Projeto de Lei Ordinária Nº , DE 2026.

(Do Sr. Rubens Pereira Júnior)

Estabelece normas mínimas de segurança, governança, rastreabilidade e responsabilização para o uso de sistemas de inteligência artificial em procedimentos judiciais eletrônicos; obriga higienização de entrada, encapsulamento e pré-filtragem de documentos, registro de logs de rastreabilidade, adoção de contratos de resposta e prompting por etapas, supervisão humana qualificada, diagnósticos de risco, auditorias periódicas e medidas de proteção contra envenenamento de bases; impõe obrigação de comunicação de suspeita de prompt injection ao juízo, ao Conselho Nacional de Justiça (CNJ) e às autoridades competentes; prevê sanções administrativas, civis e penais quando cabíveis; fixa prazo máximo de implementação e confere competência de fiscalização ao CNJ; e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta Lei estabelece normas mínimas de segurança, governança, rastreabilidade e responsabilização para o desenvolvimento, aquisição, implementação, operação, fiscalização e auditoria de sistemas de inteligência artificial (IA) empregados em procedimentos judiciais eletrônicos perante tribunais, serviços judiciais, unidades jurisdicionais e órgãos auxiliares do Poder Judiciário, sem prejuízo das competências constitucionais dos tribunais e das normas setoriais existentes.

Art. 2º Para os fins desta Lei, consideram-se, entre outras, as seguintes definições:

I - sistema de inteligência artificial (IA): sistema computacional que, mediante algoritmos, modelos estatísticos, de aprendizagem de máquina, de aprendizagem profunda ou outro método, produz saídas com suporte a decisões, triagens, análises ou sugestões em processos judiciais eletrônicos;

II - sugestão automatizada: qualquer resultado, recomendação, classificação, pontuação, parecer, texto ou anotação produzida total ou parcialmente por sistema de IA que vise subsidiar decisão, despacho ou ato processual;

III - decisão automática: ato decisório praticado sem revisão humana motivada e substantiva sobre a sugestão automatizada;

IV - higienização de entrada: conjunto de procedimentos técnicos destinados a detectar e remover textos invisíveis, camadas ocultas, fontes diminutas, baixo contraste, metadados indevidos, elementos ocultos em imagens e outros artefatos que possam interferir em processamento automático;

V - encapsulamento e pré-filtragem: procedimentos que isolam, formatam e verificam documentos externos antes de sua ingestão por sistemas de IA, de modo a impedir injeção de comandos, códigos ocultos ou manipulação do contexto;

VI - prompt injection: técnica de inserção de instruções maliciosas ou manipulação de dados que altere o comportamento previsto do sistema de IA;

VII - envenenamento de base (data poisoning): inserção deliberada de dados maliciosos em bases de treinamento ou atualização que prejudique o desempenho, integridade ou imparcialidade do modelo;

VIII - contrato de resposta: acordo técnico-jurídico, celebrado com fornecedor de IA, que estabelece obrigações de comportamento do sistema, instrumentos de

rastreabilidade, garantias de audibilidade, mecanismos de correção, níveis de serviço e responsabilidades.

Art. 3º O âmbito de aplicação desta Lei abrange:

I - todos os tribunais e unidades judiciais da Justiça Federal, Estadual, do Trabalho, Eleitoral e Militar;

II - os sistemas eletrônicos de tramitação processual, assinatura, autenticação, certificação, protocolo e peticionamento;

III - sistemas de IA empregados por terceiros contratados para prestar serviços ao Poder Judiciário que, direta ou indiretamente, atuem sobre processos ou documentos judiciais; e

IV - bases de dados, conjuntos de treinamento e modelos utilizados para fins judiciais, inclusive em ambiente de nuvem ou serviços terceirizados.

