



**INSTITUTO DOS ADVOGADOS BRASILEIROS – IAB**

**INDICAÇÃO DA PRESIDÊNCIA nº 022/2025**

**Comissão de Inteligência Artificial e Inovação**

**Relatores:** Patrícia Medeiros, Valéria Ribeiro, Ana Amelia Menna Barreto e Pedro Trovão

**Matéria:**

Inteligência Artificial. Regulação da IA no Poder Judiciário.  
Resolução CNJ nº 615/2025

**Palavras-chave:** INTELIGÊNCIA ARTIFICIAL - PODER JUDICIÁRIO - CNJ -  
REGULAÇÃO - ÉTICA - GOVERNANÇA - TRANSPARÊNCIA

No dia 11 de março de 2025 foi publicada, pelo Conselho Nacional de Justiça, a **Resolução nº 615**, que dispõe sobre as diretrizes para o desenvolvimento, a utilização e a governança de soluções de inteligência artificial no âmbito do Poder Judiciário.

Referido ato normativo atualiza o regime anteriormente estabelecido pela Resolução CNJ nº 332/2020 e decorre do trabalho do Grupo de Trabalho instituído pela Portaria CNJ nº 338/2023, além das contribuições recebidas em audiência pública e dos pareceres técnicos apresentados em sede de consulta normativa. A proposta inicial consistia em uma minuta de alteração à Resolução 332, mas que veio a ser consolidada como resolução autônoma, sob o ponto de vista jurídico-normativo.

A Resolução 615 introduz novos conceitos e institutos - a exemplo de *privacy by design*, classificação de riscos, explicabilidade, contestabilidade e outros — e estabelece parâmetros para o uso de sistemas de inteligência artificial generativa, inclusive por meio de modelos de linguagem de larga escala (LLMs).

Entre as diversas disposições, destaca-se o fato de a Resolução permitir que magistrados e servidores do Judiciário façam uso de soluções privadas de IA generativa, inclusive mediante assinatura individual, sem necessidade de prévia autorização do CNJ, desde que cumpridas regras gerais de segurança da informação, capacitação e governança.

Esse aspecto revela-se de **especial interesse para a advocacia**, tendo em vista seus possíveis reflexos sobre o equilíbrio processual, a publicidade, o contraditório, a fundamentação das decisões judiciais e a paridade de armas. Ademais, a utilização de soluções de IA de maneira individualizada, com controle interno e descentralizado, pode implicar assimetrias técnicas e demandar mecanismos mais robustos de fiscalização, transparência e controle social.

## **PARECER**

Este parecer tem por objetivo analisar a Resolução nº 615 do Conselho Nacional de Justiça (CNJ), que dispõe sobre diretrizes para o desenvolvimento, utilização, auditoria, monitoramento e governança de soluções de inteligência artificial aplicadas no Poder Judiciário

### **Tema: FUNDAMENTOS E PROTEÇÃO**

**Dra. Valéria Ribeiro**

Capítulo I (Definições e Fundamentos - Arts. 1-4)

Capítulo II (Respeito aos Direitos Fundamentais - Arts. 5-7)

Capítulo IX (Segurança da Informação e Proteção de Dados - Arts. 32-35)

Art. 1º A presente Resolução estabelece normas para o desenvolvimento, a governança, a auditoria, o monitoramento e o uso responsável de soluções que adotam técnicas de inteligência artificial (IA) no âmbito do Poder Judiciário, com o objetivo de promover a inovação tecnológica e a eficiência dos serviços judiciais de modo seguro, transparente, isonômico e ético, em benefício dos jurisdicionados e com estrita observância de seus direitos fundamentais.

O processo de governança e auditoria desempenha um papel essencial no acompanhamento da implementação de IA no Judiciário, entretanto, deve ser estruturada de forma a garantir que os modelos de IA sejam desenvolvidos e aplicados com base em princípios sólidos de ética e

responsabilidade, sendo necessário inclusive um **rigoroso controle** sobre as **decisões automatizadas** e um **processo contínuo de auditoria das soluções**, de forma a permitir a verificação da conformidade com as normas estabelecidas e a avaliação dos resultados em termos de isenção e justiça.

A **auditoria contínua** garante inclusive que os sistemas de IA não evoluam para práticas prejudiciais, como o viés algorítmico, o que poderá comprometer a igualdade e imparcialidade das decisões judiciais.

O uso da IA deve garantir que os dados sensíveis dos cidadãos sejam protegidos e utilizados apenas para fins legítimos e específicos com transparência, segurança e consentimento.

A resolução estabelece que o uso de IA no Judiciário deve ser realizado de forma **isonômica e ética** com a finalidade da **não discriminação**. Esse ponto é de crucial importância em razão da possibilidade de a IA replicar **vieses históricos e preconceitos** presentes nos dados com os quais são treinados os sistemas. Dentro desse contexto, visando combater esse risco, a Resolução determina que as soluções de IA no Judiciário sejam desenvolvidas e monitoradas de maneira a garantir que seus resultados sejam justos e imparciais, com implementação de mecanismos de auditoria para identificar e corrigir.

§ 1º A governança das soluções de IA deverá respeitar a autonomia dos tribunais, permitindo o desenvolvimento e a implementação de soluções inovadoras locais, ajustando-se aos contextos específicos de cada tribunal, desde que observados os padrões de auditoria, monitoramento e transparência definidos por esta Resolução, sem prejuízo da atuação do CNJ, no âmbito de suas competências.

Decerto que a governança envolve uma série de diretrizes e estruturas de modo a assegurar que sejam usadas de forma ética, responsável e eficiente, bem como estratégias no tocante a ataques cibernéticos.

A política de governança é cíclica e é importante que não haja um modelo centralizado nos Tribunais para que seja assegurado a autonomia dos tribunais locais. A Resolução deixa claro que a autonomia concedida ao Tribunais locais para desenvolver suas próprias soluções específicas para atender à demanda local, realidade jurídica, social e cultural não é absoluta, haja vista que deve haver observância a auditoria, monitoramento e transparência a fim de que haja uma uniformidade nas soluções.

A autonomia dos tribunais é um princípio fundamental do Poder Judiciário assegurado pela Constituição Federal e deve ser observado e respeitado na implementação de soluções de IA.

É fundamental que o tribunal local garanta que as soluções inovadoras não comprometam a imparcialidade, igualdade e justiça das decisões judiciais com um sistema de governança robusto que garanta também a transparência das decisões automatizadas.

§ 2º A auditoria e o monitoramento das soluções de IA serão realizados com base em critérios proporcionais ao impacto da solução, garantindo que os sistemas sejam auditáveis ou monitoráveis de forma prática e acessível, sem a obrigatoriedade de acesso irrestrito ao código-fonte, desde que sejam adotados mecanismos de transparência e controle sobre o uso dos dados e as decisões automatizadas.

Esse parágrafo apresenta um conjunto de reflexões sobre a auditoria prática, os mecanismos de controle aplicados à IA no Judiciário e a transparência necessária para assegurar a responsabilidade e a imparcialidade.

O princípio da proporcionalidade reflete a necessidade de adequação da fiscalização das soluções de IA em razão do impacto que essas soluções possuem no Judiciário e nos direitos dos indivíduos.

Nesse contexto, se torna imprescindível a adoção de um modelo de auditoria e monitoramento proporcional ao impacto das soluções de IA para garantir que a implementação das tecnologias não comprometa os direitos fundamentais dos cidadãos e o princípio da justiça. E mais, que a auditoria e o monitoramento proporcional assegurem que os sistemas sejam acessíveis e práticos para avaliação, ou seja, que os procedimentos de auditoria sejam objetivos, transparentes, linguagem simples e acessível de forma a garantir que, sem recorrer ao código-fonte, os auditores possam avaliar a justiça e a transparência das decisões automatizadas, sem comprometer os direitos de privacidade ou do segredo de justiça.

§ 3º A transparência no uso de IA será promovida por meio de indicadores claros e relatórios públicos, que informem o uso dessas soluções de maneira compreensível e em linguagem simples, garantindo que os jurisdicionados tenham ciência do uso de IA, quando aplicável, sem que isso prejudique a eficiência ou credibilidade dos processos e decisões judiciais.

Esse preceito normativo dispõe que as ferramentas de IA utilizadas no Judiciário não apenas cumpram sua função de otimização de processos, como também estejam em conformidade com os princípios fundamentais de acesso à justiça, igualdade e direitos humanos.

Dispõe ainda que seja adotado uma estratégia de comunicação clara e acessível, que visa garantir que todos os stakeholders possam entender os indicadores do uso de IA nos processos judiciais, e que, embora altamente técnico, seja traduzido em termos simples e **acessíveis**.

Um ponto importante é que o § 3º da Resolução deixou de fazer referência a linguagem acessível, mencionando e se limitando apenas a linguagem simples. De suma importância a adoção de linguagem simples e ACESSÍVEL, visto que corresponde a linguagem que seja compreendida, independente de deficiência, limitação e habilidade.

Outro ponto é a complexidade técnica dos modelos de IA utilizados no judiciário, no qual são baseados em aprendizado de máquina e redes neurais, o que pode tornar difícil a tradução de decisões automatizadas para uma linguagem simples e acessível. Isso implicará não só na capacitação dos operadores do direito como inclusive das ferramentas adequadas para a comunicação dos resultados de forma didática.

§ 4º Os tribunais deverão priorizar o desenvolvimento colaborativo de soluções de IA promovendo a interoperabilidade e a disseminação de tecnologias, códigos, bases de dados e boas práticas com outros órgãos do Poder Judiciário.

O § 4º da Resolução do CNJ situa a prioridade no desenvolvimento colaborativo de solução de IA como centro para a evolução da tecnologia no Poder Judiciário. Assim, a tecnologia da IA não deve ser desenvolvida de forma isolada, mas sim em conjunto entre os diferentes tribunais, órgãos e instituições dentro do Judiciário;

A interoperabilidade envolve a capacidade de diferentes sistemas e plataformas tecnológicas de IA funcionarem de maneira integrada, de maneira que os dados, algoritmos e soluções possam ser compartilhadas entre diferentes tribunais e órgãos do Judiciário de forma eficiente e segura.

A disseminação de tecnologias e códigos viabiliza que os tribunais impeçam duplicação de esforços e criem um ambiente de desenvolvimento mais eficiente.

Entretanto, não se pode desconsiderar a necessidade da adoção de protocolos de governança comuns para assegurar que as soluções de IA sejam aplicadas de forma monitorada e auditada, respeitando os direitos fundamentais.

§ 5º O CNJ poderá criar mecanismos de incentivo, tais como reconhecimento público, premiações ou priorização de recursos e investimentos em inovação, para tribunais que, dentre outros critérios previstos em regulamento, adotem práticas colaborativas/cooperativas no desenvolvimento de soluções de IA.

Este dispositivo versa sobre a criação de mecanismos de incentivo para os tribunais que adotem práticas colaborativas no desenvolvimento de soluções de IA. Visa fomentar a inovação dentro do Judiciário e estimular uma cultura de cooperação entre os tribunais brasileiros alinhados com os avanços tecnológicos.

No entanto, a adoção de IA no Judiciário exige não apenas uma abordagem técnica, mas também uma governança que assegure a equidade, transparência e respeito aos direitos fundamentais.

