INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

NOTA SOBRE PROJETO DE LEI N. 113/2020

Altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, para dispor sobre o cadastramento dos usuários de provedores de aplicações de internet.

A proposta legislativa sob análise, apresentada pelo Senador Ângelo Coronel em fevereiro de 2020, **foi alterada integralmente, em conteúdo e impacto, a partir do substitutivo** apresentado em 22 de novembro de 2023 pelo Relator Senador Astronauta Marcos Pontes. Inicialmente, a proposta legislativa tinha como objetivo assegurar o vínculo das contas de usuários em plataformas digitais a seus números de CPFs. Ainda que esta obrigação de cadastramento vinculado ao CPF também seja rechaçada, esta nota se atenta a alguns tópicos do texto substitutivo. Abaixo, **destacamos alguns pontos críticos do PL 113/20 que o colocam como uma ameaça aos direitos humanos** - em especial à privacidade, à liberdade de expressão e ao devido processo.

- Os temas abordados no PL estão sendo extensamente debatidos no âmbito do PL 2630. É inaceitável ignorar esse acúmulo.
- O PL prevê procedimentos de acesso a dados sem garantir a sua segurança; amplia o acesso aumentando o risco de abuso de poder e de estratégias vigilantistas.
- Determina uma ampliação do tempo de guarda de dados sem se ater às implicações técnicas que podem impactar o ecossistema, dificultando a inovação e operação de pequenas empresas reguladas pelo PL.

1. O PL ignora 3 anos de debate e apresenta propostas inadequadas

Tanto o Marco Civil da Internet como a Lei Geral de Proteção de Dados são duas grandes conquistas legislativas para o Brasil, reconhecidas internacionalmente, pois são resultados de um amplo debate multissetorial. Desde 2020 o congresso brasileiro, em conjunto com o setor privado, sociedade civil e comunidade técnica, tem debatido extensamente o tema da regulação de plataformas. Nos últimos três anos foram realizadas diversas audiências públicas, reuniões bilaterais, campanhas e ações conjuntas para que um tema de tamanha importância seja acompanhado de soluções eficazes.

Foram investidos grandes recursos humanos e financeiros, do governo anterior e atual, para construir uma regulação democrática e robusta de forma que os problemas reais de segurança, desinformação, discurso de ódio, crimes virtuais e tantos outros sejam diminuídos. Entretanto, o PL 113/20 ignora completamente anos de debate de diversos setores da sociedade e os acúmulos alcançados até aqui e **apresenta dispositivos descolados da construção pública da solução**. O resultado da negligência de um debate que vem sido mantido há anos é uma **proposta legislativa ineficaz, que restringe direitos e concede poderes excessivos** sem devidas amarras institucionais de freios e contrapesos.

Por isso, **recomendamos a conclusão da tramitação do PL 113/20, por arquivamento ou rejeição, e que os debates sobre os temas da propostas sejam acoplados aos extensos debates envolvendo o PL 2630/20**.

2. Ampliação de poderes de acesso à dados sem devidas garantias processuais.

Conforme disposto em pesquisa realizada pelo IRIS em 2017, " A previsão legal para guarda desses dados [de registro de conexão e acesso a aplicação] objetiva facilitar a identificação de usuários da internet pelas autoridades competentes e mediante ordem judicial"[1].

Dados de acesso à internet e aplicações são centrais para identificação de usuários, grupos, práticas e comportamentos. Tais dados são necessários para identificação de crimes cometidos pela internet. Entretanto, **caso esses dados sejam acessados por agentes maliciosos, esses mesmos dados podem ser usados para o cometimento de crimes e supressão de direitos**. Perseguição política, assédio e golpes financeiros são algumas das práticas ilícitas que podem ser cometidas a partir do acesso a tais dados. Por isso, a **proteção do fluxo de acesso** a tais dados é central à proteção da integridade física, psicológica e cidadã do usuário de internet. E, no contexto brasileiro, **temos vivido sucessivos vazamentos de dados[2] que demonstram a fragilidade de sistemas** e trazem preocupação para os cidadãos brasileiros.

Além disso, a **insegurança sobre a proteção do fluxo de tais dados é uma ameaça à liberdade de expressão**, pois usuários podem se sentir constrangidos a utilizarem determinadas aplicações na possibilidade de uma exposição indevida de tal acesso. Esse fenômeno é conhecido como chilling effect, "também chamado de "efeito inibidor", e

[1] LIMA, Iara Vianna et al. Portas lógicas e registros de acesso: das possibilidades técnicas aos entendimentos dos tribunais brasileiros. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2017. Disponível em: http://bit.ly/36bdDTC . Acesso em: 12/12/2023.
[2] ROGRIGUES, Gustavo. O Brasil teve o maior vazamento de dados de sua história. E agora?. Instituto de Referência em Internet e Sociedade. Disponível em <https://irisbh.com.br/o-brasil-teve-o-maior-vazamento-de-dados-de-sua-historia-e-agora/>

trata-se do desencorajamento do exercício legítimo de um direito por ameaça de alguma sanção"[3]. No caso, **a ameaça seria a de ter seus dados expostos ou acessados por agente desconhecido e não submetido às regras democráticas**.

