PARECER Nº , DE 2025

Da COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA, sobre o Projeto de Lei nº 4752, de 2025, do Senador Esperidião Amin e outros, que *institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei nº 13.756, de 12 de dezembro de 2018*.

Relator: Senador **HAMILTON MOURÃO**

I – RELATÓRIO

Vem para análise do Senado Federal o Projeto de Lei nº 4752, de 2025, do Senador Esperidião Amin e outros, que institui o Marco Legal da Cibersegurança, cria o Programa Nacional de Segurança e Resiliência Digital e altera a Lei nº 13.756, de 12 de dezembro de 2018.

A matéria foi distribuída à Comissão de Constituição, Justiça e Cidadania - CCJ, onde me coube a relatoria, e posteriormente seguirá para análise da Comissão de Ciência, Tecnologia, Inovação e Informática - CCT, cabendo à última comissão a decisão terminativa.

Entre os objetivos principais da proposição, ínsitos no Capítulo I, estão o fortalecimento da resiliência cibernética da administração pública, a prevenção e mitigação de incidentes cibernéticos, a promoção da integração entre políticas de segurança da informação, o estímulo à formação de recursos humanos especializados, e o fomento da cooperação entre setores público, privado e sociedade civil.

O Capítulo II do projeto define as competências da Autoridade Nacional de Cibersegurança, que incluem normatização, fiscalização, auditoria e instrução de processos administrativos. A autoridade também estabelecerá padrões mínimos de cibersegurança, que serão revisados periodicamente e submetidos a consulta pública.

O Programa Nacional de Segurança e Resiliência Digital, previsto no Capítulo III, é instituído no âmbito da administração pública federal, com possibilidade de adesão por estados, municípios e organizações do setor privado. Os seus objetivos incluem implementar princípios e diretrizes de resiliência cibernética, estabelecer planos de resiliência, definir metas e indicadores de desempenho, e promover a integração das ações entre diversos setores críticos. Para cumprir seus objetivos, o programa contará com instrumentos como planos setoriais de resiliência, protocolos de resposta a incidentes, sistemas de monitoramento, campanhas de conscientização e mecanismos de adesão voluntária.

A participação dos entes federativos no programa está associada ao compromisso de desenvolver e implementar iniciativas próprias de cibersegurança, incluindo planos locais de cibersegurança, criação de equipes de resposta a incidentes e promoção de ações de capacitação. Além disso, os entes participantes devem integrar a avaliação e mitigação de riscos cibernéticos de seus fornecedores aos seus programas internos de resiliência cibernética, bem como devem promover programas de capacitação, parcerias com universidades e centros de pesquisa, e incentivar a inclusão de conteúdos de cibersegurança nas grades curriculares. Em contrapartida, a adesão ao programa confere acesso prioritário aos recursos do Fundo Nacional de Segurança Pública destinados à cibersegurança, incluindo programas de capacitação e sistemas de alerta.

Ademais, o programa será monitorado continuamente, com publicação periódica de indicadores, metas e resultados alcançados, visando à melhoria da resiliência cibernética nacional. De acordo com o art. 25 da proposição, os órgãos responsáveis pela aplicação dos recursos devem publicar relatórios detalhados das receitas, despesas e resultados alcançados, submeter suas contas à auditoria e garantir a participação e controle social.

Nas disposições finais (Capítulo IV), altera-se a Lei nº 13.756, de 12 de dezembro de 2018, para destinar um percentual dos recursos do Fundo Nacional de Segurança Pública a ações de cibersegurança, incluindo financiamento de projetos de modernização tecnológica, formação de recursos humanos e apoio à pesquisa e inovação.

A exposição de motivos destaca, entre outros aspectos, que:

> O Brasil tem enfrentado uma escalada de incidentes cibernéticos que afetam a prestação de serviços públicos, expõem dados sensíveis de milhões de cidadãos e colocam em risco a estabilidade institucional de diversos órgãos e entidades da federação. Esses episódios evidenciam a fragilidade das estruturas nacionais diante de ameaças cada vez mais sofisticadas, persistentes e com forte impacto geopolítico. Globalmente, os crescentes prejuízos decorrentes de ciberataques têm levado governos a estruturarem marcos legais, investir em recursos humanos e criar órgãos permanentes para coordenar a segurança cibernética.

Não foram recebidas emendas no prazo regimental.

II – ANÁLISE

O projeto de lei em análise não apresenta vício de constitucionalidade, juridicidade e regimentalidade e está redigido de acordo com os padrões de redação preconizados pela Lei Complementar nº 95, de 26 de fevereiro de 1998.

Os requisitos formais e materiais de constitucionalidade são cumpridos. A iniciativa parlamentar é legítima; os termos da proposição não importam em violação de cláusula pétrea; e não há reserva temática de iniciativa que importe em vício.

Sobre o mérito, o PL nº 4752, de 2025, de autoria do Senador Esperidião Amin e outros, institui o Marco Legal da Cibersegurança com um foco pragmático: fortalecer a resiliência cibernética da administração pública em todos os entes da federação (União, estados, Distrito Federal e municípios).

As diretrizes do PL são focadas na gestão pública, incluindo a resposta coordenada a incidentes, a promoção de uma cultura de cibersegurança entre

servidores, a proteção de infraestruturas críticas e a responsabilização de gestores e agentes públicos. O projeto prevê a designação de uma "autoridade nacional de cibersegurança", que será responsável por normatizar, fiscalizar e auditar, além de estabelecer padrões mínimos de segurança, cabendo ao Poder Executivo sua determinação.

O núcleo do projeto é o Programa Nacional de Segurança e Resiliência Digital, voltado para a administração pública federal, com possível adesão de estados e municípios, comprometendo-se a desenvolver seus próprios planos locais de cibersegurança e a criar ou fortalecer equipes de resposta a incidentes.

A proposição enfatiza a governança de riscos das cadeias de suprimentos, em que cabe aos órgãos públicos participantes a avaliação dos riscos cibernéticos de seus fornecedores e parceiros. A autoridade nacional poderá, inclusive, criar um índice de maturidade e confiabilidade de fornecedores e restringir a adoção de soluções descontinuadas ou sem suporte.

Além disso, a criação de um mecanismo de financiamento estável é inovadora, mediante alteração da Lei nº 13.756, de 2018, pelo art. 26 da proposição, para determinar que, no mínimo, 3% dos recursos do Fundo Nacional de Segurança Pública (FNSP) sejam aplicados em ações de cibersegurança. Em acréscimo, destina 2% da arrecadação das apostas de quota fixa (apostas esportivas) para o FNSP, especificamente para ações de cibersegurança.

Portanto, a proposição demonstra alto grau de maturidade institucional e pragmatismo, sendo seu foco na resiliência da administração pública um recorte estratégico e factível, diante de ameaças cibernéticas que podem causar enormes danos às nossas infraestruturas críticas e soberania.

Merece, assim, total apoio deste relator.

III – VOTO

Por ser conveniente e oportuno aos interesses nacionais, constitucional, jurídico e regimental, somos pela **aprovação** do Projeto de Lei nº 4752, de 2025.

Sala da Comissão,

, Presidente

, Relator