



CÂMARA DOS DEPUTADOS
Gabinete do Deputado Federal Duda Ramos – PODE/RR

PROJETO DE LEI Nº , DE 2026

(Do Sr. DUDA RAMOS)

Institui a Política Nacional de
Localização Estratégica e Resiliência dos
Dados Críticos e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Fica instituída a Política Nacional de Localização Estratégica e Resiliência dos Dados Críticos, destinada a fortalecer a segurança nacional, a continuidade dos serviços essenciais, a soberania digital, a resiliência das infraestruturas críticas e a capacidade nacional de processamento e recuperação de informações estratégicas.

Parágrafo único. A Política observará os princípios da livre iniciativa, da livre concorrência, da segurança jurídica, da neutralidade tecnológica, da interoperabilidade, da proporcionalidade, da soberania nacional, da continuidade dos serviços essenciais e da cooperação internacional.

Art. 2º Para os fins desta Lei considera-se:

I – dados críticos: informações cuja indisponibilidade, perda de integridade ou comprometimento possa produzir impactos relevantes sobre a segurança nacional, a continuidade de serviços essenciais, a estabilidade econômica, a infraestrutura crítica ou a administração pública;

II – localização estratégica de dados: adoção de medidas destinadas a assegurar que dados críticos disponham de capacidade adequada de armazenamento, processamento, recuperação ou continuidade operacional compatível com os interesses estratégicos nacionais;



III – resiliência digital: capacidade de prevenir, resistir, responder e recuperar-se de incidentes capazes de comprometer a disponibilidade ou integridade de dados críticos;

IV – redundância operacional: manutenção de mecanismos técnicos destinados à continuidade dos serviços em caso de indisponibilidade de infraestrutura principal.

§1º Esta Lei não estabelece obrigação geral de armazenamento de dados exclusivamente em território nacional.

§2º Esta Lei não restringe a utilização de serviços de computação em nuvem, tecnologias de processamento distribuído ou infraestruturas internacionais de armazenamento de dados, observado o interesse público e a legislação aplicável.

§3º Permanecem integralmente preservados os regimes jurídicos previstos na Lei Geral de Proteção de Dados Pessoais, no Marco Civil da Internet, na Lei de Acesso à Informação, na legislação de segurança cibernética e nas demais normas aplicáveis.

Art. 3º São objetivos da Política:

I – fortalecer a continuidade dos serviços essenciais;

II – ampliar a resiliência das infraestruturas digitais críticas;

III – reduzir vulnerabilidades relacionadas à indisponibilidade de dados estratégicos;

IV – estimular o desenvolvimento da infraestrutura nacional de armazenamento e processamento de dados;

V – fortalecer a soberania digital brasileira;

VI – incentivar investimentos em infraestrutura tecnológica nacional;

VII – promover ambiente favorável à inovação e à transformação digital;



VIII – ampliar a capacidade nacional de resposta a incidentes cibernéticos.

Art. 4º Poderão ser considerados dados críticos, observado o interesse público e a regulamentação específica, aqueles relacionados:

- I – aos sistemas financeiros e de pagamentos;
- II – às infraestruturas de energia;
- III – às telecomunicações;
- IV – aos sistemas de saúde;
- V – à defesa civil;
- VI – ao abastecimento de água;
- VII – aos transportes;
- VIII – às infraestruturas digitais estratégicas;
- IX – à defesa nacional;
- X – às demais infraestruturas críticas definidas em regulamento.

Parágrafo único. A classificação prevista neste artigo possui finalidade orientadora e não altera regimes jurídicos específicos estabelecidos em legislação própria.

Art. 5º A implementação da Política buscará estimular que os dados críticos disponham de mecanismos adequados de:

- I – redundância operacional;
- II – recuperação de desastres;
- III – continuidade dos serviços;
- IV – processamento seguro;
- V – disponibilidade operacional.



Art. 6º As ações decorrentes desta Lei observarão critérios de proporcionalidade, análise de risco, viabilidade técnica, impacto econômico e natureza das atividades envolvidas.

Art. 7º As ações decorrentes desta Lei buscarão promover:

- I – continuidade operacional;
- II – segurança da informação;
- III – integridade dos dados;
- IV – disponibilidade dos sistemas;
- V – interoperabilidade;
- VI – recuperação rápida de incidentes.

Art. 8º O Poder Público deverá estimular estudos e avaliações destinados à identificação de vulnerabilidades relacionadas à localização, disponibilidade e recuperação de dados críticos.

Art. 9º A Política buscará incentivar a expansão da infraestrutura nacional de armazenamento, processamento e recuperação de dados, observados os princípios da livre iniciativa, da livre concorrência e da neutralidade tecnológica.

Art. 10. As ações decorrentes desta Lei deverão estimular:

- I – centros de processamento de dados;
- II – infraestrutura de computação em nuvem;
- III – tecnologias de recuperação de desastres;
- IV – soluções de armazenamento distribuído;
- V – computação de alto desempenho;
- VI – infraestrutura digital resiliente.



Art. 11. A implementação da Política poderá ocorrer mediante cooperação entre órgãos públicos, instituições científicas, universidades, empresas, entidades representativas e demais organizações nacionais e internacionais.