Art. 4º São princípios obrigatórios aplicáveis à utilização de sistemas de inteligência artificial em procedimentos judiciais eletrônicos:

I - legalidade, transparência e accountability;

II - supervisão humana qualificada (human-in-the-loop);

III - rastreabilidade, auditabilidade e integridade dos registros;

IV - proteção de dados pessoais e do sigilo judicial, em conformidade com a Lei nº 13.709/2018 (LGPD);

V - minimização de dados e anonimização sempre que compatível com a finalidade processual;

VI - prevenção contra prompt injection e envenenamento de bases;

VII - proporcionalidade e não discriminação nas saídas e decisões; e

VIII - observância de padrões técnicos nacionais e internacionais aplicáveis.

Art. 5º Compete ao Conselho Nacional de Justiça (CNJ), sem prejuízo das competências constitucionais dos tribunais e das normas setoriais existentes:

I - Ao CNJ compete:

a) editar normas técnicas complementares e padrões mínimos de auditoria, de segurança e de governança para implementação desta Lei;

b) estabelecer listas de controles técnicos obrigatórios, incluindo, quando aplicável, requisitos de resistência a prompt injection, prevenção de envenenamento de bases, e requisitos de hardening de infraestruturas;

c) definir procedimentos de certificação de fornecedores, critérios de qualificação técnica e modelos de contratos de resposta;

d) fiscalizar tecnicamente a implementação das normas, promover auditorias e aplicar sanções administrativas previstas nesta Lei e em legislação administrativa disciplinar aplicável, sem prejuízo da competência correicional dos tribunais;

e) editar modelos de termo de compromisso, relatórios de auditoria, checklists de higienização e protocolos de resposta a incidentes.

II - As normas expedidas pelo CNJ terão natureza técnica e complementar e poderão ser adaptadas por regulamentação interna dos tribunais, observados os requisitos mínimos dispostos nesta Lei.

Art. 6º Os tribunais e unidades judiciais deverão implementar os requisitos essenciais previstos nesta Lei nos seguintes prazos:

I - Os tribunais e unidades judiciais deverão implementar os requisitos essenciais previstos nesta Lei no prazo máximo de 12 (doze) meses, contado da publicação da norma complementar pelo CNJ, quando for o caso, ou, na ausência desta, da publicação desta Lei.

II - Requisitos secundários poderão ter prazos escalonados para implementação, conforme cronograma elaborado pelo CNJ e pelas unidades gestoras, respeitado o prazo máximo previsto no inciso I para as medidas essenciais.

Art. 7º Constituem requisitos mínimos de segurança, governança e responsabilização para uso de sistemas de inteligência artificial em procedimentos judiciais eletrônicos:

I - Higienização de entrada de arquivos eletrônicos:

a) obrigatoriedade de procedimentos de higienização que detectem e removam textos invisíveis, camadas ocultas, fontes diminutas, baixo contraste, metadados sensíveis, macros, scripts e elementos ocultos em imagens ou outros artefatos capazes de induzir comportamento não previsto do sistema;

b) registro auditável de todas as operações de higienização com indicação do operador, data e resultado.

II - Encapsulamento e pré-filtragem:

a) documentos externos deverão ser encapsulados e submetidos a pré-filtragem antes de sua ingestão por sistemas de IA, mediante transformação em formato padronizado, remoção de elementos executáveis e verificação de consistência semântica;

b) mecanismos automatizados de detecção de padrões de prompt injection deverão ser aplicados na pré-filtragem.

III - Rastreamento e logs:

a) registro obrigatório e imutável (logs) vinculando usuário, certificado digital ou credencial, carimbo temporal confiável (timestamp), hash do arquivo e identificação do ambiente/processo de ingestão;

b) os logs deverão ser preservados por prazo mínimo compatível com a prescrição e regras de arquivo judicial, e em formato que garanta integridade e auditabilidade.

IV - Cópia imutável:

a) manutenção de cópia imutável e íntegra do arquivo original recebido, preservada para fins de perícia e auditoria; qualquer processamento deverá ocorrer sobre cópia encapsulada preservando o original;

b) procedimentos de cadeia de custódia aplicáveis à cópia imutável.

