NOTA TÉCNICA SOBRE O PROJETO DE LEI 2630/2020

25 de junho de 2020

Introdução

A presente nota técnica analisa o relatório substitutivo do Projeto de Lei 2.630/2020, do Senador Alessandro Vieira, que institui a *Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. O projeto tramita no Senado Federal há pouco mais de um mês, tendo recebido ao menos 87 emendas. O PL encontra-se incluído em Ordem do Dia de sessão deliberativa remota de 25 de junho de 2020.[1]

O projeto de lei 2.630/2020 é composto por 31 artigos, divididos em seis capítulos. O projeto estipula diretrizes e mecanismos de transparência para "aplicações de redes sociais e de serviços de mensageria privada na internet, para desestimular abusos ou manipulação com potencial para causar danos". A proposta normativa não se aplica para provedores com menos de dois milhões de usuários e deve, em tese, levar em consideração o Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

Nesta análise técnica, nos debruçamos especificamente sobre as relações do substitutivo do Senador Angelo Coronel, apresentado em 24 de junho de 2020, com os direitos digitais e mais especificamente sobre a proteção de dados pessoais, com enfoque em "uma série de antinomias e sobreposições a serem resolvidas com a legislação específica da área, especialmente a Lei Geral de Proteção de Dados e o Marco Civil da Internet", como identificado pelo Requerimento n. 1030/2020.[2]

A nota técnica identifica propostas normativas no projeto de lei que **colidem com o direito fundamental à proteção de dados**, tal como reconhecido pelo Supremo Tribunal Federal e pelo direito brasileiro.[3] Recomenda-se sua análise detalhada pelo prisma da Constituição, em caráter formal, antes de sua deliberação em plenário.

As ideias presentes no substitutivo apresentam clara violação de direitos fundamentais e são incompatíveis com a arquitetura jurídica de uso da internet e proteção de dados pessoais no Brasil.

---

[1] Ver https://www25.senado.leg.br/web/atividade/materias/-/materia/141944

[2] Ver o Requerimento em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8124559&ts=1593045840023&disposition=inline

[3] ADI 6387 em que o Data Privacy Brasl foi aceito como *amicus curiae* e cuja petição de intervenção pode ser acessada em: <https://www.dataprivacybr.org/wp-content/uploads/2020/05/dpbrr_amicuscuria_stf_ibge.pdf>. Dentre os votos já publicizados, destaca-se do eminente Ministro Gilmar Mendes: <https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf>

1. Análise técnica do conteúdo do projeto de lei

Neste tópico, analisamos quatro colisões do projeto de lei com os direitos relacionados à privacidade e proteção de dados pessoais, partindo dos parâmetros assegurados em leis federais e em recentes interpretações dadas pelo Supremo Tribunal Federal.

As falhas do projeto de lei da perspectiva da proteção de dados pessoais consistem, em síntese, em:

- Inadequação do Art. 3º, II, em razão de uma visão de privacidade individual que ignora o caráter autônomo da proteção de dados pessoais e sua relação com liberdades públicas;
- Violação do princípio da necessidade da Lei Geral de Proteção de Dados Pessoais no Art. 6º, que trata do cadastro de usuários de redes sociais e serviços de mensageria privada, ampliando o tratamento de dados pessoais de forma abusiva;
- Uso abusivo de dados pessoais, no Art. 8º, para desconexão de usuários de aplicações de internet quando houver suspensão dos serviços de telecomunicações, ignorando o princípio da prevenção previsto na Lei Geral de Proteção de Dados Pessoais, com a possibilidade de inúmeros danos aos milhões de consumidores dessas aplicações de internet;
- Inconstitucionalidade do art. 10º do substitutivo do projeto de lei, no sentido de que transformação de todos os cidadãos em suspeitos e a obrigação de uma vigilância permanente, com capacidade de identificação precisa de disparo de mensagens, com data e horário, é contrária à ideia de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" previsto na Lei Geral de Proteção de Dados Pessoais.

