



CÂMARA DOS DEPUTADOS
Gabinete do Deputado Federal Duda Ramos - MDB/RR

PROJETO DE LEI Nº _____, DE 2025

(Do Sr. DUDA RAMOS)

Dispõe sobre a obrigatoriedade de fornecimento célere de dados por provedores de aplicações e redes sociais à autoridade policial, com o objetivo de desburocratizar e acelerar as investigações criminais, e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta Lei estabelece normas para o fornecimento célere, seguro e padronizado de dados cadastrais, de conexão e de conteúdo armazenado por provedores de aplicações e redes sociais à autoridade policial competente, com a finalidade de acelerar e desburocratizar os procedimentos investigativos, respeitados os direitos fundamentais e as garantias constitucionais.

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

I – provedor de aplicação de internet: pessoa jurídica que oferece serviço de comunicação, hospedagem, compartilhamento ou interação entre usuários por meio da internet;

II – dados cadastrais: informações fornecidas pelo usuário para identificação, tais como nome completo, endereço, número de documento, telefone e e-mail;

III – dados de conexão: informações referentes à data, hora, duração e endereço de IP utilizado na conexão à rede;

IV – dados de conteúdo: mensagens, postagens, imagens, vídeos, áudios ou quaisquer comunicações armazenadas digitalmente;



V – autoridade policial: delegado de polícia civil ou federal legalmente investido na função investigativa, nos termos do artigo 144 da Constituição Federal.

Art. 3º Os provedores de aplicações e redes sociais deverão fornecer dados cadastrais básicos de usuários investigados, mediante requisição direta da autoridade policial, sem necessidade de autorização judicial prévia, desde que a investigação esteja formalmente instaurada e o pedido devidamente fundamentado.

§ 1º A requisição deverá conter:

I – número do inquérito ou procedimento investigativo;

II – identificação do delegado responsável e do órgão de polícia judiciária solicitante;

III – descrição sucinta da finalidade e relevância do dado requerido.

§ 2º O provedor deverá cumprir a requisição no prazo máximo de 24 (vinte e quatro) horas, contado do recebimento, sob pena de responsabilidade administrativa e civil.

§ 3º O fornecimento de dados cadastrais nos termos deste artigo não caracteriza violação de sigilo ou de privacidade, nos termos do artigo 10, §3º, do Marco Civil da Internet.

Art. 4º O acesso a dados de conexão e a dados de conteúdo armazenado dependerá de autorização judicial específica, requerida pela autoridade policial ou pelo Ministério Público, nos termos da legislação vigente, mediante demonstração da necessidade, adequação e proporcionalidade da medida.

§ 1º Deferida a autorização judicial, o provedor de aplicação ou rede social deverá disponibilizar integralmente as informações requisitadas no prazo máximo de cinco dias úteis, contado da ciência da decisão, ressalvadas as situações de sigilo judicial diverso expressamente fixado.



§ 2º Em situações de risco iminente à vida, à integridade física, à segurança pública ou à preservação de provas digitais voláteis, a autoridade policial poderá requisitar acesso emergencial aos dados, mediante comunicação imediata ao juízo competente, que deverá homologar a medida no prazo de vinte e quatro horas.

§ 3º O provedor deverá comunicar imediatamente à autoridade requisitante a data e hora de cumprimento da medida, bem como eventuais limitações técnicas ou impossibilidades de acesso, sob pena de responsabilidade administrativa e civil em caso de omissão.

§ 4º A entrega de dados deverá observar padrões técnicos de segurança da informação, criptografia e autenticação digital, assegurando a integridade, rastreabilidade e confidencialidade das informações fornecidas.

§ 5º A preservação e guarda dos registros eletrônicos necessários à investigação deverão ser asseguradas pelo provedor de aplicação, a pedido da autoridade policial ou judicial, pelo prazo mínimo de cento e oitenta dias, prorrogável por igual período mediante justificativa.

§ 6º O descumprimento injustificado dos prazos ou das obrigações previstas neste artigo caracteriza infração grave, sujeitando o infrator às sanções administrativas e pecuniárias estabelecidas nesta Lei, sem prejuízo das responsabilidades civil e penal cabíveis.