**Art. 2º** O desenvolvimento, a governança, a auditoria, o monitoramento e o uso responsável de soluções de inteligência artificial (IA) pelo Poder Judiciário têm como fundamentos:

- I – o respeito aos direitos fundamentais e aos valores democráticos;
- II – a promoção do bem-estar dos jurisdicionados;
- III – o desenvolvimento tecnológico e o estímulo à inovação no setor público, com ênfase na colaboração entre os tribunais e o Conselho Nacional de Justiça para o incremento da eficiência dos serviços judiciários, respeitada a

autonomia dos tribunais para o desenvolvimento de soluções que atendam às suas necessidades específicas;

IV – a centralidade da pessoa humana;

V – a participação e a supervisão humana em todas as etapas dos ciclos de desenvolvimento e de utilização das soluções que adotem técnicas de inteligência artificial, ressalvado o uso dessas tecnologias como ferramentas auxiliares para aumentar a eficiência e automação de serviços judiciais meramente acessórios ou procedimentais e para suporte à decisão;

VI – a promoção da igualdade, da pluralidade e da justiça decisória;

VII – a formulação de soluções seguras para os usuários internos e externos, com a identificação, a classificação, o monitoramento e a mitigação de riscos sistêmicos;

VIII – a proteção de dados pessoais, o acesso à informação e o respeito ao segredo de justiça;

No [artigo 2º](#) da Resolução, são estruturados os princípios e diretrizes que conduzirão a aplicação da IA no Judiciário e são importantes para assegurar que a tecnologia não prejudique os direitos dos cidadãos e a isenção judicial, posto que não se trata de simples adoção de novas tecnologias, e sim, da adoção de uma abordagem responsável e ética.

Ressalte-se que um dos aspectos inovadores da Resolução é a promoção da autonomia dos tribunais para o desenvolvimento de solução de IA que atendam às necessidades locais.

Destaca-se que o uso da IA deve ser um complemento ao julgamento humano, e não um substituto da análise jurídica, e por essa razão, a resolução enfatiza a supervisão humana em todas as etapas dos ciclos de desenvolvimento e de utilização das soluções de IA.

Ao assegurar que todas as decisões automatizadas ou ações assistidas por IA no Judiciário estejam em consonância com a proteção dos direitos fundamentais, significa que o algoritmo de IA utilizado em decisões judiciais deve ser construído de forma a evitar qualquer tipo de discriminação, preconceito ou viés, quer de classe social, gênero, racial ou qualquer outro.

**Art. 3º** O desenvolvimento, a governança, a auditoria, o monitoramento e o uso responsável de soluções de inteligência artificial (IA) pelos tribunais têm como princípios:

- I – a justiça, a equidade, a inclusão e a não-discriminação abusiva ou ilícita;
- II – a transparência, a eficiência, a explicabilidade, a contestabilidade, a auditabilidade e a confiabilidade das soluções que adotam técnicas de inteligência artificial;
- III – a segurança jurídica e a segurança da informação;
- IV – a busca da eficiência e qualidade na entrega da prestação jurisdicional pelo Poder Judiciário, garantindo sempre a observância dos direitos fundamentais;
- V – o devido processo legal, a ampla defesa e o contraditório, a identidade física do juiz e a razoável duração do processo, com observância das prerrogativas e dos direitos dos atores do sistema de Justiça;
- VI – a prevenção, a precaução e o controle quanto a medidas eficazes para a mitigação de riscos derivados do uso intencional ou não-intencional de soluções que adotam técnicas de inteligência artificial;
- VII – a supervisão humana efetiva, periódica e adequada no ciclo de vida da inteligência artificial, considerando o grau de risco envolvido, com possibilidade de ajuste dessa supervisão conforme o nível de automação e impacto da solução utilizada;

VIII – a oferta, pelos tribunais e suas escolas, de capacitação contínua para magistrados e servidores sobre riscos da automação, vieses algorítmicos e análise crítica dos resultados gerados por IA.

A regulação internacional tem desempenhado um papel-chave na definição de diretrizes para garantir que as crescentes implementações de tecnologias de IA no setor público e privado não prejudiquem direitos fundamentais e que os sistemas sejam auditáveis, compreensíveis e justos.

Os princípios estabelecidos no inciso II do artigo 3º da Resolução são fundamentais para a governança e uso responsável de soluções de IA no Judiciário Brasileiro. Esses princípios estão alinhados com as diretrizes da União Europeia, OCDE, Unesco e ONU.

Os compromissos com esses princípios promovem a inclusão e a justiça no uso da IA e põe o Judiciário em conformidade com os padrões globais de governança tecnológica.

**Art. 4º** Para o disposto nesta Resolução, consideram-se:

I – sistema de inteligência artificial (IA): sistema baseado em máquina que, com diferentes níveis de autonomia e para objetivos explícitos ou implícitos, processa um conjunto de dados ou informações fornecidas e com o objetivo de gerar resultados prováveis e coerentes de decisão, recomendação ou conteúdo, que possam influenciar o ambiente virtual, físico ou real;

II – ciclo de vida: série de fases que compreende a concepção, planejamento, desenvolvimento, treinamento, retreinamento, testagem, validação, implantação, monitoramento e eventuais modificações e adaptações de um sistema de inteligência artificial, incluindo sua descontinuidade, que pode ocorrer em quaisquer das etapas referidas, e o acompanhamento de seus impactos após a implantação;

III – Sinapses: solução computacional destinada a armazenar, testar, treinar, distribuir e auditar modelos de inteligência artificial, disponível na Plataforma Digital do Poder Judiciário – PDPJ-Br;

IV – desenvolvedor de sistema de inteligência artificial: pessoa natural ou jurídica, de natureza pública ou privada, que desenvolva ou comissione um sistema de inteligência artificial, com a finalidade de colocá-lo no mercado ou aplicá-lo em serviço fornecido, sob seu próprio nome ou marca, a título oneroso ou gratuito;

V – usuário: pessoa que utiliza o sistema de IA e exerce controle sobre suas funcionalidades, podendo tal controle ser regulado ou limitado conforme seja externo ou interno ao Poder Judiciário;

VI – usuário interno: membro, servidor ou colaborador do Poder Judiciário que desenvolva ou utilize o sistema inteligente, podendo ser enquadrado em diferentes perfis conforme o cargo e área de atuação;

VII – usuário externo: pessoa externa ao Poder Judiciário, que interage diretamente com o sistema de IA do Judiciário, incluindo advogados, defensores públicos, procuradores, membros do Ministério Público, peritos, assistentes técnicos e jurisdicionados em geral; VIII – distribuidor: pessoa natural ou jurídica, de natureza pública ou privada, que disponibiliza e distribui sistema de IA para que terceiro o opere a título oneroso ou gratuito;

IX – inteligência artificial generativa (IA generativa ou IAGen): sistema de IA especificamente destinado a gerar ou modificar significativamente, com diferentes níveis de autonomia, texto, imagens, áudio, vídeo ou código de software, além dos modelos estatísticos e de aprendizado a partir dos dados treinados;

X – avaliação preliminar: processo de avaliação de um sistema de IA, pelo tribunal desenvolvedor ou contratante, antes de sua utilização ou entrada em produção na PDPJ-Br, com o objetivo de classificar seu grau de risco e atender às obrigações estabelecidas nesta Resolução;

XI – avaliação de impacto algorítmico: análise contínua dos impactos de um sistema de IA sobre os direitos fundamentais, com a identificação de medidas preventivas, mitigadoras de danos e de maximização dos impactos positivos, sem a violação da propriedade industrial e intelectual da solução de IA utilizada;

XII – Comitê Nacional de Inteligência Artificial do Judiciário: Comitê com composição plural que tem por finalidade auxiliar o Conselho Nacional de Justiça na implementação, no cumprimento na supervisão da aplicação desta Resolução, sempre mediante diálogo com os tribunais e a sociedade civil;

XIII – viés discriminatório ilegal ou abusivo: resultado indevidamente discriminatório que cria, reproduz ou reforça preconceitos ou tendências, derivados ou não dos dados ou seu treinamento;

XIV – *privacy by design*: preservação da privacidade dos dados desde a concepção de qualquer novo projeto ou serviço de IA durante todo o seu ciclo de vida, inclusive na anonimização e encriptação de dados sigilosos;

XV – *privacy by default*: utilização, por padrão, de alto nível de confidencialidade de dados;

XVI – *prompt*: texto em linguagem natural utilizado na IA generativa para execução de uma tarefa específica;

XVII – auditabilidade: capacidade de um sistema de IA se sujeitar à avaliação dos seus algoritmos, dados, processos de concepção ou resultados;

XVIII – explicabilidade: compreensão clara, sempre que tecnicamente possível, de como as “decisões” são tomadas pela IA;

XIX – contestabilidade: possibilidade de questionamento e revisão dos resultados gerados pela IA.

Ciclo de vida de um sistema de IA corresponde à sequência de etapas e processos pelos quais o sistema de IA passa desde a sua concepção inicial até sua implantação final e monitoramento contínuo.

O planejamento envolve a definição de um cronograma de desenvolvimento, a alocação de recursos e o estabelecimento de um plano de riscos. É uma etapa crítica para garantir que todas as fases subsequentes do ciclo de vida do sistema sejam bem coordenadas e executadas no prazo.

Uma das fases importantes de um sistema de IA é o treinamento do modelo, que envolve a alimentação do algoritmo com dados históricos para que ele aprenda a identificar padrões e tomar decisões de forma autônoma.

Tecnologia como contenção de dados, segurança de rede e infraestrutura de computação distribuída podem ser utilizadas para garantir que o sistema seja robusto e funcione de maneira eficiente em grande escala.

O **monitoramento** pode incluir a **deteção de falhas**, o acompanhamento de **indicadores de desempenho** e a **avaliação contínua** de possíveis **riscos** de impacto no processo decisório.

A interação das tecnologias, juntamente a supervisão humana, é essencial para garantir que os sistemas de IA no Judiciário cumpram os objetivos sem comprometer a justiça, legalidade e direitos dos cidadãos.

Plataforma Sinapses tem por objetivo principal o armazenamento, treinamento supervisionado, controle de versionamento, distribuição e auditoria de modelos de IA desenvolvidos pelos tribunais e conselhos do Judiciário.

O desenvolvedor de sistemas de IA desempenha um papel fundamental na criação de soluções que transformam tanto os mercados quanto os serviços públicos.

## **CAPÍTULO II - DO RESPEITO AOS DIREITOS FUNDAMENTAIS (Arts. 5 A 7)**

**Art. 5º** No desenvolvimento, na implantação e no uso de soluções de inteligência artificial no Judiciário, os tribunais observarão sua compatibilidade com os direitos fundamentais, especialmente aqueles

previstos na Constituição da República ou em tratados de que a República Federativa do Brasil seja parte.

§ 1º A verificação de compatibilidade com os direitos fundamentais deverá ocorrer em todas as fases do ciclo de vida da solução de inteligência artificial, incluindo o desenvolvimento, implantação, uso, atualizações e eventuais retreinamentos dos sistemas e seus dados.

§ 2º Os tribunais deverão implementar mecanismos de auditoria e monitoramento contínuos, com vistas a garantir que as soluções de IA permaneçam em conformidade com os direitos fundamentais, e proceder a ajustes sempre que forem identificadas incompatibilidades.

§ 3º Havendo notícia ou indícios de violação a direitos fundamentais, assegura-se à Ordem dos Advogados do Brasil (OAB), ao Ministério Público e demais entidades legitimadas, o acesso às avaliações de impacto algorítmico e o direito de peticionar ao Comitê, para que seja avaliada a necessidade de solicitação de auditorias e outras formas de controle.