Art. 8º Quando houver utilização de suporte de sistema de inteligência artificial para análise, triagem ou sugestão decisória, aplicam-se as seguintes regras de supervisão humana e identificação de sugestões automatizadas:

I - Quando houver utilização de suporte de IA para análise, triagem ou sugestão decisória:

a) deverá haver supervisão humana qualificada, com atuação nos termos desta Lei e das normas complementares do CNJ, incumbida de avaliação substantiva e motivada das saídas do sistema;

b) toda sugestão automatizada deverá ser claramente identificada nos autos como produção de sistema automatizado, com indicação do modelo, versão, fornecedor, parâmetros relevantes e justificativa técnica automática inicial gerada pelo sistema;

c) é vedada a adoção de decisão automática sem revisão humana motivada, isto é, sem exame substancial e manifestação expressa de servidor ou magistrado responsável;

d) a identificação referida na alínea b deverá constar com metadados estruturados no sistema processual eletrônico, passíveis de extração e auditoria.

II - A supervisão humana prevista no inciso I deverá registrar, de forma estruturada, as razões que fundamentaram a aceitação, modificação ou rejeição da sugestão automatizada.

Art. 9º Na hipótese de suspeita de prompt injection, envenenamento de base ou manipulação que possa afetar o regular andamento ou a segurança do processo, qualquer parte, advogado, servidor, membro do Ministério Público ou magistrado poderá requerer ao juízo competente medida cautelar ou tutela de urgência para:

a) suspensão imediata do uso do modelo ou do conjunto de dados em questão;

a) suspensão imediata do uso do modelo ou do conjunto de dados em questão;

b) preservação de evidências, logs e cópia imutável dos artefatos envolvidos;

c) determinação de perícia técnica independente;

d) adoção de medidas provisórias de mitigação, inclusive bloqueio de acessos suspeitos.

§ 1º O juízo poderá, de ofício, determinar as medidas previstas neste artigo quando houver indícios razoáveis de manipulação. § 2º A perícia técnica independente determinada na forma deste artigo deverá apresentar laudo preliminar no prazo máximo de 60 (sessenta) dias, salvo prorrogação fundamentada pelo juízo.

Art. 10. As obrigações de auditoria, diagnósticos de risco e proteção de bases de sistemas de inteligência artificial observarão as seguintes regras:

I - Obrigatoriedade de diagnóstico inicial de risco realizado por empresa, instituição acadêmica ou órgão independente e qualificado, com escopo que contemple análise de bases de dados, modelos, interfaces de entrada, vetores de ataque e controles de governança.

II - Auditorias técnicas periódicas:

a) auditoria anual quando o sistema for classificado como de criticidade média;

b) auditoria semestral quando classificado como de alta criticidade, sem prejuízo de auditorias extraordinárias em caso de incidentes;

c) escopo mínimo das auditorias: integridade de modelos, detecção de envenenamento de bases, avaliação de vieses e impactos, revisão dos logs de rastreabilidade e verificação dos contratos de resposta.

III - Medidas de proteção de bases e modelos:

a) políticas de hardening e controles de acesso estritos;

b) detecção proativa de envenenamento de bases e rotinas de validação de dados de entrada e atualização de modelos;

c) planos de resposta a incidentes e recuperação, incluindo backup imutável dos modelos e versões, procedimentos de rollback e documentação de mudanças.

Art. 11. A constatação ou a suspeita fundada de prompt injection, envenenamento de base, manipulação de saídas ou qualquer incidente que possa afetar a integridade processual deverá ser comunicada, de imediato:

a) ao juízo competente;

a) ao juízo competente;

b) ao Conselho Nacional de Justiça;

c) ao Ministério Público quando houver indícios de ilícito;

d) aos órgãos de investigação e segurança da informação competentes.

Parágrafo único. A comunicação deverá abranger relatório preliminar, logs relevantes, indicação das ações tomadas e das medidas de preservação de evidências.