Art. 5º Fica instituído, no âmbito do Poder Executivo Federal, o Sistema Nacional de Requisição Eletrônica de Dados Digitais, destinado à transmissão segura, rastreável e padronizada de informações entre as autoridades competentes e os provedores de aplicações e redes sociais, para fins de investigação criminal ou instrução processual.

§ 1º O Sistema Nacional de Requisição Eletrônica de Dados Digitais será gerido pelo Ministério da Justiça e Segurança Pública, que definirá os protocolos técnicos de comunicação, autenticação digital e registro de acessos, observadas as normas da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).



§ 2º Os provedores de aplicações e redes sociais deverão integrar-se obrigatoriamente ao sistema, garantindo compatibilidade tecnológica e disponibilidade permanente de canal eletrônico específico para o recebimento e resposta das requisições de dados.

§ 3º As requisições e respostas deverão ser assinadas digitalmente, com registro automático de data, hora e identificação do solicitante e do atendente, assegurando rastreabilidade, integridade e auditabilidade das operações realizadas.

§ 4º O sistema deverá assegurar níveis diferenciados de acesso conforme a natureza da informação solicitada, garantindo:

I – acesso restrito e autenticado às autoridades policiais e ministeriais;

II – controle e monitoramento contínuo de todos os pedidos e respostas;

III – mecanismos de auditoria independente e de comunicação com o Poder Judiciário e os órgãos de controle.

§ 5º Os provedores de aplicações e redes sociais deverão manter estrutura técnica e corpo especializado para o cumprimento célere das requisições, devendo garantir atendimento ininterrupto e suporte em situações de urgência ou risco grave à segurança pública.

§ 6º As informações transmitidas pelo sistema terão sigilo legal e proteção integral contra acesso não autorizado, sendo o seu uso restrito à finalidade investigativa ou processual que motivou a requisição.

§ 7º O descumprimento das obrigações previstas neste artigo sujeitará o provedor infrator às sanções administrativas e pecuniárias estabelecidas nesta Lei, sem prejuízo das responsabilidades civil e penal cabíveis.



Art. 6º O descumprimento injustificado dos prazos e obrigações previstos nesta Lei sujeitará o provedor de aplicação às seguintes penalidades, sem prejuízo das responsabilidades civil e penal:

I – advertência, com prazo de 10 (dez) dias para regularização;

II – multa administrativa de R\$ 50.000,00 (cinquenta mil reais) a R\$ 5.000.000,00 (cinco milhões de reais), de acordo com a gravidade da infração e o porte econômico da empresa;

III – suspensão temporária do funcionamento do serviço no território nacional, em caso de reincidência grave;

IV – impedimento de contratação com o poder público enquanto perdurar a irregularidade.

Parágrafo único. Os valores arrecadados com multas serão destinados ao Fundo Nacional de Segurança Pública.

Art. 7º O tratamento, o compartilhamento e o armazenamento dos dados fornecidos nos termos desta Lei deverão observar os princípios da finalidade, necessidade, proporcionalidade, segurança, transparência e responsabilidade, previstos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e as normas do Marco Civil da Internet.

§ 1º Os dados obtidos em decorrência desta Lei somente poderão ser utilizados para os fins estritamente relacionados à investigação criminal ou à instrução processual que motivaram a requisição, sendo vedada sua divulgação, reprodução ou utilização para qualquer outro propósito.

§ 2º As autoridades policiais e os agentes públicos que tiverem acesso às informações responderão civil, penal e administrativamente por qualquer uso indevido, vazamento, perda ou destruição dos dados, na forma da legislação aplicável.

§ 3º Os provedores de aplicações e redes sociais deverão manter registro eletrônico de todas as requisições recebidas e atendidas, contendo data, hora, natureza da solicitação e identificação do solicitante e do



responsável técnico pelo atendimento, pelo prazo mínimo de cinco anos, para fins de auditoria e controle externo.

§ 4º Os dados armazenados e transmitidos deverão ser protegidos por mecanismos de criptografia e autenticação digital, assegurando sua integridade, confidencialidade e rastreabilidade.