Há inúmeras outras violações de direitos fundamentais no substitutivo do projeto de lei a ser apreciado pelo Senado Federal. Por questão de escopo, analisamos em profundidade os quatro pontos listados acima.

1.1. A falha do Art. 3º no reconhecimento do direito autônomo à proteção de dados pessoais

O projeto de lei prevê, em seu artigo terceiro, que a norma será pautada pela "garantia dos direitos de personalidade, da dignidade, da honra e da privacidade do indivíduo" (Art. 3º, II). Nesse sentido, o projeto falha ao adotar uma concepção de privacidade do século XX, conectada a uma ideia exclusivamente individual. O projeto ignora o reconhecimento, no Supremo Tribunal Federal, de um direito autônomo à proteção de dados pessoais que se diferencia do direito à privacidade.

Conforme explicado em nosso *amicus curiae* na Ação Direta de Inconstitucionalidade nº 6.387, o direito à proteção de dados pessoais está ligado à proteção dos direitos da personalidade e o exercício de liberdades públicas específicas. Ele não se relaciona essencialmente com o sigilo de comunicações, mas sim, com a garantia de que a utilização de dados pessoais observará requisitos legais para coleta e tratamento, que garantam o absoluto respeito ao exercício presente e futuro de direitos e garantias constitucionais. Não se trata, portanto, de uma liberdade negativa do cidadão em restringir o acesso à informações sigilosas ou das suas comunicações, mas, pelo contrário, de

uma liberdade positiva, condicionada pelo estabelecimento de garantias, para que eventual ingerência sobre as suas informações pessoais seja legítima.

A proteção de dados é uma condição prévia para a participação imparcial dos cidadãos nos processos políticos do estado constitucional democrático. Deve-se reconhecer a proteção de dados pessoais como pilar da legislação e não somente a privacidade do indivíduo.

1.2. As potenciais violações de direitos decorrentes do cadastro obrigatório

O projeto define "rede social" como "aplicação de internet que oferece funcionalidades de publicação de conteúdo por usuários e interação entre eles, sem que haja controle editorial prévio, em um mesmo sistema de informação cuja relação é promovida por meio de contas conectáveis". Enquadram-se como RS aplicações como Facebook, Instagram, Twitter e Youtube (empresa do grupo Alphabet, controladora do Google). Todavia, esse conceito pode ser interpretado de forma bem mais ampla até mesmo para abordar outros tipos de serviços, como fóruns de discussão e até mesmo páginas com comentários em aberto.

O projeto define "serviços de mensageria privada" (SMP) como "provedores de aplicação que prestam serviços de mensagens instantâneas por meio de comunicação interpessoal, acessíveis a partir de terminais móveis com alta capacidade de processamento ou de outros equipamentos digitais conectados à rede, destinados, principalmente, à comunicação privada entre seus usuários, inclusive os criptografados, ressalvados os serviços de correio eletrônico". Enquadram-se como SMP aplicações como Whatsapp, Telegram e Signal. Todavia, esse conceito, em si, também pode ser interpretado de forma bem mais abrangente, até mesmo para incluir sistemas de mensageria simples, como os enviados entre estabelecimentos comerciais para falar com seus clientes se valendo de sistemas de *push notification*.

O art. 6º da legislação prevê que redes sociais e SMPs devem "identificar todos os conteúdos impulsionados e publicitários cujo pagamento pela distribuição foi realizado ao provedor de redes sociais" e "comunicar, ao Ministério Público Eleitoral, nos períodos de propaganda eleitoral, a propaganda potencialmente irregular de que tiver conhecimento, nos termos da Lei nº 9.504, de 30 de setembro de 1997".

No parágrafo primeiro do artigo sétimo, o projeto dispõe que é obrigatório para redes sociais e SMPS o cadastro de seus usuários. O projeto diz que "o cadastro de contas em redes sociais e nos serviços de mensageria privada **deverá exigir do usuário documento de identidade válido, número de celular registrado no Brasil e, em caso de número de celular estrangeiro, o passaporte**".