Art. 12. Todas as operações de tratamento de dados no âmbito dos sistemas de inteligência artificial deverão observar a Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD), devendo ser adotadas, dentre outras, as seguintes medidas:

a) segregação de dados sigilosos, com políticas de acesso mínimo necessário;

a) segregação de dados sigilosos, com políticas de acesso mínimo necessário;

b) anonimização sempre que possível, especialmente em bases de treinamento e em auditorias externas;

c) avaliação de impacto à proteção de dados pessoais (DPIA) antes da implantação de sistemas relevantes.

§ 1º Em hipóteses de conflito entre necessidade processual e proteção de dados pessoais, deverão ser aplicadas medidas proporcionais e restringir-se o acesso a dados sensíveis, com registro dos fundamentos.

Art. 13. Os contratos celebrados com fornecedores de sistemas de inteligência artificial destinados a uso no Judiciário e as técnicas de prompting adotarão as seguintes regras de rastreabilidade e responsabilização:

I - Os contratos celebrados com fornecedores de sistemas de IA destinados a uso no Judiciário deverão prever cláusulas mínimas de responsabilidade, garantias de integridade, obrigações de manutenção de logs, entrega de modelos explicáveis (quando possível) e cooperação em auditorias independentes.

II - Para comandos decisórios, deverá ser adotado prompting por etapas com sequência estruturada, cada etapa registrada em log auditável, acompanhado de justificativa automática inicial pelo sistema e complementada por manifestação humana.

III - Os contratos deverão prever mecanismos de contingência, de acesso aos modelos e dados para perícia e de reinstauração de versões anteriores dos modelos em caso de incidentes.

Art. 14. O CNJ, ou o órgão competente nos termos de sua regulamentação, poderá aplicar, em face do descumprimento desta Lei e das normas complementares, as seguintes sanções administrativas, sem prejuízo de encaminhamentos civis, funcionais e penais:

a) advertência formal;

a) advertência formal;

b) determinação de correção técnica e de governança no prazo definido;

c) imposição de multa administrativa proporcional à gravidade e ao porte da entidade responsável;

d) suspensão temporária do uso de ferramenta, modelo ou serviço até regularização;

e) publicização da decisão administrativa, observados sigilo e interesse público.

§ 1º As sanções administrativas não excluem o encaminhamento para apuração civil, funcional e penal quando houver indícios de ilícitos, bem como a adoção de medidas processuais de ofício pelo juízo.

§ 2º A aplicação de sanções observará o devido processo administrativo e as garantias constitucionais de ampla defesa e contraditório.

Art. 15. É obrigatória a capacitação semestral de magistrados, servidores, técnicos e demais agentes que utilizem, supervisionem ou credenciem uso de ferramentas de inteligência artificial nos tribunais, conforme as seguintes diretrizes:

I - conteúdo mínimo sobre riscos técnicos, controle de vieses, prevenção de prompt injection, procedimentos de auditoria e requisitos de conformidade com esta Lei;

II - O CNJ elaborará diretrizes e materiais de referência para os programas de capacitação.

Art. 16. O CNJ e os tribunais deverão assegurar a integração das normas técnicas e de governança desta Lei com padrões nacionais e internacionais aplicáveis, observadas as seguintes diretrizes:

I - O CNJ e os tribunais deverão assegurar a integração das normas técnicas e de governança desta Lei com padrões nacionais e internacionais aplicáveis, inclusive NBRs e normas ISO pertinentes, devendo adotar, quando possível, certificações reconhecidas.

II - Regulamentações internas dos tribunais deverão complementar as normas do CNJ, sem reduzir os requisitos mínimos previstos nesta Lei.

Art. 17. Ficam acrescidos à Lei nº 11.419, de 19 de dezembro de 2006, os arts. 3º-A, 3º-B e 3º-C, com a seguinte redação:

Ficam acrescidos à Lei nº 11.419/2006 os seguintes dispositivos:

"Art. 3º-A. Na tramitação eletrônica de processos, é obrigatória a higienização de entrada, o encapsulamento e a pré-filtragem de documentos recebidos por meio eletrônico, conforme padrões técnicos estabelecidos pelo Conselho Nacional de Justiça.

