

PROJETO DE LEI Nº _____, DE 2026.
(Do Sr. Rubens Pereira Júnior)

Institui normas de responsabilidade, transparência e auditabilidade para sistemas de inteligência artificial de alto impacto e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta Lei institui normas de responsabilidade, transparência e auditabilidade aplicáveis a sistemas de inteligência artificial de alto impacto e dá outras providências.

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

I - sistema de inteligência artificial (sistema de IA): conjunto de componentes computacionais, modelos, algoritmos, fluxos de processamento e procedimentos capazes de executar tarefas que envolvam percepção, raciocínio, decisão, classificação, predição ou geração de conteúdo, por meio de processos de aprendizagem, inferência ou regras programadas;

II - sistema de alto impacto: sistema de IA cuja utilização possa afetar direitos fundamentais, decisões administrativas, acesso a crédito, emprego, benefícios públicos, segurança pública, saúde, educação, processos judiciais, ou que possua potencial de discriminar grupos protegidos;

III - fornecedor: pessoa natural ou jurídica, pública ou privada, que desenvolve, configura, disponibiliza, comercializa ou licencia sistemas de IA;

IV - operador: pessoa natural ou jurídica responsável pela operação, parametrização, manutenção ou decisão de uso de sistema de IA em contexto aplicativo específico;



V - titular: pessoa natural ou jurídica que detém a titularidade do sistema de IA ou a quem compete a tomada de decisão estratégica sobre sua finalidade e aplicação;

VI - responsável técnico: pessoa natural indicada pelo titular ou operador, com qualificação técnica e responsabilidades regulamentadas, incumbida da supervisão técnica, validação, monitoramento e resposta a incidentes do sistema de IA;

VII - logging imutável (audit trail imutável): registro cronológico e íntegro, com garantia de autenticidade e imutabilidade, de eventos, entradas, parâmetros, versões, decisões automatizadas e decisões humanas correlatas, formalmente observável e verificável por meios técnicos e processuais;

VIII - explicação adequada: informação sobre a lógica essencial do sistema de IA, os principais fatores e critérios que influenciaram decisão individualizada, nível de confiança, e as condições sob as quais a decisão foi produzida, disponibilizada em linguagem acessível ao destinatário;

IX - humans-in-the-loop: mecanismo de intervenção humana qualificada para validação, revisão ou aprovação de decisões automatizadas que impliquem restrição de direitos ou efeitos significativos sobre pessoas;

X - auditor independente: pessoa jurídica de direito público ou privado, ou pessoa física quando competente, acreditada por organismo acreditador reconhecido, com autonomia técnica, idoneidade e competência para realizar auditorias de conformidade, segurança, integridade e ausência de vieses em sistemas de IA;

XI - versão do modelo e hash: identificação inequívoca do artefato de modelo de IA por meio de versão controlada e soma de verificação criptográfica (hash) que permita rastreabilidade de alterações.

Art. 3º São princípios aplicáveis à elaboração, desenvolvimento, implementação e operação de sistemas de IA:

I - responsabilização: atribuição clara de deveres, responsabilidades e meios de reparação quanto aos efeitos dos sistemas de IA;

II - proporcionalidade e minimização de risco: adoção de medidas proporcionais ao risco e de mitigação e minimização dos impactos adversos;



III - não discriminação e equidade: prevenção, identificação e mitigação de vieses e impactos distributivos discriminatórios;

IV - transparência e explicabilidade: disponibilização de informações adequadas sobre finalidade, funcionamento e efeitos dos sistemas de IA;

V - auditabilidade: manutenção de registros e documentação que permitam auditoria técnica, jurídica e social;

VI - integridade e segurança: implementação de medidas técnicas e organizacionais para preservar a integridade, disponibilidade e confidencialidade dos sistemas e logs;

VII - devido processo e boa-fé: respeito às garantias processuais, ao direito de defesa e à cooperação com autoridades reguladoras;

VIII - inovação responsável: estímulo à pesquisa e ao desenvolvimento responsável, sem prejuízo de salvaguardas mínimas de segurança e direitos.