O artigo 5º da Resolução reforça a necessidade de os tribunais atentem para a compatibilidade das soluções de IA com os direitos fundamentais ao estabelecer princípios e diretrizes para assegurar que o uso de IA no Judiciário esteja em conformidade com os direitos fundamentais dispostos na CFRB/88 e Tratados Internacionais no qual o Brasil é parte, bem como enfatiza a necessidade de compatibilidade da IA com os direitos humanos.

Dispõe ainda a verificação da compatibilidade com os direitos fundamentais em todas as fases do ciclo de vida da solução de IA, ou seja, desde a fase inicial de desenvolvimento e implementação.

O § 3º do artigo 5º define que na hipótese de violação ou indícios de violação de direitos fundamentais, entidades como a OAB, o MP e outras

entidades legitimadas têm o direito de acessar as avaliações de impacto algorítmico e de peticionar ao Comitê Nacional de IA do Judiciário.

**Art. 6º** A adoção de aplicações que utilizem modelos de inteligência artificial deve buscar garantir a segurança jurídica e colaborar para que o Poder Judiciário respeite os princípios previstos no art. 3º desta Resolução.

**Parágrafo único.** Os tribunais e desenvolvedores de IA serão responsáveis pela criação de diretrizes internas para assegurar que as soluções de IA estejam em conformidade com os princípios estabelecidos no art. 3º desta Resolução, com mecanismos adequados de supervisão e revisão periódica.

O artigo 6º da predita Resolução trata de garantir a segurança jurídica no uso do IA e da responsabilidade dos tribunais e desenvolvedores de IA no sentido que seja respeitado os princípios do artigo 3º da Resolução.

Define inclusive diretrizes internas que são: transparência, governança, auditabilidade, segurança de dados, prevenção de vieses discriminatórios, monitoramento contínuo, revisão periódica.

**Art. 7º** Os dados utilizados no desenvolvimento ou treinamento de modelos de inteligência artificial devem ser representativos de casos judiciais e observar as cautelas necessárias quanto ao segredo de justiça e à proteção de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). § 1º Consideram-se dados representativos aqueles que refletem de forma adequada a diversidade de situações e contextos presentes no Poder Judiciário, evitando vieses que possam comprometer a equidade e a justiça decisória.

§ 2º Os dados deverão ser anonimizados sempre que possível, providência obrigatória para os dados sigilosos ou protegidos por segredo de justiça, de

acordo com as melhores práticas de proteção de dados e segurança da informação.

§ 3º Os tribunais deverão implementar mecanismos de curadoria e monitoramento dos dados utilizados, assegurando a conformidade com a legislação de proteção de dados e a revisão periódica das práticas de tratamento de dados.

O artigo 7º da Resolução estabelece normas rigorosas para o uso de dados judiciais concentrado na segurança da informação, anonimização e equidade decisória, observando Lei Geral de Proteção de Dados – LGPD.

A anonimização e a curadoria contínua é uma prática fundamental para proteger a privacidade dos indivíduos e cumprir com as exigências da LGPD, que envolve a remoção de informação pessoal identificável dos dados.

### Segurança da Informação e Proteção de Dados

**Art. 32.** O sistema inteligente deverá assegurar a autonomia dos usuários internos, com o uso de modelos que:

I – promovam o incremento da eficiência, precisão e qualidade das atividades, sem limitar a capacidade de atuação dos usuários;

II – possibilitem a revisão detalhada do conteúdo gerado e dos dados utilizados para sua elaboração, assegurando que os usuários tenham acesso às premissas e ao método empregado pela inteligência artificial na sua formulação, sem que haja qualquer espécie de vinculação à solução apresentada pela inteligência artificial e garantindo-se a possibilidade de correções ou ajustes.

**Parágrafo único.** Em nenhum momento o sistema de IA poderá restringir ou substituir a autoridade final dos usuários internos.

O dispositivo normativo determina diretrizes para equilibrar a eficiência da IA com a autonomia humana. Tem um papel importante em razão de garantir que a IA seja uma ferramenta de apoio, e não um substituto da decisão humana.

A implementação das diretrizes dispostas no artigo 32 da Resolução, tem implicações práticas para o desenvolvimento e uso do sistema de IA, como: design centrado no usuário, interfaces intuitivas e explicativas, treinamento e capacitação, monitoramento e avaliação contínua.

**Art. 33.** Os usuários externos deverão ser informados, de maneira clara, acessível e objetiva, sobre a utilização de sistemas baseados em IA nos serviços que lhes forem prestados, devendo ser empregada linguagem simples, que possibilite a fácil compreensão por parte de pessoas não especializadas.

§ 1º A informação prevista no caput deste artigo deverá destacar o caráter consultivo e não-vinculante da proposta de solução apresentada pela inteligência artificial, a qual sempre será submetida à análise e decisão final de uma autoridade competente, que exercerá a supervisão humana sobre o caso.

§ 2º A comunicação sobre o uso de IA deverá ser realizada por meio de canais adequados, como avisos nos sistemas utilizados, materiais informativos e guias explicativos, com o intuito de orientar os usuários externos sobre o funcionamento, limitações e objetivos dos sistemas inteligentes no Judiciário.

§ 3º A comunicação sobre o eventual uso da IA no texto de decisões judiciais será uma faculdade de seu signatário, observado o disposto art. 19, § 3º, IV, e § 6º, desta Resolução.

§ 4º Os tribunais deverão disponibilizar periodicamente materiais educativos que ajudem os usuários externos a compreenderem o uso de IA

nos processos judiciais, esclarecendo que tais sistemas têm papel de suporte, sem substituir a autoridade decisória humana.

O artigo 33 define diretrizes fundamentais para a comunicação clara e acessível para o uso de IA.

Manteve a comunicação clara com a utilização de linguagem simples, deixando de incluir que a linguagem além de simples, seja acessível, posto que linguagem simples, por si só, não corresponde a ser acessível.

**Art. 34.** Os sistemas computacionais utilizados no âmbito do Poder Judiciário deverão exigir a supervisão humana e permitir a modificação pelo magistrado competente de qualquer produto gerado pela inteligência artificial, sempre que cabível, observado o art. 32 desta Resolução.

O **artigo 34** da Resolução define dois princípios para o uso da IA no Judiciário, quais sejam: supervisão humana obrigatória e possibilidade de modificação das decisões automatizadas.

Estabelece ainda que os sistemas de IA devam permitir a modificação, pelo magistrado, de produto gerado pela IA, sempre que cabível, garantindo assim aos magistrados ajustar ou corrigir as decisões propostas pela IA.

**Art. 35.** A composição de equipes para pesquisa, desenvolvimento e implantação das soluções computacionais que se utilizem de inteligência artificial será orientada pela busca da diversidade e representatividade, com ênfase na inclusão, sempre que possível, de diferentes perfis de gênero e etnia e pessoas com deficiência, bem como de experiências e formação em áreas de conhecimento diversas.

§ 1º A participação representativa deverá ser assegurada, tanto quanto possível, nas etapas de planejamento, coleta e processamento de dados, construção, verificação, validação e implementação dos modelos, tanto nas áreas técnicas como negociais.

§ 2º A diversidade na participação prevista no caput deste artigo poderá ser dispensada mediante decisão fundamentada, dentre outros motivos, pela ausência de profissionais no quadro de pessoal dos tribunais ou a necessidade de garantir eficácia e a velocidade na implementação das soluções a curto prazo.

§ 3º A formação das equipes mencionadas no caput deverá ter caráter interdisciplinar, incluindo profissionais de Tecnologia da Informação, do Direito e de outras áreas relevantes, cujo conhecimento científico possa contribuir para pesquisa, desenvolvimento ou implantação do sistema inteligente no Tribunal.

O dispositivo apresenta três diretrizes: diversidade e representatividade na composição de equipes, participação interdisciplinar no desenvolvimento, possibilidade de dispensa da diversidade por justificativa técnica.

Com a adoção da diversidade e da interdisciplinaridade se fortalece a segurança, transparência e eficiência dos sistemas, assegurando soluções tecnológicas eficazes e éticas.

### **Implicações Éticas e Legais**

A ferramenta de automação pode comprometer a imparcialidade, caso não seja devidamente controlada, auditada e corrigida. Deve -se buscar e criar um ambiente controlado e regulado, onde a ética e os direitos fundamentais sejam preservados.

Outrossim, a governança e o monitoramento contínuo devem ser acessíveis a sociedade quanto aos processos de decisão, não podendo ser impenetráveis, mantendo a transparência e a responsabilidade impõe em caso de erro ou viés, devendo (no sentido de obrigação) de fornecer explicações claras com linguagem acessível sobre a ocorrência e a sua correção.

Deve ser acrescido que o uso da linguagem deve ser simples E ACESSÍVEL, ou seja, uma abordagem de forma clara, objetiva e inclusiva, priorizando frases curtas, ordem direto, uso de palavras conhecidas, evitando termos exclusivamente técnicos.

A linguagem ACESSÍVEL é uma forma de comunicação que tem por finalidade precípua garantir que a informação seja compreendida por todos, independentemente de suas habilidades, deficiência ou limitação.

O desenvolvimento e aplicação da IA deverá ser realizado com uma **avaliação contínua do impacto social** tendo como sua base o **princípio da dignidade humana** para que não ocorra a automação excessiva para fins de atingir a sua finalidade e que as ferramentas de IA no Judiciário sejam auditáveis, transparentes com a viabilidade de explicar as decisões de forma acessível e compreensível, garantindo que a modernização do judiciário traga benefícios tangíveis e concretos à sociedade, sem prejudicar as bases democráticas e de justiça.

A inteligência artificial não pode ser entendida como uma entidade autônoma, mas sim como uma ferramenta para promover uma justiça ágil, acessível e eficiente.

O Judiciário, ao incorporar o uso da IA, deve estar diligente para que a tecnologia não se sobreponha aos direitos humanos.

Devido à complexidade dos sistemas modernos que utilizam redes distribuídas, *cloud computing e big data*, ampliando a superfície de ataque

cibernético, o que exigirá medidas de segurança cada vez mais sofisticadas e atualização das ferramentas utilizadas pelo Judiciário.

No mesmo sentido, o uso de IA no Judiciário apresenta desafios quanto à implementação e garantia da compatibilidade com os direitos fundamentais que são: complexidade dos algoritmos, transparência, evolução, monitoramento contínuo.

### **Sugestões**

A análise revelou a necessidade do uso da tecnologia blockchain e a criptografia são ferramentas que devem ser utilizadas pelo Judiciário para garantir a transparência e imutabilidade dos dados judiciais e na segurança da informação.

No mesmo contexto, a Resolução n. 615 do CNJ não tratou de conflitos harmônica e heterocompositivas como mediação e conciliação.

Faltou a consonância entre a cultura da paz no direito digital.

Outro ponto é o uso de linguagem simples sob a ótica de linguagem acessível, quando a linguagem deve ser simples e acessível, e não somente simples.

**Tema: GOVERNANÇA DE RISCOS E DADOS**

**Professor Doutor Pedro Trovão do Rosário**

Capítulo III (Categorização de riscos - Arts. 9-14)

Anexo (Classificação de Riscos)

Capítulo VIII (Qualidade e Segurança - Arts. 26-31)

*Art. 9º*

Os Tribunais, enquanto órgãos de soberania independentes, têm formação, composição, competência e funcionamento definidos na Lei Fundamental, a Constituição.