O projeto estipula que "para validar a informação requerida no caput, os provedores de redes sociais e de serviços de mensageria privada deverão enviar por SMS código de verificação ao número de celular informado".

A ideia do cadastro obrigatório faz com que as empresas de tecnologia **sejam obrigadas a coletar e tratar mais dados pessoais do que é realmente necessário para sua operações, rompendo o**

princípio da *necessidade*, ou seja, "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

O tratamento de dados de identidade (R.G.) pode implicar, também, em tratamento de dados sensíveis de acordo com a Lei Geral de Proteção de Dados Pessoais, na medida em que há tratamento da fotografia do documento, que pode implicar em tratamento biométrico.

Além do tratamento de dados de forma desproporcional, realizado em razão de uma obrigação, a proposta colide com o princípio da segurança, na medida em que obriga as empresas a "enviar por SMS o código de verificação ao número de celular informado", o que abre a possibilidade de ataques cibernéticos focados em explorar vulnerabilidades do sistema de envio de mensagens por SMS.[4]

Esta proposta vai na contramão do que prevê a LGPD em seu art. 6, VIII, por meio do princípio da prevenção, que significa a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais". Além disso, ignora outros debates já travados na esteira da aprovação do Marco Civil da Internet quando se rechaçou justamente propostas pelas quais se procurou alargar o dever de retenção de dados, na medida em que seria lesivo não só para o direito à privacidade, mas, também, para a própria liberdade de expressão.[5]

1.3. Uso abusivo de dados para desconexão de usuários

O projeto prevê, em seu artigo oitavo, que "os provedores de redes sociais e de serviços de mensageria privada ficam obrigados a suspender as contas de usuários cujos números forem desabilitados pelas operadoras de telefonia".

Trata-se de proposta que implica em um tratamento abusivo de dados pessoais, na medida em que obrigada o tratamento de dados pessoais de forma compartilhada entre prestadoras de serviços de telecomunicações (serviços móveis pessoais) e as redes sociais e SMPs.

A implementação desta norma também gera abre a possibilidade de um monitoramento constante, por parte dessas empresas de tecnologia, em violação às expectativas de privacidade dos consumidores de serviços móveis pessoais (telefonia celular), considerando que o contrato com as operadoras de serviços de telecomunicações implica em um dever de cautela no uso das informações por parte delas. No limite, a norma parece colidir também com a Lei Geral de Telecomunicações e com as normas regulatórias deste setor.

---

[4] Altieres Rohr, 'Entenda como hackers atuam para interceptar mensagens SMS', *O Globo*, 12/06/2019. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/06/12/entenda-como-hackers-atuam-para-intercepter-mensagens-sms.ghtml

[5] Para uma análise mais aprofundada em torno das opções legislativas sobre Internet e o processo de convergência em torno do Marco Civil Internet (Lei 12.965.2014), veja-se por todos a pesquisa de Francisco Brito Cruz. *Direito, democracia e cultura digital*: a experiência de elaboração legislativa do marco civil da internet. Dissertação (Mestrado) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2015.

No caso de cancelamentos de contas de telefone celular por falta de pagamento (indébito), o que não é incomum em um cenário de crise econômica crônica e Covid-19, a proposta normativa geraria uma munição para desconexões dessas pessoas em redes sociais e aplicações de internet gratuitas, como Whatsapp e Twitter, fazendo com que o consumidor tivesse uma relação de consumo interrompida de forma abusiva, em notória violação dos direitos básicos assegurados no Código de Defesa do Consumidor.

1.4. Os riscos permanentes às liberdades públicas pela rastreabilidade de mensagens

O art. 10º do projeto de lei prevê que "os serviços de mensageria privada devem guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa, pelo prazo de 3 (três) meses, resguardada a privacidade do conteúdo das mensagens". Define, para tanto, que "considera-se encaminhamento em massa o envio de uma mesma mensagem **por mais de cinco usuários**, em intervalo de até 15 dias, para grupos de conversas, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários".