Art. 4º Considera-se como critério objetivo para classificação de sistema de alto impacto qualquer sistema de IA que, isolada ou cumulativamente:

I - decida, automatize ou influencie decisões que impliquem ou possam implicar:

- a) restrição ou supressão de direitos civis ou políticos;
- b) negativa de acesso a serviços públicos ou benefícios assistenciais;
- c) concessão, recusa ou alteração de acesso a crédito ou seguros;
- d) contratação, demissão, promoção ou avaliação disciplinar de empregados;
- e) imposição de medidas de segurança, vigilância, liberdade condicional ou sanções administrativas ou penais;

f) produção de elementos utilizados em atos processuais ou decisões judiciais automatizadas;

II - possua capacidade objetiva de segmentar ou discriminar grupos protegidos em razão de raça, cor, etnia, religião, sexo, orientação sexual, deficiência, idade, nacionalidade, condição socioeconômica ou outros critérios protegidos por lei;

III - apresente potencial de causar impactos significativos sobre saúde, segurança pública, educação ou direitos fundamentais em escala coletiva ou individual.



Art. 5º É obrigatória a inscrição prévia, em cadastro público mantido pela Autoridade Nacional de Proteção de Dados (ANPD) ou por órgão regulador setorial designado pela ANPD, de todo sistema de IA classificado como de alto impacto, antes de seu uso em território nacional ou antes de sua utilização para fins que afetem pessoas no Brasil.

§1º O registro deverá conter, no mínimo:

I - identificação do titular, do fornecedor, do operador e do responsável técnico, com respectivos contatos;

II - finalidade e escopo de aplicação do sistema, incluindo descrição dos processos decisórios automatizados;

III - classificação de risco, justificando a qual critério do art. 4º corresponde;

IV - identificação da versão do modelo e do hash correspondente;

V - metadados sobre conjuntos de dados utilizados para treino, validação e teste (descrição, origem, período de coleta, tratamento realizado, indicadores de representatividade), sem prejuízo de proteção de dados pessoais e segredo industrial;

VI - política de governança do sistema, incluindo governança de dados, avaliação e mitigação de vieses, procedimentos de resposta a incidentes e plano de monitoramento contínuo;

VII - cópia da Avaliação de Impacto sócio jurídico nos termos do art. 6º e indicação de medidas mitigadoras adotadas;

VIII - procedimentos e canais de atendimento para comunicação de eventos adversos, contatos para reclamação e procedimento para contestação;

IX - documentação de conformidade técnica e de segurança, e evidências de auditorias já realizadas, quando houver;

X - informação sobre utilização de terceiros, subcontratação ou modelos pré-treinados de terceiros.

§2º O cadastro será público, observadas as disposições desta Lei sobre proteção de dados pessoais e segredo industrial, e deverá permitir consulta por cidadãos, pesquisadores, autoridade pública e auditores acreditados.

§3º A inscrição será atualizada sempre que houver alteração material nas informações declaradas, inclusive em caso de mudança de versão do modelo, alteração da finalidade ou modificação em medidas mitigadoras, devendo tais atualizações constar em até 30 (trinta) dias da alteração.



Art. 6º É obrigatória a realização prévia e pública de Avaliação de Impacto Sócio Jurídico (AISJ) para todos os sistemas de alto impacto, antes de seu registro.

§ 1º A AISJ deverá incluir, no mínimo:

I - análise dos riscos a direitos fundamentais e liberdades públicas decorrentes do uso do sistema;

II - identificação e avaliação de vieses e potenciais efeitos discriminatórios, com metodologia explícita para detecção e mitigação;

III - avaliação de impactos distributivos e de equidade entre grupos populacionais;

IV - análise de custos e benefícios, incluindo estimativas de danos potenciais e medidas de mitigação e compensação;

V - plano de monitoramento e indicadores de desempenho, segurança e equidade a serem acompanhados periodicamente;

VI - medidas técnicas e organizacionais previstas para mitigação de riscos, inclusive testes de robustez, adversarialidade e privacidade;

VII - avaliação dos meios de contestação e revisão humana previstos;

VIII - avaliação da necessidade e da forma de registro de metadados e logs;

IX - sumário executivo em linguagem acessível destinado à consulta pública.

