Considerações em relação ao Projeto de Lei nº 4939/2020

Apresentados na audiência pública de 08/07/2025, na Comissão de Segurança Pública e Combate ao Crime Organizado da Câmara dos Deputados[1]

Excelentíssimo senhor Deputado Hugo Leal e parlamentares da Comissão de Segurança Pública e Combate ao Crime Organizado.

A Derechos Digitales é uma organização da sociedade civil com âmbito de atuação latino-americano, independente, fundada em 2005, cuja missão é a defesa, promoção e desenvolvimento dos direitos humanos no ambiente digital em toda a região[2].

Parabenizamos os esforços do Projeto de Lei nº 4939/2020 ("PL"), assim como a realização desta audiência pública, que demonstra compromisso com o debate democrático e com a construção de um marco legal que reflita os desafios do avanço da digitalização que acompanhamos em nossa sociedade.

Nossos aportes ao PL se concentram em dois eixos fundamentais, que reputamos essenciais para o aprimoramento do texto legislativo: vigilância e gênero, bem como suas intersecções.

Vigilância

Em primeiro lugar, é importante situar o debate onde este PL está inserido em nosso contexto regional. Observamos um aumento preocupante da vigilância estatal e do uso de tecnologias como instrumentos de controle social. Podemos citar, por exemplo, a recente Lei da Guarda Nacional, aprovada no México, que legitima práticas de vigilância sem controle civil ou judicial[3]. No Equador, a também nova Lei de Inteligência amplia sobremaneira o poder de monitoramento

[1] A organização foi representada por Marina Meira, Coordenadora de Políticas Públicas, cujo e-mail para contato é marina.meira@derechosdigitales.org.
[2] Mais informações disponíveis em: https://www.derechosdigitales.org/
[3] R3D. Reformas de "Guardia Nacional" legalizan el espionaje militar. 2025. https://r3d.mx/2025/06/13/ley-de-la-guardia-nacional-legaliza-la-vigilancia-sin-controles-por-parte-del-ejercito/

sobre os cidadãos e suas comunicações sem prever salvaguardas a direitos fundamentais[4].

Na Argentina, foi aprovado um decreto que legitima a Polícia Federal a realizar o patrulhamento cibernético (ou *ciberpatrullaje*, como falamos em espanhol) de indivíduos ou grupos que "erosionem" ou "manipulem" a confiança pública nas políticas de segurança e econômicas do actual governo, ativamente coletando informações sobre essas pessoas em redes abertas de maneira a monitorá-las[5]. É um movimento bastante semelhante ao que ocorreu no Brasil, em 2020, quando a então Secretaria de Operações Integradas (SEOPI) do Ministério da Justiça e Segurança Pública elaborou o que ficou conhecido como dossiês antifascistas, para monitoramento de opositores políticos e movimentos sociais - que foi inclusive condenado e declarado inconstitucional pelo STF em 2022[6].

Esses são exemplos que demonstram como as tecnologias, seja por meio de buscas em fontes abertas, seja por meio de interceptações telemáticas, têm sido utilizadas para legitimar práticas de vigilância estatal massiva. E é essencial compreendermos que essa vigilância representa riscos gravíssimos a direitos fundamentais como a liberdade de expressão e a liberdade de associação, como inclusive tem sido advertido por organismos regionais e internacionais, como a Relatoria Especial para a Liberdade de Expressão da da Comissão Interamericana de Direitos Humanos da OEA[7] e em julgados da Corte Interamericana como o CAJAR *versus* Colômbia[8].

Práticas de vigilância massiva agravam a vulnerabilidade de grupos historicamente perseguidos, como jornalistas, defensores e defensoras de direitos humanos, movimentos sociais e minorias políticas. É dizer, a vigilância sem salvaguardas favorece perseguições políticas, intimidação de dissidentes e

[4] DERECHOS DIGITALES. Análisis sobre el proyecto de Ley de Inteligencia en Ecuador. 2025. https://www.derechosdigitales.org/publicaciones/analisis-sobre-el-proyecto-de-ley-de-inteligencia-en-ecuador/
[5] CHEQUEADO. Ciberpatrullaje: qué dice el nuevo decreto y qué implican los cambios en la Policía Federal. 2025. https://chequeado.com/el-explicador/ciberpatrullaje-que-dice-el-nuevo-decreto-y-que-implican-los-cambios-en-la-policia-federal/
[6] SUPREMO TRIBUNAL FEDERAL. STF julga inconstitucionais atos do Ministério da Justiça sobre dossiês contra antifascistas. 2022. https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=487103&ori=1&goal=0_069298921c-1f117722b2-288596217&mc_cid=1f117722b2
[7] RELATORIA ESPECIAL PARA A LIBERDADE DE EXPRESSÃO. Informe Anual 2023. 2023. https://www.oas.org/es/cidh/expresion/informes/IA2023%20RELE_ES.pdf
[8] CORTE IDH. A Colômbia É Responsável Internacionalmente por haver Realizado Atividades Arbitrárias De Inteligência Contra Defensores De Direitos Humanos, Que Também Foram Vítimas De atos de Violência E Estigmatização Por Parte Das Autoridades Estatais. 2024. https://www.corteidh.or.cr/comunicados_prensa.cfm?lang=pt&n=2020