Assim, cabe aos tribunais “realizar a avaliação das soluções que utilizem técnicas de inteligência artificial”, ou seja a “avaliação deverá ser realizada pelo tribunal desenvolvedor ou contratante da solução”, limitando-se o “Comitê Nacional de Inteligência Artificial do Judiciário a fixar “as diretrizes e os critérios de avaliação de risco”.

Aos tribunais incumbirá de forma independente administrar a justiça em nome do povo, assegurando a defesa dos direitos e interesses legalmente protegidos dos cidadãos, (ainda obstando à violação da legalidade democrática e resolvendo os conflitos de interesses públicos e privados).

São assim os tribunais órgãos de soberania independentes apenas sujeitos à lei, mormente à Constituição.

Se a importância da independência dos Tribunais na sua ação se faz sentir de tantas formas nos diversos sistemas jurídico-constitucionais (os juízes são inamovíveis, não podendo ser transferidos, suspensos, aposentados ou demitidos senão nos casos previstos na lei; em regra não podem ser responsabilizados pelas suas decisões, etc.), também este poder-dever “de avaliação das soluções que utilizem técnicas de inteligência artificial, com a finalidade de definir o seu grau de risco” é um modo de garantia de

independência na eleição dos instrumentos a serem utilizados na administração da justiça.

#### *Art. 10*

Aqui podemos destacar a importância da “revisão humana dos resultados propostos” e a valorização do princípio da igualdade, vedando a discriminação. Só com supervisão humana das decisões é possível assegurar que a justiça e a equidade prevaleçam, evitando a criação de novas questões de discriminação ou exclusão.

Deve acautelar-se a utilização da IA centrada no ser humano, em pleno respeito pelos direitos humanos, a democracia e o Estado de Direito. Não é admissível a discriminação em razão do sexo, raça ou origem étnica, território de origem, idade, religião ou crença, deficiência, idade ou orientação sexual, ou qualquer outro fator de desigualdade.

Assim, as decisões baseadas em IA têm que ser sempre acompanhadas e monitorizadas para que não resultem ou se fundamentem em preconceitos e “juízos” arbitrários, impondo-se a revisão humana dos resultados propostos. Assim, desde logo o cuidado nos dados e algoritmos, não podendo os dados refletirem desigualdades sociais, que os sistemas em consequência utilizariam, mantendo e agravando a desigualdade.

Igualmente preocupante a falta de transparência nos algoritmos, não sendo possível conhecer como as decisões são tomadas. Tal limita a definição da responsabilidade e a própria correção de “erros” que se verificarem no uso ou resultados. A supervisão humana é particularmente relevante na apreciação ou detecção de fatores mais subtis, os quais mais dificilmente são detetados por sistemas automatizados. É pois vital garantir a transparência nos algoritmos a par de uma seleção cuidadosa dos dados, através de auditorias regulares.

## *Art. 11*

A Resolução 615 em análise, no contexto de aprimoramento do sistema de Processo Judicial eletrônico (PJe) utiliza a palavra “risco” 72 vezes, enquanto o Regulamento da União Europeia (UE) 2024/1689, que “visa incentivar o desenvolvimento e a adoção de sistemas de inteligência artificial (IA) seguros e fiáveis em todo o mercado único da União Europeia (UE)” utiliza a palavra “risco” 778 vezes.

Tal permite verificar a importância na definição e categorização das soluções de IA. Esta legislação segue uma abordagem ‘baseada no risco’, o que significa que quanto maior for o risco de causar danos à sociedade, mais rigorosas são as regras. Os sistemas de alto risco, como os utilizados na justiça, estão sujeitos a regras mais exigentes.

Afigura-se no entanto que não devem ser apenas as “soluções de alto risco” que “deverão ser submetidas a processos regulares de auditoria e monitoramento contínuo para supervisionar seu uso e mitigar potenciais riscos aos direitos fundamentais, à privacidade e à justiça”, devendo ser todos as que estão associadas a uma atividade de risco elevado, como a Justiça.

### *Classificação de Riscos - Anexo da Resolução*

Os sistemas de IA concebidos para a administração da justiça devem ser num primeiro momento classificados como sendo de risco elevado, tendo em conta o seu impacto potencialmente significativo no Estado de Direito, nas liberdades individuais, no direito à ação e a um tribunal imparcial, livre e independente.

Para fazer face aos riscos de possíveis enviesamentos, erros e opacidade, é adequado classificar como de risco elevado os sistemas de IA concebidos para serem utilizados por um Tribunal na interpretação de factos e do Direito e na aplicação da lei aos factos *sub judice*.

Há que distinguir a utilização de ferramentas de IA enquanto “meras” auxiliares do poder de tomada de decisão pelos magistrados, da própria decisão, pois a IA não pode substituir na decisão final a atividade humana.

No entanto, a classificação de sistemas de IA como sendo de risco elevado não deverá ser alargada aos sistemas de IA concebidos para atividades administrativas meramente auxiliares que não afetem a superior administração efetiva da justiça. Neste caso a investigação jurídica, por precedentes, ou a conceção de textos de apoio. Da mesma forma, tarefas administrativas, atos como a anonimização ou a pseudonimização de decisões judiciais, documentos ou dados, comunicações entre intervenientes e pessoal.

#### *Art. 26*

Manifesta-se aqui a estreita relação entre dados utilizados no processo de desenvolvimento de soluções de inteligência artificial e a Lei Geral de Proteção de Dados Pessoais. Com a utilização de IA surgem riscos para a privacidade de dados, tais como a violação de dados, monitorização e vigilância inadequada, falta de transparência, falta de segurança, entre outros.

Os sistemas de IA são concebidos para aprender e melhorar através da análise de grandes quantidades de dados, sendo constante e colossal a quantidade de dados pessoais recolhidos pelos sistemas de IA. É essencial que os Tribunais tomem medidas proativas para proteger a privacidade dos dados, tais como, a implementação de protocolos fortes de segurança de dados, garantindo que os dados em causa são usados apenas para a finalidade pretendida, a par do desenvolvimento de sistemas transparentes que permitam explicar, inspecionar e reproduzir as decisões e a utilização dos dados em causa.

#### *Art. 27*

Deve ser assegurada pelo sistema a qualidade de dados, mantendo-os precisos, completos, consistentes, oportunos e relevantes para o uso pretendido. Assim, a sua manutenção deverá ser igualmente ponderada e assegurado que se mantém relevante a detenção dos dados, com mecanismos próprios para acompanhamento dos dados, sua qualidade e relevância.

#### *Arts. 28, 29, 30, 31*

A quantidade de dados recolhidos e armazenados deve ser limitada ao mínimo necessário para a finalidade específica do sistema de IA, impondo-se a criação de medidas robustas de segurança para proteção dos dados contra acessos não autorizados e violações.

Quem desenvolve e/ou opera sistemas de IA deve ser responsável pela proteção dos dados pessoais e pela mitigação de risco, com *“adoção de mecanismos de auditoria periódica e monitoramento contínuo para assegurar a conformidade dos ambientes com esses padrões de segurança, garantindo a proteção adequada contra acessos não autorizados, falhas de integridade e outras ameaças à segurança da informação”*, criando sistemas adequados de controle de acesso e criptografia de dados, a par de um conjunto de diretrizes e procedimentos que definem como os dados armazenados devem ser gerenciados enquanto detidos e utilizados, incluindo a recolha, armazenamento, processamento, uso, compartilhamento e destruição dos dados, garantindo que estes sejam precisos, seguros e tudo esteja conforme com às boas práticas e regras aplicáveis.

## Sugestões

**Da análise *supra* crê-se adequado manifestar particular cautela relativamente aos seguintes pontos:**

1. Que sejam já determinados mecanismos de garantia do respeito pela obrigatoriedade de “revisão humana” e as consequências de não ser respeitada tal imposição, com definição de cominação para os infratores.
2. Definição na norma de mecanismos de monitoramento contínuo para garantir o cumprimento do respeito pelas restrições e imposições legais, os quais ilustram e têm associados -sem exclusão de outros- a existência de padrões de conduta e boas práticas;
3. Não devem ser apenas as “soluções de alto risco” que “deverão ser submetidas a processos regulares de auditoria e monitoramento contínuo para supervisionar seu uso e mitigar potenciais riscos aos direitos fundamentais, à privacidade e à justiça”, mas todas as que estão associadas a uma atividade de risco elevado, como a Justiça. Assim, as soluções de “baixo risco” de desenvolvimento de soluções baseadas em inteligência artificial destinadas a desempenhar ou apoiar o usuário na realização das seguintes atividades acessórias submetidas a processos regulares de auditoria e monitoramento contínuo.

**Tema: CONTROLE E SUPERVISÃO**

**Dra. Ana Amelia Menna Barreto**

Capítulo IV (Das Medidas de Governança - Arts. 12-14)

Capítulo V (Da Supervisão e Implementação - Arts. 15-18)

Capítulo XI (Da Auditoria e do Monitoramento - Arts. 39-42)

### **Das Medidas de Governança**

Os Tribunais têm o dever de implementar mecanismos de monitoramento contínuo para garantir o desenvolvimento de soluções de IA a fim de prevenir o uso inadvertido das tecnologias proibidas por acarretarem risco excessivo à segurança da informação, aos direitos fundamentais dos cidadãos ou à independência dos magistrados (art. 10).

O tribunal desenvolvedor ou contratante deverá estabelecer processos internos aptos a garantir a segurança dos sistemas de inteligência artificial, incluindo:

- medidas de transparência quanto ao emprego e à governança de sistemas de IA, com a publicação de relatórios que detalhem o funcionamento dos sistemas, suas finalidades, dados utilizados e mecanismos de supervisão;
- a prevenção e mitigação de potenciais vieses discriminatórios ilegais ou abusivos, por meio de monitoramento contínuo, com a análise de resultados e a correção de eventuais desvios, garantindo a revisão periódica dos modelos de IA;
- a implementação de mecanismos de governança que garantam o acompanhamento contínuo dos sistemas de IA prevendo a definição de pessoas ou comitês internos responsáveis pela fiscalização do cumprimento das diretrizes de segurança e transparência, bem como pela análise de relatórios e recomendações de melhorias;

- a diretriz para que seja priorizado o desenvolvimento de soluções interoperáveis, que possam ser compartilhadas e integradas entre diferentes órgãos judiciais, evitando a duplicação de esforços e garantindo eficiência no uso de recursos tecnológicos;
- a determinação de que só deverão ser adotadas soluções de código aberto ou comerciais que permitam flexibilidade de adaptação aos contextos locais, desde que respeitadas as diretrizes de segurança, transparência e proteção de dados pessoais;
- a orientação de que as soluções de IA devem ser tratadas com práticas de gestão de produto, que incluam fases de definição de requisitos, desenvolvimento, testes, implementação, suporte e melhorias contínuas, com revisões que garantam a evolução dessas soluções e a mitigação de riscos associados;
- a diretriz de incentivo ao desenvolvimento de interfaces de programação de aplicações (APIs) que permitam a interoperabilidade para comunicação direta com os sistemas tecnológicos de outras instituições públicas que atuam junto à estrutura de Justiça, garantindo-se a celeridade, segurança e integridade dos dados; e
- acesso à OAB, à advocacia pública, ao Ministério Público e às Defensorias, conforme o caso, aos relatórios de auditoria e monitoramento e à parametrização ao longo do ciclo de vida da solução que envolver o uso de inteligência artificial, nos termos desta Resolução.

