CÂMARA DOS DEPUTADOS

PROJETO DE LEI N.º 4.356, DE 2025

(Do Sr. Romero Rodrigues)

Estabelece normas gerais programáticas, de aplicação em âmbito nacional, para a utilização de tecnologias baseadas em inteligência artificial no âmbito do Sistema Único de Segurança Pública – SUSP, visando à prevenção e à repressão de infrações penais, à proteção de pessoas e bens e à preservação da ordem pública, potencializando a observância dos direitos e garantias fundamentais.

DESPACHO:
ÀS COMISSÕES DE
CIÊNCIA, TECNOLOGIA E INOVAÇÃO;
SEGURANÇA PÚBLICA E COMBATE AO CRIME ORGANIZADO;
FINANÇAS E TRIBUTAÇÃO (MÉRITO E ART. 54, RICD) E
CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA (MÉRITO E ART. 54, RICD)

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

PUBLICAÇÃO INICIAL
Art. 137, caput - RICD

PROJETO DE LEI Nº , DE 2025

(Do Sr. ROMERO RODRIGUES)

Estabelece normas gerais programáticas, de aplicação em âmbito nacional, para a utilização de tecnologias baseadas em inteligência artificial no âmbito do Sistema Único de Segurança Pública – SUSP, visando à prevenção e à repressão de infrações penais, à proteção de pessoas e bens e à preservação da ordem pública, potencializando a observância dos direitos e garantias fundamentais.

O Congresso Nacional decreta:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Seção I
Objeto e Âmbito de Aplicação

Art. 1º Esta Lei estabelece normas gerais programáticas, de aplicação em âmbito nacional, para a utilização de tecnologias baseadas em inteligência artificial (IA) no âmbito do Sistema Único de Segurança Pública – SUSP, visando à prevenção e à repressão de infrações penais, à proteção de pessoas e bens e à preservação da ordem pública, potencializando a observância dos direitos e garantias fundamentais.

§ 1º O cumprimento das disposições desta Lei, de caráter programático, constituirá requisito para o acesso, por qualquer órgão de segurança pública, a recursos do Fundo Nacional de Segurança Pública – FNSP.

§ 2º A aplicação desta Lei observará, de forma complementar, a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e demais normas pertinentes.

Seção II – Definições

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

I – reconhecimento facial: tecnologia capaz de identificar ou verificar a identidade de pessoas por meio de análise de características faciais, em tempo real ou em registros;

II – reconhecimento de padrões biométricos: tecnologias de identificação baseadas em impressões digitais, voz, íris, retina, geometria da mão, marcha ou outros atributos físicos ou comportamentais;

III – câmeras inteligentes: sistemas de videomonitoramento com processamento de imagens capaz de detectar, rastrear e classificar objetos, pessoas ou eventos, incluindo análise comportamental automatizada;

IV – sistemas de análise preditiva: modelos de inteligência artificial que estimam probabilidades de ocorrência de eventos criminais ou identificam áreas ou alvos de risco com base em dados históricos e correlatos;

V – drones e veículos aéreos não tripulados com funções autônomas: equipamentos capazes de operar com navegação, vigilância ou monitoramento assistidos ou controlados por IA, sem intervenção humana contínua;

VI – robôs terrestres ou aquáticos com funções autônomas: plataformas móveis capazes de realizar patrulhamento, inspeção ou outras atividades de segurança de forma autônoma ou semiautônoma;

VII – sistemas de triagem automatizada de comunicações e dados: ferramentas de IA para análise de conteúdos de áudio, vídeo, texto ou metadados, visando identificar padrões ou indícios de ilícitos;

VIII – ferramentas de análise de “big data” e mineração de dados: sistemas capazes de processar grandes volumes de dados estruturados e não estruturados para fins de investigação ou inteligência de segurança pública;

IX – geradores de conteúdo sintético e “deepfakes”: sistemas que criam, modificam ou manipulam conteúdos audiovisuais com técnicas de

IA, capazes de produzir representações realistas de eventos, pessoas ou objetos inexistentes ou alterados;

X – modelos de linguagem e processamento de linguagem natural (PLN): sistemas que compreendem, interpretam, geram ou traduzem textos ou comunicações, utilizados para fins de investigação ou análise de ameaças;

XI – sistemas de detecção e neutralização de ameaças cibernéticas baseados em IA: tecnologias voltadas à identificação e resposta automatizada a incidentes de segurança da informação;

XII – outras tecnologias correlatas de inteligência artificial: qualquer sistema, método ou aplicação que, por meio de modelos computacionais de aprendizado, inferência ou decisão autônoma ou semiautônoma, possa impactar atividades de segurança pública.

Parágrafo único. A lista prevista neste artigo poderá ser atualizada por decreto regulamentador, para inclusão de novas tecnologias, respeitado o disposto nesta Lei.