Parágrafo único. Os sistemas de gestão processual eletrônica deverão manter registro imutável do arquivo original, logs de rastreabilidade vinculando usuário, certificado digital, carimbo temporal e hash do arquivo, e disponibilizar essas informações para fins de perícia e auditoria.

"Art. 3º-B. É vedada a ingestão direta de arquivos em sistemas de IA sem prévia verificação automatizada e encapsulamento; documentos externos que contenham elementos executáveis, metadados sensíveis ou formatos não padronizados deverão ser recusados para ingestão até a adequação técnica."

"Art. 3º-C. Os sistemas eletrônicos deverão assegurar que quaisquer anotações, sugeridas ou geradas por sistemas automatizados, estejam claramente identificadas nos autos, acompanhadas de metadados que permitam auditoria e rastreabilidade."

Art. 18. Fica acrescido à Lei nº 13.105, de 16 de março de 2015 (Código de Processo Civil), após o art. 10, o art. 10-A, com a seguinte redação:

Art. 10-A. Quando o processo utilizar suporte de inteligência artificial para análise, triagem ou sugestão decisória:

Art. 10-A. Quando o processo utilizar suporte de inteligência artificial para análise, triagem ou sugestão decisória:

I - deverá haver supervisão humana qualificada, responsável por manifestação motivada sobre a sugestão automatizada antes de qualquer decisão ou ato judicial;

II - toda sugestão automatizada será expressamente identificada nos autos, com indicação do modelo, fornecedor, versão e justificativa técnica automática inicial;

III - é vedada a prolação de decisões automáticas sem revisão humana motivada;

IV - em caso de suspeita de manipulação por prompt injection ou envenenamento de base, o juiz poderá deferir imediatamente medidas cautelares e determinar perícia técnica independente, preservação de logs e suspensão do uso do sistema;

V - qualquer parte poderá arguir, em peça processual, a existência de vício decorrente de uso indevido de IA, indicando elementos probatórios, sem prejuízo de determinação oficiosa pelo magistrado.

Parágrafo único. As hipóteses previstas neste artigo não excluem a necessidade de observância das garantias constitucionais de contraditório, ampla defesa e devido processo legal.

Art. 19. O CNJ e os tribunais adotarão as seguintes medidas de fiscalização técnica e cooperação:

I - O CNJ poderá celebrar termos de cooperação técnica com órgãos públicos, universidades e instituições especializadas para fins de auditoria, certificação e investigação técnica de incidentes.

II - Os tribunais e fornecedores deverão colaborar com as auditorias e perícias, fornecendo acesso a logs, modelos, bases de dados (na medida do permitido pela LGPD) e documentação técnica correlata, mediante os instrumentos legais de proteção ao segredo de justiça e à privacidade.

Art. 20. Os contratos com fornecedores de soluções de inteligência artificial destinados ao uso em ambiente judicial deverão prever, obrigatoriamente, as seguintes cláusulas:

I - Contratos com fornecedores de soluções de IA destinados ao uso em ambiente judicial deverão prever cláusulas contratuais obrigatórias relativas a:

a) obrigações de manutenção de logs e de fornecimento de evidências em caso de auditoria;

b) garantia de interoperabilidade de formatos e exportação de dados e modelos para perícia;

c) obrigação de notificação imediata sobre incidentes de segurança afetando a integridade processual;

d) cláusulas de responsabilização, indenização e medidas de remediação em caso de falha, manipulação ou envenenamento de base.

II - É vedada a contratação de fornecedores que não aceitem cláusulas de auditoria independente e acesso técnico às partes relevantes para fins de perícia.

Art. 21. Para fins de adaptação ao disposto nesta Lei, ficam estabelecidas as seguintes disposições transitórias:

I - As exigências essenciais previstas nesta Lei deverão ser implementadas no prazo máximo de 12 (doze) meses, contado da publicação da norma

complementar do CNJ ou, se esta não for editada, da publicação desta Lei, sem prejuízo das disposições escalonadas previstas pelo CNJ para requisitos secundários.

