



CÂMARA DOS DEPUTADOS

PROJETO DE LEI N.º 5.226, DE 2025

(Do Sr. Pastor Henrique Vieira)

Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), para vedar a comercialização e o compartilhamento indevido de dados sensíveis, disciplinar o uso de biometria e o acesso a dados pessoais em processos judiciais, e dá outras providências.

DESPACHO:

À COMISSÃO DE CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA
(MÉRITO E ART. 54, RICD)

APRECIÇÃO:

Proposição Sujeita à Apreciação Conclusiva pelas Comissões - Art. 24 II

PUBLICAÇÃO INICIAL

Art. 137, caput - RICD

PROJETO DE LEI Nº , DE 2025

(Do Sr. PASTOR HENRIQUE VIEIRA)

Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), para vedar a comercialização e o compartilhamento indevido de dados sensíveis, disciplinar o uso de biometria e o acesso a dados pessoais em processos judiciais, e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta Lei altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), para vedar a comercialização e o compartilhamento indevido de dados sensíveis, disciplinar o uso de biometria e o acesso a dados pessoais em processos judiciais, e dá outras providências.

Art. 2º A Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar acrescida com as seguintes alterações:

“Art. 11.

.....

§ 6º É vedada a divulgação, o compartilhamento, a cessão ou a comercialização de dados pessoais sensíveis exceto nas hipóteses dispostas neste artigo.

.....

Art. 11-A O tratamento de dados biométricos não poderá ser exigido para a finalidade de controle de acesso em áreas ou propriedades privadas, salvo se observadas, cumulativamente, as seguintes condições:



I - houver fundamento legal específico e finalidade legítima de segurança, observados os princípios da necessidade e proporcionalidade;

II - o controlador elaborar Relatório de Impacto à Proteção de Dados Pessoais (RIPD); e

III - o titular for informado de forma clara e acessível sobre a finalidade, o prazo de guarda e os direitos relativos ao uso de seus dados biométricos.

Art. 11-B. O acesso a documentos de processos judiciais eletrônicos que contenham dados pessoais sensíveis será restrito, devendo ocorrer apenas:

I - mediante solicitação formal e justificada ao Poder Judiciário;

II - quando houver mandado judicial ou autorização legal expressa; ou

III - em casos de pesquisa, jornalismo ou interesse público relevante, observadas medidas de anonimização e sigilo.

§ 1º A publicidade dos atos processuais será compatibilizada com os direitos fundamentais à privacidade e à proteção de dados pessoais.

§ 2º O Conselho Nacional de Justiça editará normas complementares para disciplinar o acesso restrito e a anonimização de dados em sistemas judiciais.

.....
Art. 55-J

XXV – coordenar, com o Ministério Público, a Polícia Federal e os órgãos de defesa do consumidor, ações de prevenção e repressão ao comércio ilícito de dados pessoais.

Art. 3º Esta lei entra em vigor na data da sua publicação.



JUSTIFICAÇÃO

Atualmente, milhões de brasileiros encontram-se expostos em um ambiente digital onde informações pessoais e corporativas circulam sem controle. Plataformas que alegam atuar em nome da “transparência” ou da “análise de crédito” comercializam dados sensíveis — como nome completo, CPF, endereço, telefone, CNPJ e histórico judicial — sem o consentimento do titular e sem base legal legítima.

Essas práticas violam os princípios da Lei Geral de Proteção de Dados (LGPD) e fragilizam a confiança no ambiente digital, transformando o país em terreno fértil para fraudes, extorsões e roubos de identidade.

O problema tem origem em bases de dados públicas mal geridas e em sites que exploram brechas legais para monetizar informações pessoais e empresariais. A exigência de CPF e reconhecimento facial para o acesso a prédios comerciais e residenciais agrava ainda mais a situação, criando bancos de dados biométricos privados sem supervisão ou auditoria que representam uma vulnerabilidade crítica de segurança.

Reportagens da Deutsche Welle Brasil¹ e do UOL² (2025) alertam para a banalização da biometria facial no país e seus riscos para a privacidade, em contraste com países desenvolvidos, onde a coleta desse tipo de dado é rigidamente controlada e submetida a avaliações de impacto de proteção de dados (Data Protection Impact Assessments).

De acordo com o relatório da DLA Piper Data Protection Laws of the World³ (2024), a Alemanha mantém um dos modelos mais avançados de proteção de dados, impondo restrições severas ao tratamento de informações biométricas e à transferência de dados sem base legal clara.

¹ DEUTSCHE WELLE. Banalização da biometria no Brasil aumenta risco de fraudes. Band, 21 maio 2025. Disponível em: <https://www.band.com.br/noticias/banalizacao-da-biometria-no-brasil-aumenta-risco-de-fraudes-202505211600>. Acesso em: 8 out. 2025.

² UOL. UOL Prime #70: Reconhecimento facial é seguro? (Podcast). 2025. Disponível em: <https://podcasts.apple.com/de/podcast/uol-prime-70-reconhecimento-facial-%C3%A9-seguro/id1574996957?i=1000708556364>. Acesso em: 8 out. 2025.

³ DLA PIPER. Data Protection Laws of the World: Germany. 2025 Edition (referencing 2024 framework). Disponível em: <https://www.dlapiperdataprotection.com/guide.pdf?c=DE>. Acesso em: 8 out. 2025.



Enquanto o GDPR estabelece consentimento explícito, minimização e proporcionalidade como princípios obrigatórios, o Brasil ainda enfrenta normalização de práticas de vigilância e coleta excessiva de dados em nome da segurança ou da transparência.

Essa disparidade expõe a população brasileira a riscos cibernéticos crescentes, que se agravam com o uso indevido de inteligência artificial para criação de fraudes personalizadas, deepfakes e golpes digitais em massa.

Ademais, formou-se no Brasil um mercado subterrâneo de dados, que abastece a indústria de golpes e fraudes. Essas plataformas atuam como verdadeiros *data brokers*, vendendo informações sigilosas que deveriam estar protegidas. Cada vazamento de dados se transforma em matéria-prima para crimes digitais, com impactos econômicos e emocionais graves para cidadãos e empresas.

Para endereçar esses problemas, o projeto de lei propõe alterações na Lei Geral de Proteção de Dados (LGPD) para:

- Proibir a divulgação, o compartilhamento e a comercialização de dados pessoais sensíveis por qualquer meio eletrônico sem consentimento ou base legal inequívoca;
- Vedar a exigência de reconhecimento facial para acesso a ambientes privados, prevenindo o avanço da vigilância biométrica;
- Restringir o acesso público a processos e documentos judiciais que contenham dados pessoais sensíveis, assegurando que a publicidade processual seja compatível com o direito à privacidade;
- Regular o chamado “mercado da transparência”, responsabilizando sites e plataformas que vendem dados sob justificativas falsas.



O objetivo central é restaurar a segurança e a privacidade dos cidadãos e do ambiente de negócios, encerrando o ciclo de exposição de dados que alimenta o crime digital no Brasil.

A medida busca alinhar o país aos padrões internacionais de proteção de dados e reafirmar o direito fundamental à privacidade, reconhecido pelo Supremo Tribunal Federal como autônomo e essencial à dignidade da pessoa humana.

Sala das Sessões, em de de 2025.

Deputado PASTOR HENRIQUE VIEIRA





CÂMARA DOS DEPUTADOS

CENTRO DE DOCUMENTAÇÃO E INFORMAÇÃO – CEDI
Coordenação de Organização da Informação Legislativa – CELEG

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

<https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto2018-787077-norma-pl.html>

FIM DO DOCUMENTO