§ 5º O Ministério da Justiça e Segurança Pública, em articulação com a Autoridade Nacional de Proteção de Dados, expedirá normas complementares para a fiscalização, auditoria e verificação de conformidade das medidas de segurança e tratamento das informações.

§ 6º O descumprimento das obrigações previstas neste artigo sujeitará o infrator — autoridade, servidor público ou provedor — às sanções civis, administrativas e penais cabíveis, sem prejuízo das previstas nesta Lei.

Art. 8º O Poder Executivo regulamentará esta Lei no prazo de 120 (cento e vinte) dias, contado da data de sua publicação, definindo:

- I – os procedimentos técnicos do SIREDD;
- II – os padrões de segurança cibernética e criptografia;
- III – os prazos e protocolos operacionais de integração;
- IV – os mecanismos de fiscalização e auditoria.

Art. 9º Esta Lei entra em vigor na data de sua publicação.

JUSTIFICAÇÃO

O presente Projeto de Lei tem por finalidade disciplinar o fornecimento célere, padronizado e seguro de dados por redes sociais e provedores de aplicações de internet à autoridade policial, de forma a modernizar e desburocratizar os procedimentos investigativos no Brasil, garantindo eficiência, transparência e respeito aos direitos fundamentais.



Atualmente, o acesso a informações digitais essenciais para a elucidação de crimes é marcado por demoras injustificadas, burocracia excessiva e ausência de integração tecnológica entre as plataformas digitais e os órgãos de segurança pública.

Casos graves de crimes cibernéticos, fraudes financeiras, sequestros, ameaças, tráfico e exploração sexual frequentemente dependem de dados que, por falta de um fluxo padronizado e célere, chegam tardiamente ou são irrecuperáveis, comprometendo a eficácia da persecução penal.

O projeto propõe um novo modelo de cooperação digital entre o Estado e as empresas de tecnologia, com fundamento no artigo 144 da Constituição Federal, que atribui ao Estado o dever de garantir a segurança pública e à polícia judiciária o exercício da investigação criminal.

Para isso, o texto estabelece três pilares essenciais:

Celeridade e eficiência — autoriza a obtenção de dados cadastrais básicos mediante requisição direta da autoridade policial, sem necessidade de autorização judicial, desde que o pedido seja formalmente justificado e vinculado a investigação regularmente instaurada, preservando o controle judicial para os dados de conteúdo e comunicação privada.

Integração tecnológica e rastreabilidade — cria o Sistema Nacional de Requisição Eletrônica de Dados Digitais, sob gestão do Ministério da Justiça e Segurança Pública, permitindo a tramitação digital segura de requisições e respostas, com autenticação, assinatura eletrônica, registros de auditoria e controle automatizado de prazos.

Proteção de dados e responsabilidade — consolida a aplicação dos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo que o uso das informações seja restrito ao contexto da investigação criminal, com proteção integral, criptografia, rastreabilidade e responsabilização objetiva de agentes públicos e provedores por vazamentos, uso indevido ou descumprimento de prazos.



A proposta não amplia poderes investigativos, mas moderniza os meios de acesso, eliminando gargalos burocráticos que atrasam ou inviabilizam investigações urgentes. A celeridade no fornecimento de dados não significa violação de sigilo, mas sim a adequação dos procedimentos à realidade tecnológica contemporânea, em que as provas digitais são muitas vezes voláteis e desaparecem em poucas horas.

A criação de um sistema nacional unificado também garante segurança jurídica às empresas provedoras, que passarão a operar dentro de um protocolo federal claro, auditável e tecnicamente seguro, em substituição à multiplicidade de ofícios e solicitações despadronizadas hoje existentes.

Trata-se, portanto, de uma proposta equilibrada e constitucionalmente adequada, que reforça o papel da polícia judiciária, fortalece a proteção de dados pessoais, impede o uso indevido de informações e garante o cumprimento do dever estatal de proteger a sociedade.

O Brasil precisa de um modelo investigativo ágil, digital e responsável, capaz de enfrentar a criminalidade organizada e cibernética com as ferramentas do século XXI — e este projeto responde precisamente a essa necessidade.

Posto isso, conto com o apoio dos nobres colegas parlamentares para a aprovação da matéria.

Sala das Sessões, em 2025.

Deputado DUDA RAMOS

