

**Projeto de Lei Ordinária Nº \_\_\_\_\_, DE 2026.**  
**(Do Sr. Rubens Pereira Júnior)**

Altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), para prever hipótese excepcional e estrita de acesso imediato a dados de conexão e tráfego sem ordem judicial prévia em casos de risco iminente à vida ou integridade física, sequestro, ataque terrorista iminente ou crime cibernético em curso que esteja causando dano imediato; exige autorização fundamentada de autoridade policial de alto escalão, comunicação imediata ao Ministério Público e homologação judicial no prazo máximo de 48 horas; veda o acesso a conteúdo de comunicações; impõe requisitos de proporcionalidade, minimização dos dados acessados, prazo máximo de retenção, registro detalhado das diligências, auditoria externa periódica e sanções para uso indevido; e dá outras providências.

O Congresso Nacional decreta:



Art. 1º Fica acrescido à Lei nº 12.965, de 23 de abril de 2014, o seguinte art. 19-A:

"Art. 19-A. Em caráter excepcional e apenas nas hipóteses e observadas as condições previstas neste artigo, admite-se o acesso imediato, sem ordem judicial prévia, a dados de conexão e registros de tráfego necessários e estritamente proporcionais à finalidade, quando cumulativamente verificados:

I. risco iminente e atual à vida ou à integridade física de pessoa(s), sequestro em curso, ameaça de ataque terrorista iminente ou crime cibernético em curso que esteja causando dano imediato e que só possa ser evitado mediante a identificação urgente de endereços IP ou outros dados de conexão/registro de tráfego; e

II. necessidade demonstrada e contemporânea de identificação de dados de conexão ou registros de tráfego imprescindíveis para a interrupção imediata do risco descrito no inciso I, não sendo suficiente a adoção de medidas alternativas viáveis em tempo hábil.

§ 1º A autorização para o acesso referido no caput dependerá de autorização prévia, fundamentada e escrita de autoridade policial de alto escalão, nos termos deste parágrafo, com exposição sucinta dos fatos, indicação dos elementos probatórios que justificam a emergência, delimitação clara e estrita dos dados solicitados (escopo temporal, tipológico e quantitativo) e assinatura do delegado de polícia com atribuição na investigação ou do chefe da unidade investigativa designada para a diligência. A autorização deverá ser comunicada de imediato, por meio eletrônico seguro, ao Ministério Público local, com juntada de cópia integral do ato de autorização.

§ 2º É vedada a requisição, coleta, interceptação, visualização, reprodução, gravação ou exploração do conteúdo das comunicações privadas (corpo da mensagem, texto, áudio, vídeo ou arquivos transferidos) no âmbito da autorização prevista no caput, salvo quando houver hipótese legal distinta que exija processo diverso e ordem judicial específica para acesso ao conteúdo.



§ 3º O acesso autorizado nos termos deste artigo deverá ser submetido a requerimento de homologação judicial no prazo máximo de 48 (quarenta e oito) horas contadas do momento do primeiro acesso efetivo aos dados. Na análise do pedido, o juiz deverá verificar a legalidade, a necessidade, a adequação e a proporcionalidade da medida, podendo determinar a manutenção, a modificação, a limitação ou a cessação da medida, bem como a produção de outras provas e a imposição de medidas de mitigação de riscos.

§ 4º Não sendo requerido o pedido de homologação no prazo previsto no § 3º, ou não sendo este homologado, o juiz deverá, salvo determinação judicial em contrário, determinar, no prazo de 48 (quarenta e oito) horas, a destruição segura e certificada dos dados coletados indevidamente, bem como o cancelamento de quaisquer cópias, réplicas ou derivações deles existentes em sistemas públicos ou privados.

§ 5º Da hipótese de autorização, independentemente do requerimento de homologação, deverá constar registro detalhado em sistema seguro e com acesso restrito, contendo: identificação da autoridade autorizante, fundamentos factuais e jurídicos, delimitação do escopo temporal e tipológico dos dados, finalidade específica, nomes e cargos dos agentes que realizaram o acesso, data e hora do início e do término da diligência, e indicação dos dados efetivamente acessados. Metadados e motivação sumarizada deverão ser divulgados em formato agregado e não identificador, respeitado o sigilo investigativo, para fins de transparência pública.