A solução que utilize modelos de inteligência artificial de alto risco - antes de ser colocada em produção - deverá adotar medidas extras de governança:

- I – sempre que tecnicamente possível, utilizar dados de treinamento, validação e teste que sejam adequados, representativos e equilibrados, contendo propriedades estatísticas apropriadas em relação às pessoas afetadas e levando em conta características e elementos específicos do

contexto geográfico, comportamental ou funcional no qual o sistema de IA de alto risco será utilizado;

II – registro de fontes automatizadas e do grau de supervisão humana que tenham contribuído para os resultados apresentados pelos sistemas IA, a serem submetidos a auditorias regulares e monitoramento contínuo;

III – indicação clara e em linguagem simples dos objetivos e resultados pretendidos pelo uso do modelo de IA, de forma que possam ser compreendidos pelos usuários e supervisionados pelos magistrados;

IV – documentação em linguagem simples, no formato adequado a cada agente de IA e à tecnologia usada, do funcionamento do sistema e das decisões envolvidas em sua construção, considerando todas as etapas relevantes no ciclo de vida do sistema e atualizado sempre que o sistema evolua;

V – uso de ferramentas ou processos de registro automático da operação do sistema (log), sempre que tecnicamente possível, para permitir a avaliação periódica de sua acurácia e robustez, apurar potenciais resultados discriminatórios, com implementação das medidas de mitigação de riscos e atenção para efeitos adversos e identificar eventual uso malicioso ou indevido do sistema;

VI – medidas para mitigar e prevenir vieses discriminatórios, bem como políticas de gestão e governança para promoção da responsabilidade social e sustentável; e

VII – adoção de medidas para viabilizar a explicabilidade adequada, sempre que tecnicamente possível, dos resultados dos sistemas de IA e de medidas para disponibilizar informações adequadas em linguagem simples e acessível que permitam a interpretação dos seus resultados e funcionamento, respeitados o direito de autor, a propriedade intelectual

e os sigilos industrial e comercial, mas garantida a transparência mínima necessária para atender ao disposto nesta Resolução.

A elaboração da avaliação de impacto deve, sempre que possível, incluir a participação pública, ainda que de maneira simplificada, e o acompanhamento, com acesso aos relatórios, de representante da OAB, do Ministério Público e da Defensoria Pública.

As conclusões da avaliação de impacto, incluindo eventuais ações corretivas adotadas, serão públicas e disponibilizadas na plataforma Sinapses, por meio de relatórios claros e acessíveis, de forma a permitir o entendimento por magistrados, servidores e o público em geral.

### **Supervisão e Implementação**

Foi instituído o **Comitê Nacional de Inteligência Artificial do Judiciário** formado por 14 membros titulares, representando o CNJ, Tribunais, Escolas de Magistratura, Magistrados, OAB, MP e Defensoria Pública e representantes da sociedade civil.

Entretanto, os representantes da OAB, do Ministério Público, da Defensoria Pública e sociedade civil, têm apenas direito a voz no âmbito do Comitê.

As competências do Comitê estão dispostas no art. 16 e dizem respeito a implantação de mecanismos de verificação, de controle e monitoramento de regras e avaliação dos riscos associados ao uso de inteligência artificial no âmbito do Poder Judiciário, com a obrigação de apresentar avaliação anual em relatório circunstanciado.

Os critérios de avaliação para atualização das hipóteses de categorização de riscos, o Comitê Nacional de Inteligência Artificial do Judiciário considerará as diretrizes da Resolução 615, obedecendo critérios dispostos no art. 17.

Empresas que prestem serviços de armazenamento, processamento, intermediação digital ou inteligência artificial ao Poder Judiciário, ou que

operem plataformas com impacto direto no exercício da jurisdição brasileira, devem observar integralmente as decisões judiciais proferidas no Brasil e atuar em conformidade com a legislação nacional, observando-se o seguinte:

- a) os tribunais deverão adotar mecanismos de monitoramento contínuo para identificar eventuais descumprimentos de decisões judiciais por parte dessas empresas, comunicando tais infrações às autoridades competentes para adoção das medidas cabíveis;
- b) nos contratos firmados com empresas de tecnologia, deverão ser incluídas cláusulas contratuais que exijam o cumprimento da legislação e das decisões judiciais brasileiras, prevendo expressamente a possibilidade de rescisão contratual e a aplicação das penalidades em caso de descumprimento.

### **Auditoria e Monitoramento**

A Resolução CNJ 615 considerou a necessidade de assegurar o desenvolvimento e a implantação de modelos de inteligência artificial no Poder Judiciário que observem critérios éticos de transparência, previsibilidade, auditabilidade e justiça substancial.

Qualquer solução computacional do Poder Judiciário que utilize modelos de inteligência artificial deverá assegurar total transparência na prestação de contas, com o objetivo de garantir um impacto positivo para os usuários finais e para a sociedade.

Entende-se como usuário externo a pessoa externa ao Poder Judiciário, que interage diretamente com o sistema de IA do Judiciário, incluindo advogados, defensores públicos, procuradores, membros do Ministério Público, peritos, assistentes técnicos e jurisdicionados em geral.

As soluções de inteligência artificial devem ser auditadas sob a ótica da segurança da informação, proteção de dados, performance, robustez,

confiabilidade, prevenção de vieses discriminatórios, correlação entre entradas e saídas e conformidade legal e ética.

A auditoria e o monitoramento das soluções de IA serão realizados com base em critérios proporcionais ao impacto da solução, garantindo que os sistemas sejam auditáveis ou monitoráveis de forma prática e acessível, sem a obrigatoriedade de acesso irrestrito ao código-fonte, desde que sejam adotados mecanismos de transparência e controle sobre o uso dos dados e as decisões automatizadas (art.1º, § 2º)

O Comitê Nacional de Inteligência Artificial do Judiciário estabelecerá protocolo de auditoria e monitoramento para modelos e soluções de inteligência artificial em uso no Poder Judiciário.

O monitoramento consistirá em um conjunto simplificado de análise, verificação e adoção de boas práticas de gestão de dados, processos e produtos, a fim de verificar a regularidade do funcionamento da solução baseada em IA e a manutenção de sua conformidade com as diretrizes desta Resolução.

Havendo identificação de desconformidades, o Comitê fixará prazo para recomendar ações corretivas, que será definido com base na gravidade e impactos da desconformidade.

Os órgãos do Poder Judiciário deverão informar ao Comitê Nacional de Inteligência Artificial do Judiciário todos os eventos adversos relacionados ao uso de soluções de inteligência artificial, no prazo de até setenta e duas horas após a sua identificação, contendo descrição do incidente, suas causas e as medidas adotadas para correção.

Consideram-se eventos adversos os incidentes que resultem em impactos negativos sobre a operação do sistema, a segurança dos dados ou a prestação de serviços.

## Sugestões

A efetiva implementação de mecanismos de verificação, de controle, de monitoramento contínuo, auditoria, o estabelecimento de processos internos aptos a garantir a segurança dos sistemas de IA não estão garantidos pelas regras instituídas pela Resolução 615.

Os Tribunais estão obrigados a informar os eventos adversos ao Comitê Nacional de Inteligência Artificial do Judiciário somente **após** sua identificação, em se tratando da aplicação de sistemas de alto risco. Quando deveriam comunicar **antes** de aplicar o uso do sistema.

A liberalidade da possibilidade de utilização de licenças privadas por magistrados e servidores - no exercício das funções do seu cargo no Judiciário - coloca em risco as condições de uso dos dados pessoais e a segurança da informação como um todo (art. 16, VI).

Em que pese a possibilidade de serem ouvidos especialistas externos e a sociedade civil, assim como a OAB, estes não têm direito a voto.

Deve ser fiscalizado -em caráter primordial- a efetiva e indispensável capacitação de magistrados e servidores, assim como a avaliação do conhecimento adquirido, para prevenir o uso de tecnologias proibidas por acarretarem risco excessivo à segurança da informação, aos direitos fundamentais dos cidadãos ou à independência dos magistrados.

**TEMA: Uso Prático e Capacitação****Dra. Patrícia Medeiros**

Capítulo VI (Uso e Contratação de LLMs e IAGens - Arts. 19-20)

Capítulo VII (Transparência e Registro no Sinapses - Arts. 21-25)

Capítulo X (Da Pesquisa, desenvolvimento e da implantação de serviços de IA - Arts. 35-38)

Capítulo XII (Disposições Finais - Arts. 43-47)

**Capítulo VI - Do Uso e da Contratação de LLMs e IAGens (Arts. 19-20)**

O **Art. 19** da Resolução estabelece que modelos de linguagem de larga escala (LLMs), de pequena escala (SLMs) e outros sistemas de inteligência artificial generativa (IAGen) poderão ser utilizados por magistrados e servidores como ferramentas auxiliares à gestão ou de apoio à decisão. Este dispositivo merece especial atenção por representar uma mudança paradigmática em relação à minuta inicial, que previa uma abordagem mais restritiva.

Enquanto a minuta de proposta de alteração da Resolução 332/2020 estabelecia em seu **Art. 8º-E, §1º**, uma vedação expressa à "utilização dos modelos e dos sistemas mediante assinaturas ou cadastros de natureza privada ou pessoal dos magistrados, dos servidores ou de terceiros, ressalvadas as hipóteses expressamente autorizadas pelo Comitê de Inteligência Artificial do CNJ", a versão final da Resolução 615/2025 adotou uma abordagem significativamente mais permissiva.

O **§ 2º do Art. 19** possibilita o magistrado, servidor ou colaborador a contratação direta de solução mediante assinatura ou cadastro de natureza privada quando o tribunal não oferecer solução corporativa específica, desde que atendidas as diretrizes do §3º. Esta flexibilização, embora condicionada a requisitos como capacitação específica, uso auxiliar (não autônomo), conformidade com proteção de dados e vedações para dados sigilosos,

representa um ponto crítico para a efetiva transparência, auditabilidade e segurança da informação.

O **§3º do Art. 19** estabelece cinco condições para a contratação direta de ferramentas de IA para uso individual, que merecem análise pormenorizada:

**Inciso I** - Capacitação e letramento digital: Este inciso determina que "os usuários deverão realizar capacitação e treinamentos específicos sobre melhores práticas, limitações, riscos, e uso ético, responsável e eficiente de LLMs e dos sistemas de IA generativa para a utilização em suas atividades, conforme programa de letramento digital padronizado, nos termos do inciso VII do art. 16 desta Resolução, ficando a cargo dos tribunais e de suas escolas a promoção dos treinamentos continuados aos magistrados e servidores."

Este requisito é fundamental, porém apresenta lacunas críticas: (1) não estabelece a obrigatoriedade de capacitação prévia ao uso das ferramentas, permitindo que magistrados e servidores utilizem sistemas de IA antes de estarem devidamente capacitados; (2) não define parâmetros mínimos para essa capacitação nem mecanismos de verificação de sua efetividade; (3) não estabelece a periodicidade para atualização da capacitação, essencial considerando a rápida evolução das tecnologias de IA; e (4) não prevê consequências concretas para o descumprimento deste requisito.

