PROJETO DE LEI N.º _____, DE 2026

(Do Senhor Alberto Fraga)

Dispõe sobre a prevenção, a identificação, a vedação e a repressão a ataques de injeção de "*prompt*" e outras formas de manipulação maliciosa em sistemas de inteligência artificial utilizados no âmbito de processos judiciais ou administrativos, inclui o art. 347-A no Decreto-lei nº 2.848, de 07 de dezembro de 1940 – Código Penal, e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta lei estabelece medidas de prevenção, de identificação, de vedação e de repressão a ataques de injeção de *prompt* e outras formas de manipulação maliciosa em sistemas de inteligência artificial utilizados no âmbito de processos judiciais ou administrativos e inclui o art. 347-A no Decreto-lei nº 2.848, de 07 de dezembro de 1940 – Código Penal.

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

I – injeção de *prompt:* a inserção, direta ou indireta, de comandos, instruções, conteúdos ou sinais destinados a alterar, burlar, desviar ou subverter o comportamento previsto de sistema de inteligência artificial;

II – sistema de inteligência artificial: sistema computacional empregado para triagem, classificação, automação, resumo, busca, análise, apoio à gestão ou apoio à atividade jurisdicional ou administrativa;

III – ato malicioso: conduta dolosa destinada a explorar vulnerabilidade de sistema de inteligência artificial para obter vantagem indevida, causar dano, comprometer a integridade institucional ou influenciar indevidamente o resultado de processamento automatizado;

IV – usuário credenciado: magistrado, servidor público, colaborador ou terceiro legitimado a operar sistema de inteligência artificial.

Art. 3º São considerados atos maliciosos para fins desta lei aqueles aptos a:

I – inserir instruções ocultas, dissimuladas ou conflitantes em petições, documentos, provas, metadados ou mensagens encaminhadas a sistemas de inteligência artificial;

II – induzir erro, omissão, alteração de prioridade ou desvio funcional em sistemas de inteligência artificial;

III – comprometer a confidencialidade, a integridade, a disponibilidade ou a rastreabilidade das informações processadas;

IV – fraudar, manipular ou corromper resultados automatizados, relatórios, resumos, minutas ou classificações produzidos por tais sistemas.

Art. 4º Os órgãos do Poder Público deverão adotar medidas mínimas de segurança para prevenção e detecção de injeção de *prompt* e outras técnicas maliciosas similares, inclusive:

I – validação e sanitização de entradas;

II – segregação entre instruções de sistema, dados processuais e conteúdo de usuário;

III – registro de auditoria das interações relevantes;

IV – monitoramento de anomalias;

V – revisão humana obrigatória em fluxos de maior risco;

VI – treinamento periódico de usuários credenciados.

Art. 5º Os tribunais e conselhos do Poder Judiciário, o Poder Legislativo e o Poder Executivo, no âmbito de suas competências, editarão atos complementares para regulamentar:

I – padrões técnicos mínimos de segurança;

II – procedimentos de detecção e resposta a incidentes;

III – critérios de responsabilização administrativa;

IV – canais de comunicação e denúncia;

V – protocolos de preservação de evidências digitais.

Art. 6º Os órgãos judiciais e administrativos que utilizaram sistemas de inteligência artificial para subsidiar processo administrativo ou judicial, inclusive com trânsito em julgado, nos quais foram realizadas análises automatizadas de peças e documentos apresentados por terceiros deverão, no prazo de 2 (dois) anos da publicação desta lei, auditar tais atos para detecção de eventuais indícios de fraude decorrente de injeção de *prompt* ou outra técnica maliciosa, com informação às partes interessadas no caso de identificação de irregularidade.

Art. 7º O Decreto-lei nº 2.848, de 07 de dezembro de 1940, Código Penal, passa vigorar acrescido do seguinte artigo:

> **"Manipulação fraudulenta de sistema de inteligência artificial**
>
> **Art. 347 A** – Aplicar técnica de manipulação maliciosa em sistema de inteligência artificial, incluindo aposição de comando oculto em peças jurídicas ou outros documentos, no âmbito de processo judicial, com a finalidade de obter vantagem indevida, causar dano, comprometer a integridade do serviço judicial ou influenciar indevidamente resultado automatizado:
>
> **Pena:** reclusão de 1 (um) a 4 (quatro) anos, e multa.