II - No prazo de 180 (cento e oitenta) dias da publicação desta Lei, o CNJ deverá publicar diretrizes iniciais e critérios de criticidade para fins de auditoria e prazos de implementação.

III - Enquanto não houver certificação formal de fornecedor ou modelo, o uso de sistemas de IA com impacto decisório deverá observar medidas complementares de mitigação de risco, inclusive supervisão humana reforçada e auditoria prévia.

Art. 22. Esta Lei entra em vigor na data de sua publicação.

Art. 23. Revogam-se as disposições em contrário.

JUSTIFICAÇÃO

O uso de sistemas de inteligência artificial pelo Poder Judiciário brasileiro cresceu exponencialmente nos últimos cinco anos. A Resolução CNJ nº 615, publicada em 11 de março de 2025, revogou a Resolução nº 332/2020 e estabeleceu normas para o desenvolvimento, a governança, a auditoria e o uso responsável de soluções de IA no âmbito dos tribunais, criando o Comitê Nacional de IA do Judiciário e determinando supervisão humana obrigatória, classificação de risco, auditorias periódicas e proteção de dados.[1] Essa Resolução representa um avanço significativo, mas opera no plano administrativo: pode ser alterada ou revogada pelo próprio CNJ, não cria base legal para aplicação de sanções penais, e não tem força para alterar as Leis nº 11.419/2006 (processo eletrônico) e nº 13.105/2015 (CPC). Esta proposição converte as obrigações essenciais da Resolução nº 615/2025 em lei ordinária, tornando-as permanentes, vinculantes para todos os poderes e passíveis de sanção mais severa, e adiciona dimensões técnicas que a Resolução não desceu a regular.

O diagnóstico técnico que motiva esta proposição vai além da regulação geral. A técnica de prompt injection — inserção de instruções maliciosas em documentos submetidos a sistemas de IA para alterar seu comportamento — é hoje a principal ameaça documentada à integridade dos processos judiciais eletrônicos que utilizam IA. O TRT-2 aplicou multa por litigância de má-fé em fevereiro de 2026 (Processo nº 1001128-84.2024.5.02.0044) exatamente em razão de manipulação de IA em peças processuais, mas o fundamento legal foi o art. 80 do CPC, não norma específica para esse tipo de fraude.[2]

A ausência de definição legal de prompt injection e de data poisoning no ordenamento brasileiro deixa os tribunais sem instrumento normativo preciso para qualificar a conduta, aplicar sanções proporcionais e determinar medidas cautelares específicas. Esta proposição cria esse instrumento no único plano normativo com força suficiente para isso: a lei ordinária. O PL 2338/2023 (Marco Legal da IA), aprovado pelo Senado em

dezembro de 2024 e ainda em tramitação na Câmara, trata da regulação geral e horizontal, sem descer às especificidades do processo judicial eletrônico que esta proposta cobre.[3]

Contamos com o apoio dos nobres pares para a aprovação desta proposição, que dota o Brasil de um dos marcos legislativos mais completos do mundo em segurança de IA no ambiente forense.

[1] CNJ. Resolução nº 615, de 11 de março de 2025. Disponível em: https://atos.cnj.jus.br/atos/detalhar/6001.

[2] CONJUR. Uso de jurisprudência falsa criada por IA gera multa e ofício à OAB. 16 fev. 2026. Disponível em: https://www.conjur.com.br/2026-fev-16/uso-de-jurisprudencia-criada-por-ia-gera-multa-por-ma-fe-e-oficio-a-oab/.

[3] BARBIERI ADVOGADOS. Regulamentação da Inteligência Artificial no Brasil: Estado Atual e Perspectivas. Mar. 2026. Disponível em: https://www.barbieriadvogados.com/regulamentacao-inteligencia-artificial-brasil/.

Sala das Sessões, de junho de 2026.

RUBENS PEREIRA JÚNIOR

Deputado Federal