CAPÍTULO II
REQUISITOS E PADRÕES TÉCNICOS

Seção I
Limiar de Performance

Art. 3º As tecnologias de inteligência artificial utilizadas no seio da segurança pública deverão manter desempenho mínimo comprovado por meio de métricas padronizadas, aferidas por auditoria independente.

§ 1º O limiar mínimo de acurácia não poderá ser inferior a 95% (noventa e cinco por cento) para reconhecimento facial e biométrico, nem inferior a 90% (noventa por cento) para demais tecnologias previstas no art. 2º, salvo hipóteses técnicas justificadas e previamente autorizadas pelo órgão competente da União.

§ 2º A taxa de falso positivo e de falso negativo deverá manter paridade de desempenho entre diferentes grupos étnicos, de gênero, faixa

etária ou outros critérios protegidos, não sendo admitida discrepância superior a 5% (cinco por cento) entre qualquer desses grupos.

§ 3º O descumprimento dos limiares definidos nos §§ 1º e 2º implicará suspensão imediata do uso da tecnologia até sua adequação, sob pena de responsabilização administrativa, civil e penal.

Seção II

Auditoria e Mitigação de Viés

Art. 4º As tecnologias de inteligência artificial previstas nesta Lei deverão ser submetidas, no mínimo uma vez por ano, a auditorias técnicas independentes que avaliem:

I – desempenho geral e por subgrupos populacionais;

II – taxas de erro e vieses identificáveis;

III – robustez contra tentativas de manipulação, como “deepfakes”, “spoofing” e “adversarial attacks”;

IV – conformidade com as finalidades autorizadas e restrições previstas nesta Lei.

§ 1º As auditorias deverão gerar relatórios públicos resumidos, garantindo transparência sem comprometer informações sigilosas de segurança ou investigação.

§ 2º Havendo detecção de viés discriminatório ou degradação relevante de desempenho, o órgão responsável deverá apresentar, no prazo máximo de 90 (noventa) dias, plano de mitigação com medidas corretivas e cronograma de implementação.

§ 3º Enquanto não implementadas as medidas corretivas, poderá ser determinada a restrição ou suspensão parcial do uso da tecnologia, conforme a gravidade do problema.

CAPÍTULO III

FINALIDADES E VEDAÇÕES

Seção I

Hipóteses Legítimas de Uso

Art. 5º As tecnologias de inteligência artificial previstas nesta Lei somente poderão ser utilizadas para as seguintes finalidades:

I – prevenção, investigação e repressão de infrações penais;

II – localização de pessoas desaparecidas ou procuradas pela Justiça;

III – proteção de eventos, instalações e áreas de interesse estratégico para a segurança pública;

IV – prevenção e resposta a situações de risco coletivo, como desastres, incidentes de grande porte e emergências;

V – apoio a operações de busca e salvamento;

VI – proteção de vítimas de violência doméstica, familiar ou outras situações de risco grave, mediante ordem judicial ou autorização legal;

VII – segurança de fronteiras, portos, aeroportos e áreas de controle alfandegário;

VIII – prevenção e repressão de crimes cibernéticos e fraudes eletrônicas;

IX – apoio a operações de inteligência de segurança pública, nos termos da legislação específica.

Parágrafo único. O uso de tecnologias de inteligência artificial em segurança pública deverá sempre estar vinculado a procedimento formalmente autorizado e documentado, com registro de finalidades, bases legais e responsáveis pela operação.

Seção II

Usos Vedados e Restrições Absolutas

Art. 6º É vedada a utilização das tecnologias de que trata esta Lei para:

I – vigilância em massa não vinculada a investigação ou ação específica, sem base legal ou ordem judicial;

II – monitoramento contínuo e indiscriminado de pessoas ou grupos por critérios de opinião política, religião, convicção filosófica ou orientação sexual;

III – coleta ou tratamento de dados sensíveis sem previsão legal expressa ou autorização judicial, ressalvadas as hipóteses previstas em lei;

IV – criação, uso ou disseminação de conteúdos sintéticos ou “deepfakes” com o intuito de difamar, intimidar, manipular processos democráticos ou enganar autoridades;

V – tomada de decisão automatizada sem revisão humana quando esta implicar restrição de direitos fundamentais, salvo autorização legal expressa;

VI – adoção de sistemas cuja arquitetura, funcionamento ou código-fonte sejam inacessíveis à auditoria técnica independente;

VII – compartilhamento de dados obtidos por IA com terceiros não autorizados ou para finalidades diversas daquelas expressamente previstas.

Parágrafo único. O descumprimento das disposições desta Seção acarretará nulidade das provas obtidas, responsabilização dos agentes envolvidos e aplicação das sanções cabíveis.