Na prática, isso cria uma obrigação de rastreabilidade por parte das aplicações como Twitter, WhatsApp, Telegram, e outros. A proposta é altamente problemática, considerando que, para que exista um efetivo monitoramento de todas as mensagens idênticas enviadas por mais de cinco usuários, será necessário identificar individualmente os usuários.

Isso fica explícito no texto, considerando que o parágrafo segundo estipula que "os registros de que trata o caput devem conter a **indicação dos usuários** que realizaram encaminhamentos em massa da mensagem, **com data e horário deste encaminhamento**, e o quantitativo total de usuários que receberam a mensagem".

Mesmo com a menção de que tais registros somente serão acessados mediante ordem judicial e para fins de investigação criminal e instrução processual penal, cria-se um aparato de vigilância abusivo, transformando todos os cidadãos em suspeitos.

Essa transformação de todos os cidadãos em suspeitos e a obrigação de uma vigilância permanente, com capacidade de identificação precisa de disparo de mensagens, com data e horário, é contrária à ideia de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", de que fala o artigo primeiro da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

Como notado por Namrata Maheshwari, pesquisador da Columbia Law School que analisou o projeto de lei brasileiro, "as plataformas seriam obrigadas rastrear todas as cadeias de comunicação e reter os metadados, independentemente da natureza da mensagem ou da intenção com a qual foram compartilhadas". Nas palavras de Maheshwari, "esse mandato de rastreabilidade é contrário às normas internacionais sobre o princípio da minimização de dados e, como resultado de sua implementação, mesmo que um usuário não tenha sido o criador de conteúdo considerado

problemático ou esteja compartilhando o conteúdo apenas para condená-lo, os dados ainda estariam associados à cadeia impugnada de comunicação e às conseqüentes investigações"[6].

A proposta de rastreabilidade implicaria na adição de elementos identificadores pessoais nos metadados das mensagens compartilhadas, o que violaria a lógica da criptografia ponta-a-ponta e a impossibilidade de acesso aos conteúdos das mensagens e identificação de "quem enviou o que". A proposta de lei, nesse sentido, ignora completamente a decisão parcial do Supremo Tribunal Federal sobre a legalidade da criptografia ponta-a-ponta, no famoso "caso Whatsapp", isto é, o julgamento conjunto da Ação Direta de Inconstitucionalidade (ADI) 5527 e da Arguição de Descumprimento de Preceito Fundamental (ADPF) 403.

O voto do ministro Fachin na ADI 5527/ADPF 403 expõe sete premissas básicas para o debate sobre direitos digitais em sede constitucional no Brasil:

> "*Primeira*: o impacto tecnológico das mudanças porque passa a sociedade reclamam um permanente atualizar do alcance dos direitos e garantias fundamentais. *Segunda*: os direitos que as pessoas têm offline devem também devem ser protegidos online. Direitos digitais são direitos fundamentais. *Terceira*: a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. *Quarta*: a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública. *Quinta*: A liberdade de expressão tem primazia prima facie e constitui condição essencial ao pluralismo de ideias, vetor estruturante do sistema democrático de direito. *Sexta*: Na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações. A criptografia, em especial, é um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública. Sétima: É contraditório que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas".

Como sustentado pelo Comitê Gestor da Internet nesta ação relatada pelos ministros Fachin e Weber, que contou com audiência pública participativa em 2017, a criptografia é instrumental aos direitos humanos de privacidade e liberdade de expressão. É uma tecnologia que deve ser estimulada e não restringida. As plataformas que disponibilizam tecnologias de segurança da informação não devem ser penalizadas pelos usos de seus usuários.

---

[6] Namrata Maheshwari, 'Traceability Under Brazil's Proposed Fake News Law Would Undermine Users' Privacy and Freedom of Expression', *Center for Democracy & Technology*, 23/06/2020. Disponível em: https://cdt.org/insights/traceability-under-brazils-proposed-fake-news-law-would-undermine-users-privacy-and-freedom-of-expression/

Direitos digitais são direitos fundamentais. Como lembrado pelo ministro Fachin, “essa é a orientação do Conselho de Direitos Humanos das Nações Unidas (A/HRC/RES/32/13) e é também a orientação que começou a ser esboçada por este Tribunal no julgamento da ADI 6.387, relatada pela e. Ministra Rosa Weber”.