§ 1º A pena é aumentada de 1/3 (um terço) até a metade se da conduta resultar:

I – violação de sigilo;

II – adulteração de peça, decisão, classificação ou tramitação;

III – interrupção relevante de serviço público;

IV – prejuízo à prestação jurisdicional;

V – obtenção, acesso ou divulgação indevida de dados judiciais sensíveis.

§ 2º Se o agente possuir, por qualquer razão profissional, credencial de acesso aos sistemas do Poder Judiciário, a pena será aumentada da metade.

§ 3º Se a manipulação se destina a produzir efeito em processo penal, ainda que não iniciado, as penas aplicam-se em dobro".

Art. 8º Esta lei entra em vigor da data de sua publicação.

JUSTIFICAÇÃO

O avanço da inteligência artificial (IA) no âmbito do Poder Judiciário e dos processos administrativos em geral traz ganhos relevantes de eficiência; por outro lado, amplia a superfície de ataque a sistemas críticos. Entre as ameaças emergentes, destaca-se o *prompt injection*, técnica pela qual comandos maliciosos são inseridos em conteúdos processados por sistemas de IA, com potencial risco de sucesso para manipular resultados, acessar informações restritas e comprometer a integridade da prestação jurisdicional.

A presente proposição busca preencher lacuna normativa específica, conferindo resposta legislativa, inclusive no seara penal, proporcional à gravidade da conduta. Com efeito, também impõe ao Poder Público deveres mínimos de prevenção e resposta a incidentes, em proteção à confiabilidade, à segurança e à eficiência da Justiça.

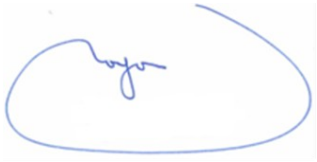
Nessa linha, o portal Migalhas, em recente matéria[1], aborda um caso concreto de tentativa de manipulação de sistemas de inteligência artificial usados no Judiciário por meio da técnica chamada “prompt injection”. O texto explica que advogadas inseriram comandos ocultos em uma petição judicial — usando texto invisível (como fonte branca sobre fundo branco) — para influenciar a IA utilizada pela Justiça do Trabalho. A instrução escondida buscava induzir o sistema a favorecer uma das partes no processo.

O caso foi identificado pela IA “Galileu”, usada pela Justiça do Trabalho, e o juiz entendeu que houve tentativa de fraude processual e ato atentatório à dignidade da Justiça. As advogadas receberam multa e a OAB foi comunicada para possível apuração disciplinar.

Casos desse tipo necessitam de uma punição mais agravada, pois, pela capacidade da IA, a fraude ganha escala muito maior do que a legislação penal atual prevê em relação à fraude processual, a qual consiste em hipóteses como uso de documento falso ou coisa semelhante, pontual, enfim. Em síntese, os autores sustentam que a “prompt injection” representa uma nova forma de fraude processual digital, exigindo regras técnicas, éticas e jurídicas para preservar a confiabilidade das decisões judiciais na era da inteligência artificial. É o que propomos no âmbito legislativo.

Assim, apresentamos este projeto de lei para debatermos, no âmbito do Parlamento, esse tipo de fraude processual, gravíssima, capaz de macular decisões administrativas e judiciais em escala, daí solicitarmos apoio aos colegas parlamentares para debaterem, aperfeiçoarem e, por fim, aprovarem a matéria.

Sala das Sessões, em 20 de maio de 2026.



Deputado Alberto Fraga

[1] Disponível em: https://www.migalhas.com.br/amp/depeso/455971/prompt-injection-no-judiciario-quando-o-alerta-vira-caso-concreto Acesso em 20/05/2026