São Paulo, 04 de novembro de 2026
Nota pública 007/2026

Nota Pública sobre a PEC da Segurança Pública (PEC 18/2025)

O Senado Federal aprovou, no dia 3 de novembro de 2026, a Proposta de Emenda à Constituição (PEC) nº 18/2025, conhecida como “PEC da Segurança Pública”. Dentre as principais mudanças estão a maior capacidade de ação pelo governo federal, punições mais severas a chefes de facções criminosas, a criação de polícias municipais e a instituição de conselhos de segurança pública e defesa social.

O texto segue para promulgação, mas já é possível prever algumas alterações significativas no campo dos direitos digitais. Primeiramente, a lógica da PEC é trazer maior integração aos entes federativos na investigação e repressão penal, como a criação do Sistema Único de Segurança Pública (SUSP). De forma prática, há exigência da interoperabilidade dos sistemas, compartilhamento de informações e ação articulada para produção de provas (art. 144-A, II, III e IV). Isso significa que o fluxo de dados será cada vez mais intenso entre diferentes organizações, com competências e entes federativos distintos.

Ainda que esse compartilhamento traga potenciais benefícios, é preciso considerar como será efetivada a governança de dados em um cenário de ausência de uma legislação de proteção de dados pessoais para persecução penal.

Para além das medidas técnicas e administrativas adequadas à manutenção dos sistemas, a possibilidade de acesso e compartilhamento de informações voltadas à investigação e repressão penal têm, muitas vezes, caráter sigiloso. Nesse cenário, todos os órgãos integrantes do sistema precisarão observar os princípios e os direitos do titular previstos na LGPD, conforme o art. 4º, § 1º. Isso vale também para o planejamento da aquisição de tecnologias. Ele deverá ir além da exigência de conformidade das empresas privadas fornecedoras e prever, desde a fase de contratação:a) avaliação prévia de impacto; b) cláusulas de auditoria e de acesso às informações pelo poder público; c) vedação ao uso secundário dos dados

pelos fornecedores; e d) definição clara sobre onde os dados serão armazenados e quem poderá acessá-los.

Atribui-se à lei prevista no parágrafo 7º do art. 144 a organização e funcionamento do SUSP, inclusive quanto ao registro, compartilhamento de dados e aquisição de tecnologias para essas finalidades. Destaca-se, no entanto, que o Projeto de Lei nº 1515/2022, também conhecido como "LGPD Penal", aguarda andamento na Comissão de Ciência, Tecnologia e Inovação (CCT) desde outubro de 2025. Trata-se do dispositivo jurídico adequado para regular o fluxo cada vez mais intenso de dados pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Sem a definição desses termos, o projeto de integração do SUSP corre o risco de ser implementado sem a devida segurança jurídica necessária.

Escândalos recentes como os incidentes de segurança do Smart Sampa – que permitiram acesso a milhares de câmeras na cidade de São Paulo – bem como o do Sistema Córtex, plataforma do governo federal que buscava unificar bases e permitir acesso facilitado a agentes de segurança pública para investigações, demonstram que práticas de vigilância podem violar direitos fundamentais de milhões de pessoas. Intensificar a interoperabilidade de dados em segurança pública sem cuidar dos aspectos preventivos em proteção de dados pessoais pode criar uma situação detrimental para a população brasileira no médio prazo.

Sem o devido respeito aos limites constitucionalmente estabelecidos, projetos de interoperabilidade e compartilhamento de dados podem trazer riscos que sabotam a intenção legislativa de trazer eficiência e integração aos entes federativos. A Data Privacy Brasil defende que órgãos de segurança pública tenham políticas de governança de dados bem estabelecidas, com planejamento da aquisição de tecnologias mediante a produção e publicação de Relatórios de Impacto à Proteção de Dados (RIPD), respeito aos princípios da Lei Geral de Proteção de Dados (LGPD) e garantia de direitos de titulares de dados. Como forma de contribuir nesta direção, a instituição promove a formação "Inteligência Artificial e Segurança Pública: governança de dados e direitos fundamentais", em caráter gratuito e exclusivo para agentes de segurança pública. Além disso, a Agência Nacional de Proteção de Dados (ANPD) deve ser fortalecida para que possa fiscalizar e auxiliar em políticas voltadas a esse tema nos próximos anos.

A PEC de Segurança Pública não pode ser um movimento isolado, mas deve estar combinado com a retomada de uma LGPD Penal e com uma cultura preventiva e de participação cívica mais intensa, considerando os riscos a liberdades civis e potenciais lesões ao direito fundamental à proteção de dados pessoais.

A Data Privacy Brasil disponibiliza seus especialistas e porta-vozes para comentários e mais informações sobre a pauta.

Assessoria de Imprensa da Data Privacy Brasil
imprensa@dataprivacybr.org