CAPÍTULO IV
REVISÃO HUMANA E RESPONSABILIZAÇÃO

Seção I
Revisão Humana Obrigatória

Art. 7º Qualquer decisão ou recomendação produzida por tecnologia de inteligência artificial que possa impactar direitos fundamentais deverá ser objeto de revisão e validação por agente público competente antes de gerar efeitos externos.

§ 1º A revisão humana deverá:

I – avaliar a pertinência e a confiabilidade do resultado;

II – verificar a conformidade com a finalidade autorizada e com os limites legais;

III – registrar, em sistema próprio, a análise realizada e a decisão final adotada.

§ 2º É vedada a execução automática de medidas restritivas de direitos, como prisões, apreensões ou bloqueios, sem intervenção humana qualificada, salvo hipóteses expressamente previstas em lei.

Seção II

Controle Interno e Externo

Art. 8º O uso das tecnologias previstas nesta Lei estará sujeito a:

I – controle interno, realizado por unidade especializada do próprio órgão, responsável por monitorar conformidade, desempenho e segurança das operações;

II – controle externo, realizado por órgãos de controle e fiscalização competentes, inclusive o Ministério Público e os Tribunais de Contas, nos limites de suas atribuições;

III – supervisão técnica periódica, conforme disposto no art. 4º desta Lei.

Parágrafo único. Deverão ser mantidos registros auditáveis de todas as operações realizadas com tecnologias de inteligência artificial, preservando informações suficientes para reconstituir a decisão ou ação resultante de seu uso.

Seção III

Responsabilização

Art. 9º O agente público que, por ação ou omissão, der causa a uso indevido ou ilegal das tecnologias previstas nesta Lei responderá nas esferas administrativa, civil e penal, conforme o caso.

§ 1º O fornecedor ou desenvolvedor de tecnologia de inteligência artificial poderá ser responsabilizado solidariamente quando

comprovado que falhas técnicas ou de conformidade, de sua responsabilidade, contribuíram para o dano causado.

§ 2º A responsabilização prevista neste artigo não exclui a possibilidade de reparação de danos individuais ou coletivos, inclusive morais, decorrentes do uso indevido ou incorreto da tecnologia.

CAPÍTULO V
TRANSPARÊNCIA E PRESTAÇÃO DE CONTAS

Seção I
Publicidade e Acesso à Informação

Art. 10. Os órgãos de segurança pública que utilizarem tecnologias de inteligência artificial deverão disponibilizar, em portal eletrônico de acesso público:

I – descrição das tecnologias empregadas e suas finalidades;

II – políticas internas e protocolos de uso;

III – relatórios anuais de desempenho e de auditorias independentes, nos termos do art. 4º;

IV – informações agregadas sobre número de operações, acurácia, vieses detectados e medidas corretivas adotadas;

V – atos normativos internos que regulamentem o uso das tecnologias no órgão.

§ 1º A divulgação deverá preservar informações sigilosas cuja revelação possa comprometer a segurança pública, investigações ou direitos de terceiros.

§ 2º Os dados divulgados deverão estar em formato aberto e acessível, permitindo análise por órgãos de controle e pela sociedade civil.

Seção II
Prestação de Contas Periódica

Art. 11. A prestação de contas anual do uso da IA em atividades de segurança pública deverá conter:

I – inventário das tecnologias de inteligência artificial utilizadas;

II – dados consolidados de acurácia, taxas de erro e paridade de desempenho;

III – registro de incidentes relevantes e respectivas providências;

IV – resultados das auditorias internas e externas;

V – plano de ação para mitigação de riscos e aprimoramento da tecnologia.

Parágrafo único. O descumprimento reiterado das obrigações de transparência e prestação de contas poderá implicar suspensão do acesso a recursos do Fundo Nacional de Segurança Pública, nos termos da lei específica.

CAPÍTULO VI
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Seção I
Alterações Legislativas

Art. 12. A Lei nº 13.756, de 12 de dezembro de 2018, passa a vigorar acrescida do art. 8º-A, com a seguinte redação:

> **"Art. 8º-A.** O repasse de recursos do Fundo Nacional de Segurança Pública aos entes federativos e órgãos integrantes do Sistema Único de Segurança Pública – SUSP fica condicionado à comprovação de cumprimento integral das disposições da Lei que regulamenta, em âmbito nacional, o uso de tecnologias de inteligência artificial na segurança pública.
>
> Parágrafo único. O descumprimento das disposições mencionadas no caput implicará suspensão imediata de novos repasses, até a regularização da situação pelo ente ou órgão beneficiário". (NR).

Seção II
Regulamentação

Art. 13. Regulamento do Poder Executivo definirá, entre outros aspectos:

I – critérios técnicos complementares para aferição de desempenho e mitigação de viés;

II – procedimentos de auditoria e certificação de tecnologias;

III – mecanismos de controle e supervisão.

Seção III

Vigência

Art. 14. Esta Lei entra em vigor 180 (cento e oitenta) dias após a data de sua publicação.