desencoraja a participação cívica, contribuindo para uma erosão progressiva do tecido democrático.

Em relação ao Projeto de Lei em análise, destacamos preocupações concretas e apontamos sugestões de aprimoramento do texto, a fim de que suas disposições não se tornem mecanismos que, mesmo que pensados com intuito protetivo, possam vir a legitimar práticas de vigilância estatal. O art. 7º, §1º, bem como o art. 14, incisos I e II (na última versão atualizada, de maio), permitem que autoridades estatais — como o Ministério Público e as polícias — requisitem informações pessoais detalhadas, incluindo dados de qualificação, endereço e local de instalação, sem necessidade de ordem judicial. Outro ponto sensível é o art. 9ª, inciso V da versão original (repetido no art. 14, inciso V da versão atualizada, de maio), que autoriza a aquisição de dados em fontes abertas independentemente de autorização judicial, o que tem sido utilizado em outros países e já foi utilizado em âmbito nacional para criar margem para abusos. Um exemplo é a utilização de informações públicas para formulação de dossiês ideológicos.

Em 2023, a Derechos Digitales publicou pesquisa com a também organização internacional APC (Association for Progressive Communications) na qual mapeou 11 casos ao redor do mundo nos quais leis de cibercrime, mesmo que desenhadas para proteção dos cidadãos, acabaram sendo instrumentalizadas para perseguir minorias políticas e sociais[9]. As preocupações apontadas aqui estão, portanto, baseadas em evidências concretas.

Gênero

Em relação a preocupações sobre gênero, é indispensável reconhecer que mulheres e pessoas LGBTQIA+ são desproporcionalmente impactadas tanto pela vigilância estatal quanto por outros atos de violência digital.

Os casos mapeados pela pesquisa mencionada, desenvolvida pela Derechos Digitales e pela APC, mostram como a vigilância reiteradamente se converte em instrumento de controle social e disciplinamento de corpos e vozes dissidentes, afetando especialmente mulheres e a população LGBTQIA+.

Além disso, são estes grupos os principais alvos de crimes e violências perpetrados no ambiente digital, seja por indivíduos, seja por grupos organizados.

[9] DERECHOS DIGITALES; ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS. When protection becomes an excuse for criminalization: gender considerations on cybercrime frameworks. 2023. https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf

Destacamos a situação da violência política de gênero, que tem números alarmantes no Brasil, além da importância de um olhar interseccional que considere outros fatores como raça e território. Segundo dados do Instituto Marielle Franco, 8 em cada 10 mulheres negras que concorreram às eleições em 2020 relataram ataques digitais motivados por gênero, sendo que 42% consideraram abandonar a vida pública[10]. Situação semelhante é enfrentada por mulheres jornalistas[11] e defensoras de direitos humanos[12]. As consequências são graves: autocensura, exclusão de espaços digitais e, consequentemente, exclusão da vida política.

Ao mesmo tempo, as principais pesquisas sobre internet no Brasil, como as conduzidas pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), vinculado ao Comitê Gestor da Internet do Brasil, mostram que as mulheres, e especialmente as mulheres negras, apresentam índices mais baixos de habilidades digitais quando comparadas aos homens, o que as torna mais vulneráveis em relação a fraudes e outros crimes digitais[13].

O PL 4939/2020, tal como redigido, não contempla mecanismos de proteção específicos para essas populações. Na versão original, o projeto reconhece apenas o impacto diferenciado de crimes cibernéticos apenas para políticos do alto escalão. E na última versão, de maio, além desses políticos, no crime de "fraude informática" (previsto na redação do art. 13 da versão atualizada), prevê aumento de pena para crimes cometidos contra "idosos ou vulneráveis".
Há aqui, inclusive, um problema conceitual: a figura jurídica de "vulnerável" é demasiadamente indeterminada e corre o risco de ser instrumentalizada. Mulheres, crianças, jornalistas e defensores e defensoras de direitos humanos são, como apontei, vulneráveis no ambiente digital. Mas é importante que isso seja explicitamente reconhecido, ou que o texto de alguma maneira traga critérios para identificação do que é considerado um sujeito vulnerável, reconhecendo também que essa vulnerabilidade não se limita ao crime de fraude informática, mas a toda a vivência no ambiente digital.