§ 6º É exigido o envio, em prazo oportuno e compatível com o sigilo da investigação, de relatório circunstanciado ao juízo competente e ao Ministério Público, contendo descrição dos atos praticados, justificativa da excepcionalidade e laudo técnico sobre os dados obtidos e sua utilização para interromper o risco iminente.

§ 7º O acesso deverá observar estrito princípio da minimização: apenas os dados estritamente necessários ao cumprimento da finalidade e no menor recorte temporal possível poderão ser solicitados e acessados. Salvo homologação judicial em sentido diverso, o prazo máximo de retenção dos dados acessados no âmbito da



autorização emergencial será de 30 (trinta) dias, findo o qual deverá ocorrer sua eliminação segura e certificada, sem prejuízo de cópias indispensáveis a fins de prova autorizadas em decisão judicial posterior.

§ 8º Submete-se o procedimento de autorização e os registros a auditoria externa periódica por órgão independente designado por ato do Poder Legislativo ou por autoridade constituída para esse fim (entre as quais, o Tribunal de Contas da União, a Autoridade Nacional de Proteção de Dados ou comissão técnica designada pelo Congresso Nacional), com acesso a logs e registros, observadas as limitações inerentes a investigações em curso; o relatório de auditoria deverá ser divulgado em versão consolidada, de caráter público, preservando-se informações sigilosas que possam comprometer investigações em andamento.

§ 9º A autoridade ou agente público que autorizar, praticar, ordenar, executar ou utilizar indevidamente o acesso previsto neste artigo responde administrativa, civil e penalmente, nos termos da lei, sem prejuízo da responsabilização das empresas provedoras que, com conhecimento de sua irregularidade, colaborarem ou permitirem a medida, sendo assegurados meios de reparação às vítimas.

§ 10. As disposições deste artigo aplicam-se prospectivamente. Quanto aos acessos realizados antes da vigência da presente norma, os atos em curso deverão ser objeto de procedimento de regularização e revisão, nos termos e limites que o regulamento do dispositivo estabelecer, que poderão compreender requerimento de homologação judicial, preservação eventual de dados essenciais à continuidade de investigações devidamente justificadas e destruição dos demais dados, respeitados os direitos das partes e garantias constitucionais."

Art. 2º O art. 5º da Lei nº 12.965, de 2014, passa a vigorar acrescido do seguinte § 4º:

"§ 4º Para efeitos desta Lei, os conceitos de 'dados de conexão' e 'registros de tráfego' correspondem às definições constantes da legislação específica aplicável, e o acesso emergencial a tais dados observará as condições e limites previstos no art. 19-A."



Art. 3º As autoridades policiais e o Ministério Público da União e dos Estados deverão elaborar, publicar e manter atualizados, no prazo de 60 (sessenta) dias contados da entrada em vigor desta Lei, procedimentos internos padronizados para atendimento de pedidos emergenciais previstos no art. 19-A, contendo, no mínimo:

- I. formulários e modelos de requisição fundamentada;
- II. fluxo de comunicação imediata entre autoridade policial e Ministério Público local;
- III. cronograma e responsáveis para o requerimento de homologação judicial nos prazos legais;
- IV. medidas de preservação e segurança dos registros e dados acessados; e
- V. diretrizes para elaboração do relatório circunstanciado referido no § 6º do art. 19-A.

Parágrafo único. Os procedimentos previstos neste artigo deverão ser publicados em sítio eletrônico oficial, ressalvadas informações cuja divulgação comprometa investigações em curso, e disponibilizados a órgãos de controle e às autoridades designadas para auditoria.

Art. 4º Os provedores de conexão e de aplicações de internet deverão implementar, no prazo de 60 (sessenta) dias contados da entrada em vigor desta Lei, canais técnicos e seguros para o atendimento de pedidos emergenciais previstos no art. 19-A, observando as seguintes obrigações mínimas:

- I. disponibilizar mecanismo eletrônico seguro para recebimento de requisições fundamentadas e autorização escrita da autoridade policial, com confirmação imediata de recebimento;
- II. manter registro eletrônico auditável de todas as comunicações com as autoridades, incluindo data, hora, identificação do pedido, elementos técnicos fornecidos e identificação do operador responsável;
- III. preservar logs e elementos técnicos fornecidos pelo prazo mínimo de 90 (noventa) dias, ressalvadas hipóteses de destruição ou retenção diversa determinada por decisão judicial;



IV. promover a adoção de medidas técnicas e administrativas de segurança da informação, incluindo criptografia e controles de acesso, para armazenamento e transmissão dos dados acarretados pela medida emergencial;

V. recusar solicitações que não atendam aos requisitos formais previstos nesta Lei e comunicar, de forma imediata e eletrônica, o motivo da recusa à autoridade requerente e ao Ministério Público.