§ 2º A AISJ completa deverá ser disponibilizada no registro público e uma versão resumida em linguagem acessível deverá ser sujeita a consulta pública por, no mínimo, 30 (trinta) dias, observadas restrições legítimas de segredo industrial e proteção de dados pessoais.

§3º A avaliação deverá ser atualizada sempre que ocorrerem mudanças materiais no sistema ou quando novas evidências técnicas indicarem a necessidade de revisão.

Art. 7º Obrigam-se titulares e operadores de sistemas de alto impacto a manter logging imutável que registre, com integridade verificável:

I - identificação da versão do modelo e hash;

II - parâmetros, pesos ou configurações relevantes aplicados em cada execução;

III - metadados dos dados de entrada usados em cada decisão, logs de pré-processamento e transformações aplicadas;



IV - timestamp criptográfico (carimbo temporal) e provas de integridade;
V - resultado da inferência e justificativa automática gerada pelo sistema;
VI - decisão humana correlata, quando houver, incluindo identificação do responsável e justificativa para manutenção, modificação ou rejeição da decisão automatizada;

VII - alertas, incidentes e ações corretivas.

§1º Os registros referidos deverão ser preservados em formato que garanta integridade e imutabilidade por prazo mínimo de 5 (cinco) anos, contado da data de geração, salvo disposição legal diversa ou determinação judicial, observadas as proteções necessárias aos dados pessoais e ao segredo industrial.

§2º O acesso aos logs por autoridades, auditores credenciados e titulares de dados observará requisitos de confidencialidade, necessidade, proporcionalidade, bem como medidas técnicas de anonimização ou pseudonimização quando cabíveis e garantias processuais para preservação de segredo industrial.

Art. 8º A pessoa natural ou jurídica afetada por decisão automatizada proferida por sistema de IA de alto impacto terá direito a:

I - explicação adequada e compreensível da lógica essencial do sistema, dos principais fatores e critérios que conduziram à decisão e do nível de confiança associado;

II - orientação sobre as medidas possíveis para contestar a decisão, incluindo o canal de reclamação e os prazos aplicáveis;

III - acesso, em linguagem acessível, ao resumo dos dados pessoais utilizados, às fontes e à metodologia de avaliação, observado o disposto no art. 13 sobre proteção de segredo industrial e dados pessoais.

§1º O titular ou operador deverá disponibilizar meios efetivos de contestação e de revisão humana das decisões em prazo razoável, que, salvo justificativa fundamentada, não poderá exceder 30 (trinta) dias úteis contados do registro formal da contestação.

§2º No caso de decisão que determine restrição de direitos ou prejuízo significativo, a contestação deverá ensejar suspensão dos efeitos da decisão até que haja revisão humana motivada, quando requerido pelo interessado, salvo risco comprovado e justificado de dano iminente que exija manutenção imediata da



medida, hipótese em que o titular/operador deverá adotar medidas compensatórias e de minimização do dano.

Art. 9º É exigida aprovação humana qualificada (humans-in-the-loop) em todas as decisões derivadas de sistemas de IA de alto impacto que impliquem:

- I - negativa ou suspensão de benefício público;
- II - demissão ou alteração substancial de relação de trabalho;
- III - bloqueio ou suspensão de contas de usuário que causem prejuízo relevante;
- IV - imposição de medidas de segurança ou sanções administrativas;
- V - decisões que tenham efeitos determinantes em processos judiciais ou administrativos vinculantes.

§1º Excepcionalmente, regimes experimentais e controlados poderão ser autorizados por autoridade competente mediante requerimento específico, com licenciamento condicionado, observância de salvaguardas adicionais, supervisão contínua e prazo máximo de vigência, nos termos regulamentares.

§2º A aprovação humana deverá ser exercida por pessoa identificada, qualificada e vinculada a procedimentos de governança e registro auditável, devendo constar nos logs a justificativa para concordância ou discordância com a decisão automatizada.