A ausência de capacitação prévia obrigatória compromete seriamente a supervisão humana efetiva, pois magistrados e servidores sem conhecimento adequado sobre as limitações e riscos das ferramentas de IA podem não realizar a revisão crítica necessária dos resultados gerados por esses sistemas e tampouco a utilização responsável e segura.

**Inciso II** - Caráter auxiliar e complementar: Este inciso estabelece que "o uso dessas ferramentas será de caráter auxiliar e complementar, consistindo em mecanismos de apoio à decisão, vedada a utilização como instrumento autônomo de tomada de decisões judiciais sem a devida orientação, interpretação, verificação e revisão por parte do magistrado, que permanecerá

integralmente responsável pelas decisões tomadas e pelas informações nelas contidas."

Embora este inciso reafirme o *princípio da supervisão humana*, sua efetividade é comprometida pela ausência de mecanismos concretos para verificar se essa supervisão está de fato ocorrendo.

Ademais, a facultatividade da menção ao uso de IA no corpo da decisão (§6º do Art. 19) torna praticamente impossível para as partes e seus advogados identificarem quando e como a IA foi utilizada, comprometendo a contestabilidade e a transparência do processo decisório.

De fato, o §6º do Art. 19 estabelece que a menção ao uso de IA generativa no corpo da decisão é facultativa ("poderá ser mencionada [...] a critério do magistrado").

Quando um magistrado utiliza uma ferramenta de IA privada, contratada individualmente, torna-se praticamente impossível para o usuário externo (jurisdicionado, advogado) verificar se houve efetivamente supervisão humana adequada, se os dados foram tratados conforme as normas de proteção e segurança, e se os resultados gerados pela IA foram devidamente revisados e interpretados pelo magistrado. A contestabilidade, princípio fundamental previsto no Art. 3º, II, da Resolução, fica severamente comprometida nesse cenário.

Esta facultatividade compromete a *transparência externa* e a possibilidade de contestação pelos usuários externos, que não terão conhecimento sobre quando e como a IA foi utilizada na elaboração de decisões judiciais.

**Inciso III** - Proteção de dados e propriedade intelectual: Este inciso determina que "as empresas fornecedoras dos serviços de LLMs e IA generativa devem observar padrões de política de proteção de dados e de propriedade intelectual, em conformidade com a legislação aplicável, sendo vedado o tratamento, uso ou compartilhamento dos dados fornecidos pelos usuários do Poder Judiciário, bem como dos dados inferidos a partir desses, para

treinamento, aperfeiçoamento ou quaisquer outros fins não expressamente autorizados."

Este requisito, embora essencial, apresenta um problema fundamental de verificabilidade, ponto crítico no que diz respeito à segurança da informação e ao princípio do *privacy by default*.

O §3º, III, do Art. 19 exige que as empresas fornecedoras dos serviços de LLMs e IA generativa contratadas observem padrões de política de proteção de dados e de propriedade intelectual, vedando o tratamento, uso ou compartilhamento dos dados fornecidos pelos usuários do Poder Judiciário para treinamento ou outros fins não autorizados. Contudo, é praticamente impossível para o magistrado, ao contratar individualmente uma ferramenta de IA verificar se essa conformidade está sendo efetivamente cumprida pela empresa fornecedora.

Além disso, não há mecanismos de verificação da conformidade das empresas fornecedoras com esses requisitos. A mera declaração de conformidade por parte da empresa não é suficiente para garantir a proteção efetiva dos dados judiciais, muitos dos quais contêm informações sensíveis mesmo quando não classificados como sigilosos.

**Inciso IV** - Vedação ao uso com dados sigilosos: Este inciso estabelece que "é vedado o uso de LLMs e sistemas de IA generativa de natureza privada ou externos ao Judiciário para processar, analisar, gerar conteúdo ou servir de suporte a decisões a partir de documentos ou dados sigilosos ou protegidos por segredo de justiça, nos termos da legislação aplicável, salvo quando devidamente anonimizados na origem ou quando forem adotados mecanismos técnicos e procedimentais que garantam a efetiva proteção e segurança desses dados e de seus titulares."

Este inciso apresenta duas exceções problemáticas à vedação: (1) anonimização na origem e (2) adoção de mecanismos técnicos e procedimentais de proteção. Ambas as exceções são de difícil verificação e

implementação por magistrados individualmente, sem apoio técnico especializado.

A anonimização efetiva de dados judiciais é um processo complexo que requer conhecimento técnico específico, especialmente considerando que muitos detalhes aparentemente inócuos podem levar à reidentificação quando combinados. Já a adoção de "mecanismos técnicos e procedimentais" é uma expressão vaga que não define parâmetros concretos de segurança.

Ademais, mesmo com anonimização, o envio de dados judiciais para sistemas de IA externos representa um risco significativo, pois esses dados podem ser utilizados para inferir padrões decisórios, estratégias processuais e outras informações sensíveis.

**Inciso V** - Vedação ao uso para finalidades de risco excessivo ou alto risco: Este inciso determina que "é vedado o uso de LLMs e sistemas de IA generativa de natureza privada ou externos ao Judiciário para as finalidades previstas nesta Resolução como de risco excessivo ou de alto risco, nos termos do art. 10 e 11 desta Resolução."

Embora esta vedação seja crucial, sua efetividade depende da correta classificação de risco das atividades, o que requer conhecimento técnico específico que muitos magistrados ou servidores podem não possuir.

Além disso, a ausência de mecanismos de verificação e fiscalização torna esta vedação de difícil aplicação prática. Sem um sistema robusto de monitoramento e auditoria, não há como garantir que ferramentas de IA privadas não estejam sendo utilizadas para finalidades de alto risco ou risco excessivo.

### **Importância dos parágrafos 7º e 8º do Art. 19:**

Os parágrafos 7º e 8º do Art. 19 estabelecem um mecanismo de prestação de informações que, embora insuficiente, representa uma tentativa de mitigar os riscos associados ao uso individual de ferramentas de IA privadas:

**§7º** - Dever de informação ao tribunal: "Na hipótese do § 2º deste artigo, o magistrado que contratar solução de mercado de inteligência artificial para uso em suas atividades no Poder Judiciário, ou o gestor que tiver em sua equipe servidor ou colaborador que utilize essas soluções, deverá prestar informações ao seu respectivo tribunal sobre sua utilização, na forma do regulamento."

Este parágrafo estabelece um dever fundamental de *transparência interna*, exigindo que magistrados e gestores informem aos tribunais sobre o uso de soluções de IA contratadas individualmente. Este mecanismo é essencial para que os tribunais possam ter conhecimento das ferramentas utilizadas em sua jurisdição e, potencialmente, identificar riscos e problemas.

Contudo, a eficácia deste dispositivo depende criticamente de regulamentação posterior ("na forma do regulamento"), que deverá definir quais informações devem ser prestadas, com que periodicidade e em que formato. Sem uma regulamentação detalhada, este dever de informação pode se tornar meramente formal, sem conteúdo substantivo que permita uma efetiva supervisão.

**§8º** - Consolidação e envio de informações ao Comitê Nacional: "Os tribunais consolidarão as informações recebidas na forma do § 7º deste artigo para envio ao Comitê Nacional de Inteligência Artificial do Judiciário, que as utilizará para os fins previstos no art. 25 desta Resolução."

Este parágrafo complementa o anterior, estabelecendo um fluxo de informações dos tribunais para o Comitê Nacional de Inteligência Artificial do Judiciário. Este mecanismo é fundamental para uma visão sistêmica do uso de IA no Judiciário, permitindo ao Comitê identificar tendências, riscos e boas práticas em nível nacional.

A referência ao art. 25 indica que estas informações serão utilizadas para a publicação, pelo CNJ, da "relação das aplicações que adotam técnicas de inteligência artificial, desenvolvidas ou utilizadas pelos órgãos do Poder Judiciário, com descrição em linguagem simples e precisa e a indicação do grau de risco respectivo".

Contudo, para que este mecanismo seja efetivo, é essencial que: (1) os tribunais estabeleçam processos robustos de consolidação e análise das informações recebidas, não se limitando a repassá-las mecanicamente ao Comitê; (2) o Comitê Nacional desenvolva metodologias para análise sistemática dessas informações, identificando padrões, riscos e oportunidades de melhoria; e (3) os resultados dessas análises sejam efetivamente utilizados para aprimorar a governança de IA no Judiciário, incluindo possíveis revisões da própria Resolução.

A análise detalhada dos incisos do §3º e dos parágrafos 7º e 8º do Art. 19 revela que, embora a Resolução estabeleça condições e mecanismos de prestação de informações para o uso individual de ferramentas de IA privadas, estes são insuficientes para garantir a efetiva transparência, auditabilidade, confiabilidade, explicabilidade e supervisão humana.

Os principais problemas identificados, portanto, são:

**1.Verificabilidade limitada:** Não há mecanismos efetivos para verificar se as condições do §3º estão sendo cumpridas, especialmente no que diz respeito à proteção de dados e à supervisão humana efetiva.

**2.Capacitação não prévia:** A capacitação não é exigida como condição prévia ao uso das ferramentas, permitindo que magistrados sem conhecimento adequado utilizem sistemas de IA em suas decisões.

**3. Transparência externa comprometida:** A facultatividade da menção ao uso de IA nas decisões compromete a transparência externa e a contestabilidade.

**4. Regulamentação pendente:** A eficácia dos mecanismos de prestação de informações depende de regulamentação posterior, que pode variar significativamente entre os tribunais.

**5. Ausência de consequências:** Não há previsão de consequências para o descumprimento das condições estabelecidas, o que pode comprometer sua efetividade.

A permissão para uso individual de ferramentas de IA mediante assinaturas privadas (Art. 19, §2º) representa um dos pontos mais críticos da Resolução. Esta flexibilização compromete seriamente a possibilidade de verificação da supervisão humana efetiva, princípio fundamental previsto no Art. 3º, VII, da Resolução.

### Sugestões

1. Limitar o uso individual a ferramentas corporativas: O ideal seria limitar o uso individual apenas a ferramentas corporativas desenvolvidas ou contratadas pelos tribunais, que passaram por processos rigorosos de verificação de conformidade.

2. Exigir capacitação prévia: Caso a permissão para uso individual de ferramentas privadas seja mantida, deve-se exigir capacitação prévia obrigatória, com certificação específica.

3. Tornar obrigatória a menção ao uso de IA: A menção ao uso de IA generativa no corpo das decisões judiciais deve ser obrigatória, não facultativa.

4. Estabelecer mecanismos de verificação: Devem ser criados mecanismos concretos para verificar o cumprimento das condições estabelecidas, incluindo auditorias periódicas.

5. Detalhar a regulamentação: O CNJ deve estabelecer diretrizes detalhadas para a regulamentação dos mecanismos de prestação de informações,

garantindo uniformidade e efetividade em todos os tribunais. Nessa toada, a regulamentação deverá exigir, no mínimo: (1) identificação precisa da ferramenta utilizada, incluindo versão e fornecedor; (2) finalidades específicas de uso; (3) tipos de dados fornecidos à ferramenta; (4) medidas adotadas para garantir a conformidade com os requisitos do §3º; e (5) relatório periódico de uso, incluindo estatísticas sobre frequência e contexto de utilização.

6. Criação de um programa nacional de letramento digital para magistrados e servidores, com foco específico em transparência, auditabilidade, confiabilidade, explicabilidade e supervisão humana efetiva no uso de IA.

7. Obrigatoriedade de adoção de mecanismos de privacy by design e privacy by default em todas as ferramentas de IA utilizadas no Judiciário, com verificação prévia de conformidade antes de sua utilização.