O ministro Fachin corretamente pontua que “na internet, a proteção de privacidade não é apenas proteção individual, mas garantia instrumental do direito à liberdade de expressão. Isso porque o fluxo de informações é feito tanto pelos dados que são recebidos, quanto pelos dados enviados”.

Valendo-se dessa recente interpretação do significado dos direitos digitais à luz da teoria dos direitos fundamentais, fica evidente que a proposta de ampla rastreabilidade de mensagens do PL 2.630 viola esses direitos e torna nebuloso o cenário de proteção de direitos fundamentais no século XXI.

Conclusão

Em sua redação final, dada pelo substitutivo de 24 de junho de 2020, o projeto de lei 2.630 possui artigos incompatíveis com a proteção dos dados pessoais e com garantias constitucionais aplicadas às liberdades públicas e aos direitos digitais.

É crucial que o projeto seja analisado pela Comissão de Constituição e Justiça do Senado e que seu mérito seja analisado à luz da Proposta de Emenda Constitucional n. 17/2019, que garante o direito fundamental à proteção de dados pessoais, e, especialmente, à luz dos julgamentos da ADI 6.387 e da ADI 5527/ADPF 403 pelo Supremo Tribunal Federal, considerando que esses casos apresentam interpretações sobre o significado dos direitos digitais de acordo com os parâmetros da Constituição Federal. Em resumo:

a) sob o ponto de vista procedimental, a proposta legislativa deve seguir o rito ordinário com análise pelas Comissões Parlamentares em especial pela Comissão de Constituição e Justiça, sem prejuízo de audiências públicas, dada a complexidade da matéria e repercussão transversal sobre direitos e liberdades fundamentais. Em especial, porque colide com leis que contaram com ampla participação pública, como é o caso do Marco Civil da Internet (Lei 12.965/2014) e da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018);

b) sob o ponto de vista material, a proposta legislativa alarga o dever de retenção de dados sendo perniciosa para uma vigilância em massa, o que é contrário não só ao direito à privacidade e proteção de dados pessoais, mas, também, à liberdade de expressão. Ao final e ao cabo, coloca-se em rota de colisão com os recentes precedentes do Supremo Tribunal Federal sobre a proteção de dados pessoais como um direito fundamental autônomo e o paralelismo de que as liberdades públicas experimentadas no mundo *offlline* também devem valer no mundo *online*.

Sobre o Data Privacy Brasil

A Associação Data Privacy Brasil de Pesquisa ("Data Privacy Brasil") é uma entidade civil sem fins lucrativos sediada em São Paulo. A organização dedica-se à interface entre proteção de dados pessoais, tecnologia e direitos fundamentais, produzindo pesquisas e ações de incidência perante o sistema de Justiça, órgãos legislativos e governo. A partir de uma Política de Financiamento Ético e Transparência, a associação desenvolve projetos estratégicos de pesquisa em proteção de dados pessoais, mobilizando conhecimentos que podem ajudar reguladores, juízes e profissionais do direito a lidar com questões complexas que exigem conhecimento profundo sobre como tecnologias e sistemas sócio-técnicos afetam os direitos fundamentais. A Associação possui financiamento de filantropias internacionais como Ford Foundation, Open Society Foundations e AccessNow. Para mais informações, visite www.dataprivacybr.org

Diretores

Bruno R. Bioni e Rafael A. F. Zanatta

Líder de projetos

Mariana Rielli

Pesquisadoras

Gabriela Vergili, Iasmine Favaro, Jacqueline Pigatto & Marina Kitayama

Contatos da Associação Data Privacy Brasil de Pesquisa

contato@dataprivacybr.org

imprensa@dataprivacybr.org