Art. 10 São atribuídos ao titular e ao operador do sistema, solidária ou separadamente conforme o caso, os deveres de:

- I - diligência na concepção, validação, testes, implantação e monitoramento do sistema;
- II - implementação de políticas, procedimentos e controles para mitigação de riscos e remoção de vieses;
- III - manutenção de documentação técnica, registros de auditoria e relatórios de conformidade;
- IV - comunicação imediata à ANPD e às autoridades competentes de incidentes graves que representem risco a direitos fundamentais ou à segurança pública, bem como adoção de medidas corretivas imediatas;
- V - garantia de mecanismos de atendimento a solicitações de explicação e contestação;



VI - manutenção de plano de continuidade e de recuperação de desastres.

§ 1º É obrigatória a designação de responsável técnico pelo titular/operador, cujas qualificações mínimas e campo de atuação serão definidos em regulamento, com responsabilidades expressas de supervisão, validação de modelos e coordenação de auditorias e respostas a incidentes.

§ 2º O não cumprimento dos deveres previstos neste artigo sujeitará os responsáveis às sanções administrativas, civis e criminais cabíveis.

Art. 11 Os sistemas de IA de alto impacto sofrerão auditorias independentes periódicas, com frequência proporcional ao risco, sendo recomendada, sem prejuízo de exigência regulamentar, frequência mínima anual para sistemas de alto impacto.

§1º As auditorias deverão ser realizadas por auditores independentes acreditados, observando critérios técnicos, de imparcialidade e confidencialidade definidos em regulamentação, e abranger:

I - avaliação de conformidade com a presente Lei e regulamentações setoriais;

II - análise de logs, modelos, documentação técnica, protocolos de testes e AISJ;

III - verificação de medidas de mitigação de riscos e de planos de monitoramento;

IV - testes de robustez, segurança, privacidade e ausência de vieses.

§2º Os relatórios de auditoria terão:

I - versão resumida e pública, de fácil compreensão, contendo conclusões e recomendações essenciais;

II - versão técnica detalhada, disponibilizada às autoridades competentes e a auditores credenciados, mediante procedimentos que preservem segredo industrial e dados pessoais.

§3º A acreditação de auditores será procedida por organismo acreditador designado em regulamentação, com critérios que assegurem independência, competência técnica e incompatibilidades.

Art. 12 O descumprimento das obrigações previstas nesta Lei sujeitará o infrator às seguintes sanções administrativas, aplicadas de forma proporcional e considerando a capacidade econômica do infrator:



- I - advertência;
- II - obrigação de adoção de medidas de mitigação e correção;
- III - imposição de auditoria especial e acompanhamento técnico;
- IV - multa administrativa graduada, nos termos regulamentares;
- V - suspensão temporária de operação do sistema;
- VI - publicação pública de conduta ou de medida corretiva;
- VII - outras previstas em regulamento.

§1º Em caso de risco iminente a direitos fundamentais, à segurança pública ou à ordem social, a autoridade competente poderá determinar, em caráter de urgência e por prazo determinado, medidas cautelares, inclusive:

- I - bloqueio temporário de acesso ao sistema;
- II - suspensão imediata do uso do modelo ou de versões específicas;
- III - remoção de modelos ou funcionalidades identificadas como danosas.

§2º A aplicação de medidas urgentes será motivada, comunicada ao titular e sujeita a revisão administrativa e judicial em prazo oportuno.

§3º A responsabilidade civil por danos causados pelo uso do sistema de IA observará as normas gerais de responsabilidade civil, podendo ser aplicada a responsabilização objetiva ou subjetiva conforme a natureza do dano e o dever de diligência do agente.

§4º Quando a conduta constituir crime previsto em lei penal, será promovida a responsabilidade criminal dos agentes envolvidos, sem prejuízo das sanções administrativas e civis.

Art. 13 A aplicação desta Lei será compatibilizada com a Lei nº 13.709, de 14 de agosto de 2018, assegurando que o tratamento de dados pessoais resulte de base legal adequada, observando princípios de minimização, finalidade, necessidade e segurança.