Uma decisão judicial, ainda que passível de erros e revisões, deve observar diversos elementos processuais e materiais que a revestem de legitimidade. O PL expande poderes para requisição de dados de acesso e concede a delegados de polícia e representantes do ministério público o poder de requisição de tais dados. Apesar de mencionar a necessidade de observar o art. 7º do MCI nos pedidos de requisição de dados, **o dispositivo não estabelece nenhuma garantia processual para estabelecer limites à requisição de dados tão centrais**. Considerando que o art. 7º do MCI é meramente principiológico, a ampliação de poderes de acesso a dados de acesso significa uma ampliação da possibilidade de **abuso de autoridade** por parte dos atores envolvidos.

Aprofundando os riscos, a proposta de art. 10, § 3º concede a Delegado de Polícia, membro do Ministério Público ou autoridade administrativa competente o poder de acessar dados cadastrais que informem qualificação pessoal, filiação e endereço. Assim, **além de ampliar o tipo de dado que pode ser acessado, a proposta inclui um novo agente de forma abstrata e generalista**, afinal "autoridade administrativa competente" é um termo que pode se referir a uma vastidão de agentes reguladores, autarquias ou outros órgãos.

Por esses motivos, **recomendamos que qualquer proposta legislativa possibilite a solicitação de dados de acesso exclusivamente mediante ordem judicial** para que abusos de autoridades sejam evitados e o direito à privacidade e liberdade de expressão sejam garantidos.

3. Ampliação do tempo de armazenamento de dados sem avaliação de impacto em modelos de negócio.

O projeto amplia o tempo de armazenamento de dados **desconsiderando a infraestrutura necessária para o cumprimento de tal obrigação**. Assim, considerando a relevância e impacto do projeto, se faz necessário ampliar o debate e incluir o setor privado, especialmente os pequenos provedores de aplicação.

Considerando a diversidade de organizações que estão na categoria de provedor de aplicações, estabelecer uma obrigação homogênea que demanda investimentos massivos em segurança da informação, recursos de armazenamento de dados e capacitação técnica,

[3] OLIVAI, Thiago Dias; ANTONIALLII, Dennys Marcelo; DOS SANTOSII, Maike Wile. Censura Judicial ao Humor: análise de decisões judiciais envolvendo liberdade de expressão na internet. **Revista Direitos Culturais**, v. 14, n. 34, p. 19-44, 2019.

pode impactar negativamente a inovação. Regulações eficazes aplicadas ao ecossistema digital devem partir de uma **abordagem proporcional atenta à capacidade e o tamanho de cada agente regulado** ao aplicar regras e medidas regulatórias.

Sendo assim, **recomendamos a ampliação do debate acerca do tempo de armazenamento de dados** de acesso e conexão, incluindo os diversos atores que seriam impactados pela regulação.

Sobre o IRIS

Fundado em 2015, o IRIS é um centro de pesquisa independente dedicado a produzir e comunicar conhecimento científico sobre os temas de internet e sociedade, além de defender e fomentar políticas públicas que avancem os direitos humanos na área digital. Nossa atuação busca qualificar e democratizar os debates sobre internet, sociedade e novas tecnologias ao trazer insumos científicos aos usuários da internet e aos diferentes setores que compõem a sociedade.

No tema de regulação de plataformas digitais, temos extensa experiência, como:

- Atuação destacada no Grupo de Trabalho (GT) de Regulação de Plataformas da Coalizão Direitos na Rede (CDR) — entidade composta por mais de 50 organizações;
- Participação em audiência pública intitulada “Alterações no Marco Civil da Internet e Responsabilização das Plataformas”;
- Contribuições à Consulta Pública do CGI.br;
- Contribuições ao Oversight Board (OVB) da Meta (citado pelo OVB como apêndice de sua decisão);
- Desenvolvimento de projeto de pesquisa sobre a normativa europeia para regulação dos serviços digitais, o *Digital Services Act* (*DSA*);
- Diversas pesquisas publicadas sobre questões atinentes à moderação de conteúdo em plataformas digitais, como:
    - Transparência sobre moderação de conteúdo em políticas de comunidade;
    - Transparência na moderação de conteúdo: tendências regulatórias nacionais;
    - Governança da moderação de conteúdo online: percepções sobre o papel dos atores e regimes.
    - Guia Informativo: Devido processo na regulação da moderação de conteúdo ao redor do mundo.