8. Criação de um protocolo específico para verificação de conformidade das ferramentas de IA com os requisitos de segurança da informação e proteção de dados, a ser aplicado antes de sua utilização, especialmente no caso de ferramentas de uso individual.

9. Obrigatoriedade de registro e documentação de todos os incidentes de segurança envolvendo ferramentas de IA, com comunicação imediata ao CNJ e aos usuários potencialmente afetados.

10. Obrigatoriedade de adoção de mecanismos de explicabilidade em todas as ferramentas de IA utilizadas no Judiciário, com documentação detalhada sobre como as decisões são tomadas e quais fatores são considerados.

11. Criação de um procedimento específico para contestação de decisões judiciais baseadas em IA garantindo o direito ao contraditório e à ampla defesa.

12. Obrigatoriedade de disponibilização, mediante solicitação, de informações detalhadas sobre o funcionamento da ferramenta de IA utilizada em uma decisão judicial específica, garantindo a transparência e a possibilidade de contestação.

A governança de riscos em IA requer mecanismos institucionais robustos de supervisão e auditoria, que são inviabilizados quando o uso ocorre de forma individualizada e descentralizada. A impossibilidade de verificação efetiva da

## **Capítulo VII - Transparência e Registro no Sinapses (Arts. 21-25)**

O Capítulo VII estabelece mecanismos de transparência e registro das soluções de IA no Sinapses, plataforma mantida pelo CNJ.

Entretanto, a efetividade desses mecanismos de transparência é severamente comprometida pela permissão de uso individual de ferramentas privadas estabelecida no Capítulo VI.

O **Art. 23, III**, por exemplo, dispensa o depósito do código-fonte, bases de dados e demais partes da solução quando as licenças de proteção ao direito autoral e à propriedade intelectual limitem seu compartilhamento público, exigindo apenas a indicação dos sistemas, motores e bases utilizados.

Esta exceção, embora compreensível do ponto de vista da propriedade intelectual, cria uma lacuna significativa na transparência e auditabilidade das soluções de IA utilizadas no Judiciário, especialmente quando combinada com a permissão para uso individual de ferramentas privadas.

O **Art. 24** estabelece a obrigatoriedade de cadastro das soluções de IA no Sinapses, com diferentes requisitos conforme a classificação de risco. Para soluções de alto risco, o cadastro deve ser realizado antes do início do desenvolvimento, enquanto para soluções de baixo risco, basta o cadastro antes da entrada em produção.

O **Art. 25** determina que o CNJ publicará a relação das aplicações de IA em seu site, com descrição em linguagem simples e indicação do grau de risco. Esta publicidade é essencial para o controle social, mas sua eficácia depende da completude e precisão das informações fornecidas

Destaca-se a importância da transparência e do registro adequado das soluções de IA para sua governança efetiva. Contudo, a permissão para uso individual de ferramentas privadas cria um cenário de opacidade que compromete esses objetivos.

Os mecanismos de transparência e registro estabelecidos no Capítulo VII são importantes, mas sua efetividade é comprometida pela permissão de uso individual de ferramentas privadas e pela dispensa de depósito do código-fonte e bases de dados em determinadas situações.

**Diante do exposto, sugere-se/recomenda-se:**

O aprimoramento dos mecanismos de transparência externa, garantindo que todas as ferramentas de IA utilizadas no Judiciário, sejam devidamente registradas e documentadas no Sinapses, com informações acessíveis à advocacia e ao público.

A criação de um sistema de certificação de conformidade para ferramentas de IA utilizadas no Judiciário, que ateste o cumprimento dos requisitos de transparência, auditabilidade, confiabilidade e explicabilidade, a ser realizado por entidade independente.

A obrigatoriedade de relatórios periódicos pelos tribunais sobre o uso de IA incluindo estatísticas sobre o uso individual e seu impacto na transparência e auditabilidade das decisões judiciais.

**Capítulo X - Da Pesquisa, do Desenvolvimento e da Implantação de Serviços de IA (Arts. 35-38)**

O Capítulo X estabelece diretrizes para pesquisa, desenvolvimento e implantação de serviços de IA no Judiciário.

### **Art. 35 - Diversidade e Representatividade nas Equipes**

O Art. 35 orienta que a composição das equipes deve buscar diversidade e representatividade, com ênfase na inclusão de diferentes perfis de gênero, etnia e pessoas com deficiência, bem como diversidade de formação e experiência. Esta disposição é fundamental para mitigar vieses algorítmicos, mas apresenta fragilidades:

O §2º permite a dispensa da diversidade mediante decisão fundamentada, por motivos como ausência de profissionais no quadro ou necessidade de garantir eficácia e velocidade na implementação.

Não há métricas ou parâmetros objetivos para avaliar a diversidade das equipes.

Não há mecanismos de verificação ou incentivo para garantir a efetiva implementação desta diretriz.

### **Art. 36 - Princípios Éticos para Pesquisa em IA**

O Art. 36 estabelece princípios éticos para pesquisa em IA incluindo respeito à dignidade humana, coibição de práticas discriminatórias e identificação de vieses. Contudo, não há diretrizes específicas sobre como implementar esses princípios na prática. Não há exigência de documentação ou registro das medidas adotadas para garantir o respeito a esses princípios. Não há tampouco mecanismos de verificação ou auditoria para avaliar o cumprimento desses princípios.

### **Art. 37 - Cadastro e Continuidade das Soluções**

O Art. 37 determina o cadastro das iniciativas no Sinapses e a continuidade das soluções enquanto forem úteis, prevendo seu encerramento quando houver desconformidade com a Resolução. Entretanto, não há critérios objetivos para avaliar a "utilidade" das soluções. Tampouco há diretrizes para a transição ou migração de dados quando uma solução for descontinuada. O §2º estabelece requisitos adicionais para modelos de reconhecimento facial ou

análise biométrica, mas não detalha os critérios para autorização pelo Comitê Nacional.

### **Art. 38 - Uso de Ferramentas de Mercado ou Código Aberto**

O Art. 38 permite o uso de ferramentas de mercado ou soluções de código aberto que facilitem integração, interoperabilidade, desenvolvimento colaborativo, transparência, cooperação, segurança de dados e não-dependência tecnológica. Contudo, não há critérios específicos para avaliação e seleção dessas ferramentas.

Tampouco diretrizes para verificar a conformidade dessas ferramentas com os requisitos de segurança e proteção de dados.

#### **Diante do exposto, sugere-se/recomenda-se:**

-A criação de métricas objetivas para avaliar a diversidade nas equipes de desenvolvimento de IA incluindo indicadores quantitativos e qualitativos que considerem não apenas a composição demográfica, mas também a efetiva participação de diferentes perfis nas decisões críticas.

Sugere-se a limitação das hipóteses de dispensa da diversidade (§2º do Art. 35), estabelecendo critérios mais rigorosos e exigindo justificativa detalhada e aprovação prévia pelo Comitê Nacional de IA do Judiciário, especialmente para projetos de alto risco.

- A criação de um programa de capacitação e inclusão para aumentar a disponibilidade de profissionais diversos nas equipes de desenvolvimento de IA no Judiciário, incluindo parcerias com universidades e organizações da sociedade civil.

- A obrigatoriedade de documentação e registro das medidas adotadas para garantir a diversidade nas equipes, com publicação periódica de relatórios sobre a composição das equipes e seu impacto na mitigação de vieses algorítmicos.

- A elaboração de diretrizes específicas para a implementação prática dos princípios éticos estabelecidos no Art. 36, incluindo metodologias para identificação e mitigação de vieses, protocolos para testes de segurança e procedimentos para avaliação de impacto ético.
- A criação de um comitê de ética em IA em cada tribunal, com participação multidisciplinar, incluindo representantes da advocacia, academia e sociedade civil, para supervisionar a aplicação dos princípios éticos nos projetos de IA.
- A obrigatoriedade de documentação e registro das medidas adotadas para garantir o respeito aos princípios éticos, incluindo relatórios de avaliação de impacto ético para todos os projetos de IA, independentemente de sua classificação de risco.
- O estabelecimento de critérios objetivos para avaliar a "utilidade" das soluções de IA incluindo métricas de desempenho, impacto na eficiência judicial, satisfação dos usuários e conformidade com princípios éticos e jurídicos.

A criação de diretrizes específicas para a transição ou migração de dados quando uma solução for descontinuada, garantindo a preservação da memória institucional e a continuidade dos serviços.

- O detalhamento dos critérios para autorização de modelos de reconhecimento facial ou análise biométrica pelo Comitê Nacional (§2º do Art. 37), incluindo requisitos técnicos específicos, metodologias de teste e validação, e procedimentos de revisão periódica.
- Criação de um repositório público de lições aprendidas com projetos de IA descontinuados, para evitar a repetição de erros e promover a melhoria contínua das soluções.
- O estabelecimento de critérios específicos para avaliação e seleção de ferramentas de mercado ou código aberto, incluindo requisitos de segurança, proteção de dados, transparência, auditabilidade e conformidade.

- Criação de um processo de certificação para ferramentas externas utilizadas no desenvolvimento de IA no Judiciário, com verificação periódica de conformidade e publicação dos resultados.
- A obrigatoriedade de documentação detalhada sobre todas as ferramentas externas utilizadas em cada projeto de IA incluindo versões, configurações, modificações realizadas e avaliações de segurança.
- A obrigatoriedade de documentação detalhada de todo o processo de desenvolvimento de soluções de IA incluindo decisões de design, escolhas técnicas, dados utilizados para treinamento e validação, e resultados de testes.
- A criação de um protocolo de auditoria específico para o desenvolvimento de IA no Judiciário, com verificações em diferentes etapas do ciclo de vida do projeto e publicação dos resultados.
- A obrigatoriedade de publicação de relatórios periódicos sobre o desenvolvimento e implantação de soluções de IA, em linguagem acessível e com detalhamento técnico suficiente para permitir a avaliação por especialistas.
- A criação de mecanismos de participação da sociedade civil no acompanhamento do desenvolvimento de soluções de IA no Judiciário, incluindo consultas públicas, audiências e grupos de trabalho multissetoriais.

## Capítulo XII - Das Disposições Finais (Arts. 43-47)

O Capítulo XII estabelece disposições finais importantes para a implementação da Resolução. O **Art. 43** permite a cooperação técnica com outras instituições para desenvolvimento colaborativo de modelos de IA, desde que observadas as disposições da Resolução, especialmente quanto à proteção de dados e confidencialidade.

O **Art. 45** estabelece um prazo de 12 meses para adequação dos projetos e modelos existentes às novas disposições, a partir da publicação da Resolução.

Este prazo é razoável, mas a efetividade da adequação dependerá do monitoramento e fiscalização pelo CNJ, especialmente no que diz respeito ao uso individual de ferramentas privadas.

O **Art. 47** determina que a Resolução entrará em vigor após 120 dias de sua publicação, revogando a Resolução CNJ nº 332/2020. Este período de *vacatio legis* é importante para permitir a adaptação dos tribunais e demais atores do sistema de justiça às novas regras.

O prazo de 12 meses para adequação dos projetos e modelos existentes (Art. 45) é razoável, mas a efetividade da adequação dependerá do monitoramento e fiscalização pelo CNJ.