Art. 5º A autoridade administrativa competente para a aplicação de sanções por violação das disposições relativas ao acesso emergencial será a prevista em lei para a tutela dos direitos e garantias relativas à proteção de dados pessoais e ao sigilo das comunicações, sem prejuízo da competência de outros órgãos reguladores e autoridades administrativas. São passíveis de aplicação sanções administrativas, entre outras, as previstas em legislação específica, além da responsabilidade civil e penal cabível.

Parágrafo único. A fiscalização do cumprimento das obrigações previstas nesta Lei poderá ser exercida pela Autoridade Nacional de Proteção de Dados, pelo Ministério Público e por demais órgãos de controle, na esfera de suas competências legais.

Art. 6º O Poder Executivo, em conjunto com o Ministério Público da União, os tribunais competentes e demais órgãos afetos à matéria, deverá editar ato normativo e protocolos técnicos no prazo máximo de 120 (cento e vinte) dias, contados da data de publicação desta Lei, para detalhar:

I. mecanismos técnicos de acesso e formatos padronizados de requisição, resposta e registro eletrônico;

II. formatos de registro, modelos de logs e critérios de guarda e eliminação segura de dados;

III. critérios e procedimentos para auditoria externa e mecanismos de cooperação com órgãos de controle; e

IV. demais regras operacionais necessárias à efetivação e controle das hipóteses previstas no art. 19-A.



Parágrafo único. O Conselho Nacional de Justiça e o Conselho Nacional do Ministério Público deverão promover diretrizes e práticas para apreciação prioritária e célere dos pedidos de homologação judicial previstos no § 3º do art. 19-A, sem prejuízo da independência e do exame judicial previsto na legislação processual aplicável.

Art. 7º Princípios orientadores da aplicação das disposições introduzidas por esta Lei são: legalidade, necessidade, proporcionalidade, finalidade, transparência, minimização de dados, presunção de inviolabilidade do sigilo das comunicações, publicidade agregada dos atos de exceção para fins de controle e responsabilização, e garantia do devido processo legal.

Art. 8º Revoga-se, naquilo que lhes for incompatível, as disposições em contrário.

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



## JUSTIFICAÇÃO

Possibilidade de iniciativa parlamentar: Sim. A matéria disciplina matéria administrativa e de proteção de direitos fundamentais no âmbito da legislação federal sobre a internet, sendo adequada a apresentação por Deputado Federal na forma de Projeto de Lei Ordinária.

A norma proposta responde à necessidade de conciliar duas exigências constitucionais convergentes: proteção da vida e segurança pública, por um lado, e tutela da privacidade, intimidade e do sigilo das comunicações, por outro. O Marco Civil consagra princípios de inviolabilidade e proteção de dados e somente excepcionalidades justificadas e estritamente delimitadas podem autorizar interferências. Em respeito à jurisprudência do Supremo Tribunal Federal que tem reforçado o controle judicial e a fundamentação das medidas invasivas, a proposta limita a exceção a hipóteses de risco iminente e grave, condiciona o acesso imediato à autorização motivada de autoridade policial de alto escalão e exige comunicação ao Ministério Público, com homologação judicial obrigatória em 48 horas. Ademais, veda expressamente acesso ao conteúdo das comunicações, impõe exigências de proporcionalidade e minimização, estabelece prazos de retenção e mecanismos de registro e auditoria externa e prevê sanções administrativas e criminais para abuso, de modo a oferecer segurança jurídica, mecanismo de fiscalização e prevenção de arbitrariedades, sem prejuízo da eficácia na resposta a situações de perigo iminente.

Sala das Sessões, de fevereiro de 2026.

**RUBENS PEREIRA JÚNIOR**



Deputado Federal

Apresentação: 30/03/2026 14:29:33.857 - Mesa

PL n.1480/2026



Para verificar a assinatura, acesse <https://infoleg-autenticidade-assinatura.camara.leg.br/CD268693327400>  
Assinado eletronicamente pelo(a) Dep. Rubens Pereira Júnior