Art. 12. A cooperação internacional observará os interesses estratégicos nacionais, os acordos internacionais dos quais o Brasil seja parte e a legislação brasileira.

Art. 13. A Política Nacional de Localização Estratégica e Resiliência dos Dados Críticos será implementada em articulação com as políticas nacionais de transformação digital, segurança cibernética, ciência, tecnologia e inovação, defesa nacional, infraestrutura digital e proteção de infraestruturas críticas.

Art. 14. A implementação desta Lei observará as disponibilidades orçamentárias e financeiras dos órgãos e entidades competentes.

Art. 15. Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

A transformação digital tornou-se elemento central para o funcionamento do Estado, da economia e dos serviços essenciais. Sistemas financeiros, plataformas de pagamento, redes de saúde, energia, telecomunicações, transportes, defesa civil, serviços públicos digitais e infraestruturas críticas dependem, cada vez mais, da disponibilidade, integridade, armazenamento, processamento e recuperação de dados.

Nesse contexto, a ausência de uma política nacional voltada à localização estratégica e à resiliência dos dados críticos representa risco crescente para o País. Não se trata de impor armazenamento obrigatório de todos os dados em território nacional, mas de reconhecer que determinadas



informações são tão relevantes para a continuidade dos serviços essenciais que sua indisponibilidade, perda ou comprometimento pode produzir efeitos econômicos, sociais e institucionais graves.

Os riscos já são concretos. Relatório do Fundo Monetário Internacional aponta que o número de ataques cibernéticos praticamente dobrou desde o período anterior à pandemia de Covid-19 e que eventos extremos podem gerar perdas de pelo menos US\$ 2,5 bilhões. O mesmo relatório alerta que incidentes cibernéticos severos podem afetar a estabilidade macrofinanceira, especialmente quando atingem instituições financeiras ou serviços essenciais.

A gravidade do cenário também aparece nos custos de violações de dados. Estudo global da IBM indicou custo médio de US\$ 4,88 milhões por violação de dados em 2024, enquanto, no setor financeiro, esse valor alcançou US\$ 6,08 milhões. Ou seja, a indisponibilidade ou o comprometimento de dados deixou de ser apenas problema técnico, tornou-se risco econômico relevante.

Além dos ataques cibernéticos, há o risco operacional. Falhas em data centers, indisponibilidades de nuvem, interrupções de conectividade e ausência de redundância podem afetar serviços essenciais e gerar prejuízos expressivos. Levantamentos internacionais sobre interrupções em infraestruturas digitais indicam que os apagões tecnológicos, embora menos frequentes em alguns segmentos, tornaram-se cada vez mais caros, com parte relevante dos incidentes superando centenas de milhares ou até milhões de dólares.

No Brasil, a relevância dos dados críticos é evidente. O funcionamento cotidiano do País depende de sistemas digitais de pagamentos, serviços públicos eletrônicos, registros administrativos, bases de saúde, telecomunicações, redes de energia, sistemas logísticos e plataformas de atendimento ao cidadão. A interrupção de qualquer dessas estruturas pode



afetar milhões de pessoas, comprometer atividades econômicas e reduzir a capacidade de resposta do Estado.

A presente proposição institui a Política Nacional de Localização Estratégica e Resiliência dos Dados Críticos, com a finalidade de fortalecer a continuidade operacional, a segurança nacional, a soberania digital e a capacidade de recuperação de informações essenciais ao funcionamento do País.

A proposta foi construída com cautela. Não cria obrigação geral de armazenamento de dados exclusivamente no Brasil, não impede o uso de computação em nuvem, não restringe o comércio digital e não interfere indevidamente nos modelos de negócio. O objetivo é estabelecer diretrizes para que dados críticos contem com mecanismos adequados de redundância, recuperação de desastres, continuidade operacional, segurança da informação e disponibilidade.

Trata-se de política de prevenção. A ausência de planejamento nesse campo pode deixar o País vulnerável a falhas sistêmicas, ataques cibernéticos, interrupções externas, indisponibilidade de serviços e dependências tecnológicas incompatíveis com a proteção de infraestruturas essenciais.

A medida também contribui para estimular investimentos em data centers, computação em nuvem, recuperação de desastres, armazenamento distribuído, segurança cibernética e infraestrutura digital resiliente, fortalecendo a economia digital brasileira sem criar barreiras artificiais à inovação.

Em um mundo marcado por crescente competição tecnológica e por riscos cibernéticos cada vez mais sofisticados, a proteção dos dados críticos deve ser compreendida como componente da soberania nacional, da segurança econômica e da continuidade dos serviços públicos e privados essenciais.



A presente proposição, portanto, busca preparar o Brasil para os desafios da economia digital contemporânea, assegurando que os dados indispensáveis ao funcionamento do Estado, da sociedade e da economia disponham de níveis adequados de resiliência, proteção e capacidade de recuperação.

Diante da relevância estratégica, econômica, tecnológica e institucional da matéria, conclamamos os Nobres Pares a apoiarem a presente proposição.

Sala das Sessões, em 2026.

Deputado DUDA RAMOS