JUSTIFICAÇÃO

O presente Projeto de Lei busca disciplinar, em âmbito nacional, a utilização de tecnologias de inteligência artificial (IA) no Sistema Único de Segurança Pública – SUSP, estabelecendo parâmetros técnicos, éticos e jurídicos que assegurem a eficiência operacional e, ao mesmo tempo, resguardem os direitos e garantias fundamentais previstos na Constituição Federal. A regulamentação se mostra urgente diante da rápida expansão de soluções tecnológicas de IA já empregadas em diversos países e em algumas localidades brasileiras, sem um marco legal unificado que defina padrões de desempenho, limites de uso e mecanismos de controle.

Em primeiro lugar, a proposta atende a uma demanda real do setor de segurança pública. Hoje, tecnologias como reconhecimento facial, drones, câmeras inteligentes, mineração de dados e sistemas de predição criminal já vêm sendo testadas e aplicadas por órgãos policiais. No entanto, a ausência de parâmetros claros compromete a eficácia, cria insegurança jurídica e aumenta o risco de violações a direitos individuais. Ao estabelecer normas gerais, o projeto proporciona um equilíbrio necessário entre inovação tecnológica e proteção da cidadania.

Outro ponto fundamental diz respeito ao desempenho técnico. Tecnologias de IA, se mal calibradas, podem gerar resultados incorretos, com alto índice de falsos positivos ou negativos, especialmente em populações minoritárias. O texto prevê limiares mínimos de acurácia, auditoria independente e mitigação de vieses, garantindo que o uso dessas ferramentas não reforce desigualdades estruturais ou discriminações, mas sim fortaleça a confiança pública no aparato estatal de segurança.

A proposta também define hipóteses legítimas de uso, como prevenção e repressão de crimes, localização de pessoas desaparecidas, proteção de vítimas e segurança de fronteiras. Ao mesmo tempo, estabelece vedações absolutas a práticas que configurariam vigilância massiva indiscriminada, perseguição por motivos políticos, manipulação de processos democráticos e uso de “deepfakes” para fins ilícitos. Essa dupla abordagem – permitir usos legítimos e proibir abusos – confere clareza e segurança aos órgãos de segurança e à sociedade.

Outro aspecto relevante é a previsão de revisão humana obrigatória em decisões que possam restringir direitos fundamentais. Esse dispositivo assegura que a tecnologia não substitua a autoridade e a responsabilidade do agente público, evitando que algoritmos determinem, de forma automática e sem supervisão, medidas que impactem diretamente a liberdade e a dignidade das pessoas. A IA, nesse sentido, é tratada como ferramenta de apoio e não como substituta do julgamento humano.

A responsabilização solidária de agentes públicos e desenvolvedores também é um ponto de destaque. O texto prevê que eventuais danos decorrentes do mau uso da tecnologia poderão gerar consequências nas esferas administrativa, civil e penal. Essa previsão é essencial para garantir responsabilidade compartilhada entre Estado e fornecedores, criando incentivos para o desenvolvimento ético e seguro das soluções tecnológicas.

A transparência é igualmente valorizada no projeto. A obrigatoriedade de divulgação de relatórios públicos, auditorias e protocolos de uso permite que a sociedade civil, a academia e órgãos de controle

acompanhem a aplicação das tecnologias, evitando seu uso em segredo e garantindo legitimidade democrática. Esse mecanismo de prestação de contas aumenta a confiança social e fortalece a legitimidade das políticas de segurança.

Por fim, ao vincular o cumprimento da lei ao acesso aos recursos do Fundo Nacional de Segurança Pública – FNSP, o projeto cria um incentivo concreto para que estados e municípios adotem as normas propostas. Essa condição garante homogeneidade na aplicação da legislação em todo o território nacional, evitando assimetrias e assegurando que a modernização tecnológica na segurança pública ocorra de forma uniforme, responsável e alinhada aos princípios constitucionais.

Dessa forma, o presente Projeto de Lei constitui um marco regulatório moderno, equilibrado e necessário para o Brasil. Ele permite que o país acompanhe as inovações tecnológicas internacionais, fortaleça a segurança pública, aumente a eficiência das forças de segurança e, ao mesmo tempo, preserve a democracia, a privacidade e os direitos fundamentais dos cidadãos. Trata-se de medida que conjuga segurança e liberdade, inovação e responsabilidade, tecnologia e cidadania.

Sala das Sessões, em de de 2025.

Deputado ROMERO RODRIGUES

2025-12540

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018	https://normas.leg.br/?urn=urn:lex:br:federal:lei:201808-14;13709
LEI Nº 13.756, DE 12 DE DEZEMBRO DE 2018	https://normas.leg.br/?urn=urn:lex:br:federal:lei:201812-12;13756

FIM DO DOCUMENTO