. O art. 15 do mesmo diploma apresenta mecanismo semelhante, só que referindo-se aos registros de provedores de aplicação.

Os dados referidos pelos arts. 13 e 15 são expressos nos parágrafos do art. 10 do MCI, sendo eles: dados cadastrais (qualificação pessoal, filiação e endereço) e registros de conexão e acesso a aplicações de Internet. O que o art. 36 do texto proposto faz é ampliar essa guarda para todo e qualquer tipo de dado que o usuário tenha compartilhado com a plataforma, ampliando, por consequência, os poderes das plataformas no que se refere às suas capacidades vigilantistas. Vale mencionar ainda que os incisos I e II constituem um rol exemplificativo no dispositivo, podendo o dever de guarda ser expandido para toda e

qualquer informação presente na plataforma, mesmo que não relacionada à investigação em andamento.

Esta discussão se conecta também com a proposta de alteração dos arts. 13 e 15 do MCI, presente no art. 57 da proposta do governo federal. As alterações vislumbradas pelo governo ampliam os poderes de requisição cautelar de informações de identificação dos usuários, já explicitadas acima, para quaisquer informações sobre os usuários, extrapolando inclusive a incidência da lei, já que o texto em comento é direcionado apenas a provedores de aplicação, mas tais alterações seriam aplicáveis também a provedores de conexão.

Todas essas alterações, em última instância, infringem a LGPD, já que esta inclui como princípios para o tratamento de dados a finalidade, necessidade, a segurança e a prevenção (art. 6º, I, III, VII, VIII e art. 46). Além disso, ao ampliar a base de dados a serem coletados pelas plataformas, incorre-se num risco aumentado de incidentes de segurança e danos aos usuários.

Adicionalmente, chamamos a atenção para a ausência de uma LGPD Penal, já que a LGPD prevê sua não aplicação no âmbito de investigações criminais. Nesse cenário de vácuo regulatório sobre dados pessoais no âmbito penal, práticas danosas, entre abusos, falhas de segurança e condutas desproporcionais já vêm se disseminando, como apontamos, por exemplo, em nosso estudo "Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil".

Por isso, pedimos atenção e esforços para retomar as discussões a partir do Anteprojeto de Lei (APL) de Proteção de Dados para segurança pública e investigação criminal elaborado pela Comissão de Juristas instituída pelo então Presidente da Câmara dos Deputados, Rodrigo Maia, em 2019. O APL, em oposição ao problemático Projeto de Lei 1515/2022, respeita as garantias constitucionais e é um bom ponto de partida para as urgentes e necessárias discussões sobre o tema.

Em razão disso, recomendamos a supressão integral do art. 36 e a manutenção do regime estabelecido no Marco Civil da Internet para guarda e acesso a dados pelas autoridades de investigação. Alternativamente, que sejam definidas no texto as informações que deverão ser guardadas pelas plataformas, com critérios para concessão do acesso e uso pelas autoridades no bojo das investigações criminais, mediante ordem judicial, e com definição de garantias de direitos fundamentais das pessoas investigadas.

8 AUTORIDADE ADMINISTRATIVA (Cap. XIV, XV)

Muito se discute, entre membros da sociedade civil organizada, acerca da natureza jurídica da "entidade autônoma de supervisão", se instituição integrante da administração pública ou sem qualquer vínculo com o Estado.

Acreditamos que a "entidade autônoma de supervisão" deve ser uma autoridade da administração pública indireta federal, de natureza autárquica especial, dotada de personalidade jurídica de direito público, justificada por exercer função regulatória, exercer poder de polícia, fiscalizar atividades e aplicar sanções às plataformas digitais, ou seja, por executar competências que são próprias do Estado.

De acordo com o art. 49 do projeto em análise, o Poder Executivo poderá estabelecer entidade autônoma de supervisão para detalhar em regulamentação os dispositivos de que trata a Lei, fiscalizar sua observância pelas plataformas digitais de conteúdo de terceiros, instaurar processos administrativos e, comprovado o descumprimento das obrigações pela plataforma, aplicar as sanções cabíveis, devendo contar com as garantias de autonomia administrativa e independência no processo de tomada de decisões e deve contar com espaços formais de participação multissetorial.

A independência esperada de um órgão de regulação passa também pela autonomia orçamentária, financeira e patrimonial, além da autonomia técnica e de gestão, de forma a garantir o pleno exercício das atividades de regulação, controle, fiscalização e aplicação de sanções. Não identificamos no projeto qualquer menção sobre a natureza dessas autonomias, limitando-se a administrativa e decisória.

Não há, também, qualquer indicação ao Órgão Público ao qual estará vinculada (sem subordinação hierárquica) a “entidade autônoma de supervisão”.

Por fim, não se pode olvidar que, para, sua instituição, é prudente considerar os percalços que acompanharam a recente criação da Autoridade Nacional de Proteção de Dados - ANPD, como, por exemplo, o vício de iniciativa do projeto de lei original, para que não se repitam os equívocos cometidos. Ainda, é necessário levar em conta a proliferação de agentes reguladores e fiscalizadores no contexto das tecnologias. O tema merece detida e exigente reflexão sob o ponto de vista da estruturação da burocracia estatal, de modo a coordenar as diferentes competências setoriais.

9 CONCLUSÃO

Do estudo da sugestão enviada pelo Governo Federal para o Congresso Nacional como substitutivo ao PL 2630/2020, é possível observar que há um descompasso entre normas já existentes de regulação de tecnologia no país, considerando a pouca coesão com tais diplomas, em especial de termos e conceitos já firmados no ordenamento jurídico brasileiro, como o Marco Civil da Internet. Além disso, diversos dispositivos do texto não estão em consonância com o próprio MCI, com a Lei Geral de Proteção de Dados e com a própria Constituição Federal.

Nesse sentido, entendemos que todo o texto merece aprimoramentos a fim de estabelecer uma regulação de provedores de aplicação que respeite as evidências científicas, garanta direitos dos usuários e traga segurança jurídica às empresas que prestam os serviços afetados pela regulação, reduzindo, ainda, a influência das plataformas no debate público e sua assimetria informacional em relação aos usuários.

Instituto de
Pesquisa em
Direito & Tecnologia
do Recife

www.ip.rec.br