---

[10] FOLHA DE SÃO PAULO. Em cada 10 mulheres negras, 8 sofreram violência virtual nas eleições em 2020, diz estudo. 2021. https://www1.folha.uol.com.br/colunas/monicabergamo/2020/12/em-cada-10-mulheres-negras-8-sofreram-violencia-virtual-nas-eleicoes-em-2020-diz-estudo.shtml

[11] ABRAJI. Violência de gênero contra jornalistas. https://abraji.org.br/projetos/violencia-de-genero-contra-jornalistas

[12] AGÊNCIA PATRÍCIA GALVÃO. Cem mulheres defensoras de direitos humanos e meio ambiente afirmam ter sofrido algum tipo de violência entre 2021 e 2022. 2023. https://dossies.agenciapatriciagalvao.org.br/violencia-em-dados/cem-mulheres-defensoras-de-direitos-humanos-e-meio-ambiente-afirmam-ter-sofrido-algum-tipo-de-violencia-entre-2021-e-2022/

[13] Nesse sentido: CETIC.BR. TIC Domicílios 2024. https://cetic.br/pt/tics/domicilios/2024/individuos/I1A/

Nesse sentido, o alinhamento do PL a legislações já existentes, como a Lei Maria da Penha, a Lei Carolina Dieckmann, o Estatuto da Criança e do Adolescente e a Lei de Violência Política de Gênero, é fundamental para garantir coerência e efetividade protetiva.

Por fim, ainda no âmbito do reconhecimento da vulnerabilidade agravada de mulheres, questionamos a figura de "dados íntimos" prevista no art. 24 da versão original do PL. Trata-se de conceito que não existe na legislação brasileira, e que tampouco é definido pelo texto legislativo, o que pode gerar insegurança jurídica. Aqui, indagamos: o intuito do termo é proteger casos de divulgação não consentida de imagens íntimas? Se for este o objetivo, é necessário explicitar a dimensão de gênero envolvida e prever mecanismos facilitados de produção de prova digital.

Pesquisas indicam que mulheres vítimas de disseminação não consentida de imagens íntimas se sentem desestimuladas a formalizar denúncias, em grande parte devido à burocracia e à revitimização[14]. Se possui essa intenção protetiva, seria de grande valia que o texto pensasse medidas inovadoras em relação a esse tipo de violência de gênero. Um exemplo inclui a atribuição de ônus às plataformas digitais para criação de ferramenta validada de "printscreen" para situações de violações de direitos (sobretudo de mulheres e crianças), evitando que recaia sobre a vítima a necessidade ou o custo de ir a cartórios para fazer autenticação desse meio de prova.

Conclusões e recomendações

- O PL deve se fundamentar marcos de direitos humanos, em conformidade com o direito internacional e regional, pautando-se sempre em princípios de proporcionalidade, legalidade e necessidade.

- Seria interessante fortalecer a exigência de ordem judicial para requisições de dados identificáveis e buscas em fontes abertas, ou então delinear mecanismos de salvaguardas específicos com vistas a evitar abusos e práticas que possam levar à vigilância.

- Definir expressamente a categoria prevista no texto de sujeito "vulnerável", incluindo mulheres, crianças, jornalistas, defensores de direitos humanos e

[14] UMBACH, R. Prevalence and Impacts of Image-Based Sexual Abuse Victimization: A Multinational Study. 2025. https://arxiv.org/abs/2503.04988

pessoas LGBTQIA+.

- Rever o conceito de "dados íntimos", alinhando-o à LGPD e às normativas brasileiras existentes, ou definindo-o no texto.

- Incluir dispositivos que reconheçam e enfrentem explicitamente a violência de gênero online.

- Estimular medidas de prevenção e proteção a essa violência, para garantir a participação política e a liberdade de expressão, especialmente de grupos historicamente minoritários.

Parabenizamos a iniciativa do PL, sempre ressaltando que segurança pública e direitos humanos não são incompatíveis, mas, ao contrário, são complementares e indissociáveis.

Colocamo-nos como Derechos Digitales à disposição desta Comissão e da Câmara dos Deputados para oferecer apoio técnico e seguir contribuindo no aprimoramento do texto, buscando sempre o fortalecimento da democracia, da liberdade e da proteção dos direitos fundamentais no ambiente digital.