§1º O acesso a logs, modelos e documentação técnica por autoridades, auditores e terceiros deverá observar:

- I - estrita necessidade, proporcionalidade e previsão legal ou contratual;
- II - medidas de confidencialidade, incluindo acordos de não divulgação e acesso supervisionado;
- III - uso preferencial de dados pseudonimizados ou agregados quando possíveis;



IV - possibilidade de acesso judicial para levantamento de segredo industrial quando imprescindível para a proteção de direitos fundamentais, mediante garantias processuais.

§2º O disposto nesta Lei não poderá ser invocado para ocultar condutas ilícitas, fraudes ou violação de direitos fundamentais.

Art. 14 A ANPD e os órgãos setoriais competentes promoverão consultas públicas para:

I - estabelecer e atualizar critérios de classificação de risco e listas de sistemas de alto impacto;

II - definir requisitos técnicos mínimos para logging imutável, AISJ e acreditação de auditores;

III - priorizar setores e sistemas para fiscalização, auditoria e orientação técnica.

§ 1º Fica instituído canal público e eletrônico para denúncias e comunicações de incidentes relacionados a sistemas de IA, com mecanismo de resposta estatal e de encaminhamento para investigação e fiscalização.

§ 2º As consultas públicas deverão respeitar prazos mínimos e garantir ampla publicidade, participação de sociedade civil, academia, setor privado e órgãos públicos setoriais.

Art. 15º A ANPD é designada autoridade coordenadora para manutenção do registro nacional de sistemas de IA de alto impacto, para coordenação de auditorias e para supervisionar a observância das obrigações previstas nesta Lei, em articulação com órgãos setoriais.

§ 1º A ANPD atuará em coordenação técnica com:

I - Ministério da Justiça e Segurança Pública;

II - Banco Central do Brasil, no que tange a sistemas financeiros e de crédito;

III - Ministério da Saúde, no que tange a sistemas de saúde;

IV - Ministério da Educação, no que tange a sistemas educacionais;

V - demais órgãos e entidades setoriais competentes, segundo regulamentação.



§ 2º A ANPD poderá firmar convênios, acordos de cooperação técnica e compartilhamento de informações, observar restrições de sigilo legal e medidas de proteção previstas nesta Lei.

Art. 16 A Lei nº 13.709, de 14 de agosto de 2018 passa a vigorar com a seguinte redação:

"Art. 18-A. Para fins de decisões automatizadas de alto impacto, há o dever expresso de transparência e de explicação, na forma desta Lei específica, sendo a ANPD competente para cooperar na fiscalização, estabelecer critérios de acesso a informações protegidas e harmonizar bases legais aplicáveis, observadas garantias processuais e medidas de proteção do segredo industrial."

Art. 17 A Lei nº 12.965, de 23 de abril de 2014, passa a vigorar com a seguinte redação:

"Art. 10-A. Plataformas e provedores que utilizem sistemas automatizados de moderação, curadoria ou recomendação classificados como de alto impacto, e que afetem a pluralidade da informação, ficam obrigados a inscrever tais sistemas no registro público referido na Lei de Responsabilidade, Transparência e Auditabilidade de Sistemas de IA, e a publicar relatórios de transparência contendo métricas, descrições da finalidade e dos impactos, e informações sobre mecanismos de contestação, preservando segredo comercial nos limites estritamente necessários."

Art. 18 A Lei nº 8.078, de 11 de setembro de 1990, passa a vigorar com a seguinte redação:

"Art. 6º-A. Nas relações de consumo, o consumidor tem direito à informação adequada e à revisão humana em decisões automatizadas que afetem condições contratuais, negativa de crédito, recusa de contratação ou imposição de ônus, sendo possível a inversão do ônus da prova quando o fornecedor não apresentar documentação ou explicação suficiente acerca da decisão automatizada."



Art. 19 A Lei nº. 9.784, de 29 de janeiro de 1999, passa a vigorar com a seguinte redação:

"Art. 50-A. Quando órgãos e entidades públicas utilizarem sistemas automatizados em processos decisórios administrativos, serão obrigados a divulgar, na medida do possível e compatível com segurança e segredos legalmente protegidos, os modelos, parâmetros, logs relevantes e justificativas, assegurando o dever de motivação e a possibilidade de revisão administrativa por agente humano identificado."

Art. 20 O Poder Executivo regulamentará, no prazo de 180 (cento e oitenta) dias contados da publicação desta Lei, os requisitos técnicos e operacionais necessários ao seu cumprimento, inclusive:

- I - requisitos mínimos para logging imutável e carimbo temporal;
- II - critérios de acreditação de auditores independentes;
- III - modelo e conteúdo mínimo da Avaliação de Impacto Sociojurídico;
- IV - procedimentos para registros, atualizações, acesso e proteção de informações sensíveis;
- V - parâmetros para aplicação das sanções administrativas.

§1º Os titulares e operadores de sistemas de alto impacto em operação na data de publicação desta Lei deverão promover o registro e realizar a AISJ no prazo de 12 (doze) meses, contado da publicação.

§2º Sistemas de alto impacto novos, após a publicação desta Lei, somente poderão entrar em operação após o registro prévio e a apresentação da AISJ, observando prazo máximo de 6 (seis) meses para implementação dos requisitos, salvo autorização de regime experimental prevista no § 3º.

§3º Regimes experimentais e pilotos poderão ser autorizados pela ANPD ou por órgão setorial competente, mediante requerimento, observadas salvaguardas, supervisão e limitação temporal, e devendo constar em registro público identificador do regime.

Art. 21 Até a regulamentação indicada no anterior, a ANPD publicará orientações provisórias e guias técnicos de conformidade a serem considerados como referência obrigatória para fins de fiscalização.



Art. 22 Compete primariamente à ANPD a fiscalização do cumprimento das obrigações previstas nesta Lei, sem prejuízo da atuação concorrente de outros órgãos setoriais no âmbito de suas competências legais.

Parágrafo único. Na aplicação de sanções administrativas, serão observados o contraditório e a ampla defesa, o devido processo legal e os princípios da proporcionalidade e da razoabilidade.

Art. 23 As contratações públicas de sistemas de IA de alto impacto deverão exigir, no edital e no contrato, cumprimento das obrigações desta Lei, demonstração de AISJ, logging imutável e auditabilidade, bem como cláusulas de responsabilidade e de garantia de integridade e segurança.

§1º Recomenda-se que instituições financeiras, de saúde, educação e de assistência social incorporem em suas políticas internas os padrões de governança previstos nesta Lei.

§2º As disposições desta Lei não excluem ou reduzem obrigações previstas em legislação setorial específica que imponha requisitos mais gravosos ou detalhados.

Art. 24 Esta Lei entra em vigor na data de sua publicação, observado o disposto no art. 20 quanto ao prazo de regulamentação e aos prazos escalonados de conformidade.



JUSTIFICAÇÃO

A rápida difusão de sistemas de inteligência artificial coloca desafios centrais ao Estado de Direito: opacidade das decisões automatizadas, difusão de poder sem sujeito responsável, dificuldades de atribuição de causalidade e deficits de auditabilidade e contestabilidade.

A Lei proposta transforma em política pública os princípios básicos que permitem responsabilizar e controlar decisões automatizadas: identifica-se quando um sistema é de alto impacto, exige-se avaliação prévia de seus efeitos sócio jurídicos, impõe-se requisitos de registro e logging imutável, garante-se explicação adequada e direito de contestação, e estabelece-se obrigação de presença humana em decisões que afetem direitos.

A iniciativa complementa a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014) e as normas de defesa do consumidor, harmonizando proteção de direitos fundamentais, transparência regulatória e inovação responsável. Ao tornar auditáveis e atribuíveis os processos decisórios automatizados, a norma resguarda liberdade, dignidade e segurança jurídica, sem interditar tecnologias, mas condicionando sua operação a garantias democráticas e técnicas verificáveis.

Sala das Sessões, março de 2026.

RUBENS PEREIRA JÚNIOR

Deputado Federal