#### **Diante do exposto, sugere-se/recomenda-se:**

A criação de um comitê de acompanhamento da implementação da Resolução 615/2025, com participação da advocacia, para monitorar o cumprimento dos requisitos de transparência, auditabilidade, confiabilidade, explicabilidade e supervisão humana efetiva.

A realização de auditorias periódicas independentes sobre o uso de IA no Judiciário, com foco específico na verificação da conformidade com os requisitos de transparência, auditabilidade, confiabilidade, explicabilidade e supervisão humana efetiva.

#### **Conclusão**

A Resolução CNJ nº 615/2025 representa um avanço significativo na regulação do uso de IA no Judiciário brasileiro, estabelecendo princípios, diretrizes e mecanismos de governança importantes. Contudo, a permissão

para uso individual de ferramentas privadas, a facultatividade da menção ao uso de IA nas decisões e as exceções aos requisitos de transparência e auditabilidade suscitam preocupações quanto à efetiva supervisão humana, à transparência, à auditabilidade, à confiabilidade, à explicabilidade e à segurança da informação.

O IAB, como instituição comprometida com o aperfeiçoamento do ordenamento jurídico e a defesa do Estado Democrático de Direito, tem um papel fundamental na proposição de aprimoramentos à Resolução e no monitoramento de sua implementação, garantindo que o uso de IA no Judiciário respeite os princípios constitucionais do devido processo legal, contraditório, ampla defesa e publicidade.

As recomendações apresentadas neste parecer visam contribuir para esse objetivo, promovendo um uso ético, transparente e responsável da IA no sistema de justiça brasileiro, com ênfase na supervisão humana efetiva, na transparência, na auditabilidade, na confiabilidade, na explicabilidade e na segurança da informação, em benefício de todos os jurisdicionados e com respeito aos direitos fundamentais dos cidadãos.

## **RECOMENDAÇÕES**

1. Uso de linguagem simples sob a ótica de linguagem acessível. Inclusão linguagem acessível
2. Que sejam já determinados mecanismos de garantia do respeito pela obrigatoriedade de “revisão humana” e as consequências de não ser respeitada tal imposição, com definição de cominação para os infratores.

3. Definição na norma de mecanismos de monitoramento contínuo para garantir o cumprimento do respeito pelas restrições e imposições legais, os quais ilustram e têm associados -sem exclusão de outros- a existência de padrões de conduta e boas práticas;

4. Não devem ser apenas as “soluções de alto risco” que “deverão ser submetidas a processos regulares de auditoria e monitoramento contínuo para supervisionar seu uso e mitigar potenciais riscos aos direitos fundamentais, à privacidade e à justiça”, mas todas as que estão associadas a uma atividade de risco elevado, como a Justiça. Assim, as soluções de “baixo risco” de desenvolvimento de soluções baseadas em inteligência artificial destinadas a desempenhar ou apoiar o usuário na realização das seguintes atividades acessórias submetidas a processos regulares de auditoria e monitoramento contínuo.

5. A efetiva implementação de mecanismos de verificação, de controle, de monitoramento contínuo, auditoria, o estabelecimento de processos internos aptos a garantir a segurança dos sistemas de IA não estão garantidos pelas regras instituídas pela Resolução 615.

6. Instituir obrigação aos Tribunais de comunicar a possibilidade de ocorrência de eventos adversos antes da aplicação do uso do sistema.

7. Revogar a possibilidade de utilização de licenças privadas por magistrados e servidores - no exercício das funções do seu cargo no Judiciário (art. 16, VI).

8. Tendo em vista que a Ordem dos Advogados do Brasil integra o Conselho Nacional de Justiça através de seus dois representantes é necessário que tenha direito a voto.

9. Efetiva fiscalização da capacitação de magistrados e servidores, assim como a avaliação do conhecimento adquirido.

10. Limitar o uso individual a ferramentas corporativas: O ideal seria limitar o uso individual apenas a ferramentas corporativas desenvolvidas ou contratadas pelos tribunais, que passaram por processos rigorosos de verificação de conformidade.

11. Exigir capacitação prévia: Caso a permissão para uso individual de ferramentas privadas seja mantida, deve-se exigir capacitação prévia obrigatória, com certificação específica.

12. Tornar obrigatória a menção ao uso de IA: A menção ao uso de IA generativa no corpo das decisões judiciais deve ser obrigatória, não facultativa.

13. Estabelecer mecanismos de verificação: Devem ser criados mecanismos concretos para verificar o cumprimento das condições estabelecidas, incluindo auditorias periódicas.

14. Detalhar a regulamentação: O CNJ deve estabelecer diretrizes detalhadas para a regulamentação dos mecanismos de prestação de informações, garantindo uniformidade e efetividade em todos os tribunais.

15. Criação de um programa nacional de letramento digital para magistrados e servidores, com foco específico em transparência, auditabilidade, confiabilidade, explicabilidade e supervisão humana efetiva no uso de IA.

16. Obrigatoriedade de adoção de mecanismos de privacy by design e privacy by default em todas as ferramentas de IA utilizadas no Judiciário, com verificação prévia de conformidade antes de sua utilização.

17. Criação de um protocolo específico para verificação de conformidade das ferramentas de IA com os requisitos de segurança da informação e proteção de dados, a ser aplicado antes de sua utilização, especialmente no caso de ferramentas de uso individual.

18. Obrigatoriedade de registro e documentação de todos os incidentes de segurança envolvendo ferramentas de IA, com comunicação imediata ao CNJ e aos usuários potencialmente afetados.

19. Obrigatoriedade de adoção de mecanismos de explicabilidade em todas as ferramentas de IA utilizadas no Judiciário, com documentação detalhada sobre como as decisões são tomadas e quais fatores são considerados.

20. Criação de um procedimento específico para contestação de decisões judiciais baseadas em IA garantindo o direito ao contraditório e à ampla defesa.

21. Obrigatoriedade de disponibilização, mediante solicitação, de informações detalhadas sobre o funcionamento da ferramenta de IA utilizada em uma decisão judicial específica, garantindo a transparência e a possibilidade de contestação.

22. O aprimoramento dos mecanismos de transparência externa, garantindo que todas as ferramentas de IA utilizadas no Judiciário, sejam devidamente

registradas e documentadas no Sinapses, com informações acessíveis à advocacia e ao público.

23. A criação de um sistema de certificação de conformidade para ferramentas de IA utilizadas no Judiciário, que ateste o cumprimento dos requisitos de transparência, auditabilidade, confiabilidade e explicabilidade, a ser realizado por entidade independente.

24. A obrigatoriedade de relatórios periódicos pelos tribunais sobre o uso de IA incluindo estatísticas sobre o uso individual e seu impacto na transparência e auditabilidade das decisões judiciais.

25. A criação de métricas objetivas para avaliar a diversidade nas equipes de desenvolvimento de IA incluindo indicadores quantitativos e qualitativos que considerem não apenas a composição demográfica, mas também a efetiva participação de diferentes perfis nas decisões críticas.

26. Sugere-se a limitação das hipóteses de dispensa da diversidade (§2º do Art. 35), estabelecendo critérios mais rigorosos e exigindo justificativa detalhada e aprovação prévia pelo Comitê Nacional de IA do Judiciário, especialmente para projetos de alto risco.

27. A criação de um programa de capacitação e inclusão para aumentar a disponibilidade de profissionais diversos nas equipes de desenvolvimento de IA no Judiciário, incluindo parcerias com universidades e organizações da sociedade civil.

28. A obrigatoriedade de documentação e registro das medidas adotadas para garantir a diversidade nas equipes, com publicação periódica de relatórios

sobre a composição das equipes e seu impacto na mitigação de vieses algorítmicos.

29. A elaboração de diretrizes específicas para a implementação prática dos princípios éticos estabelecidos no Art. 36, incluindo metodologias para identificação e mitigação de vieses, protocolos para testes de segurança e procedimentos para avaliação de impacto ético.

30. A criação de um comitê de ética em IA em cada tribunal, com participação multidisciplinar, incluindo representantes da advocacia, academia e sociedade civil, para supervisionar a aplicação dos princípios éticos nos projetos de IA.

31. A obrigatoriedade de documentação e registro das medidas adotadas para garantir o respeito aos princípios éticos, incluindo relatórios de avaliação de impacto ético para todos os projetos de IA, independentemente de sua classificação de risco.

32. O estabelecimento de critérios objetivos para avaliar a "utilidade" das soluções de IA incluindo métricas de desempenho, impacto na eficiência judicial, satisfação dos usuários e conformidade com princípios éticos e jurídicos.

33. A criação de diretrizes específicas para a transição ou migração de dados quando uma solução for descontinuada, garantindo a preservação da memória institucional e a continuidade dos serviços.

34. O detalhamento dos critérios para autorização de modelos de reconhecimento facial ou análise biométrica pelo Comitê Nacional (§2º do Art.

37), incluindo requisitos técnicos específicos, metodologias de teste e validação, e procedimentos de revisão periódica.

35. Criação de um repositório público de lições aprendidas com projetos de IA descontinuados, para evitar a repetição de erros e promover a melhoria contínua das soluções.

36. O estabelecimento de critérios específicos para avaliação e seleção de ferramentas de mercado ou código aberto, incluindo requisitos de segurança, proteção de dados, transparência, auditabilidade e conformidade.

37. Criação de um processo de certificação para ferramentas externas utilizadas no desenvolvimento de IA no Judiciário, com verificação periódica de conformidade e publicação dos resultados.

38. A obrigatoriedade de documentação detalhada sobre todas as ferramentas externas utilizadas em cada projeto de IA incluindo versões, configurações, modificações realizadas e avaliações de segurança.

39. A obrigatoriedade de documentação detalhada de todo o processo de desenvolvimento de soluções de IA incluindo decisões de design, escolhas técnicas, dados utilizados para treinamento e validação, e resultados de testes.

40. A criação de um protocolo de auditoria específico para o desenvolvimento de IA no Judiciário, com verificações em diferentes etapas do ciclo de vida do projeto e publicação dos resultados.

41. A obrigatoriedade de publicação de relatórios periódicos sobre o desenvolvimento e implantação de soluções de IA, em linguagem acessível e com detalhamento técnico suficiente para permitir a avaliação por especialistas.

42. A criação de mecanismos de participação da sociedade civil no acompanhamento do desenvolvimento de soluções de IA no Judiciário, incluindo consultas públicas, audiências e grupos de trabalho multissetoriais.

43. Criação de um comitê de acompanhamento da implementação da Resolução 615/2025, com participação da advocacia, para monitorar o cumprimento dos requisitos de transparência, auditabilidade, confiabilidade, explicabilidade e supervisão humana efetiva.

44. Realização de auditorias periódicas independentes sobre o uso de IA no Judiciário, com foco específico na verificação da conformidade com os requisitos de transparência, auditabilidade, confiabilidade, explicabilidade e supervisão humana efetiva.

## **SUGESTÕES DE ENCAMINHAMENTO**

Em sendo aprovado o parecer sugere-se seu encaminhamento:

. À presidência do Conselho Nacional de Justiça, via correio eletrônico, tendo em vista que a Resolução 615 entrará em vigor no próximo dia 12 de julho de 2025.

. E ao Conselho Federal da OAB, em vista da manifestação para que seus representantes no Conselho Nacional de Justiça tenham direito a voz e a voto no Comitê Nacional de Inteligência Artificial.

**Esse é o parecer.**

Rio de Janeiro, 26 de junho de 2025

Relatores membros da Comissão de Inteligência Artificial e Inovação

**Patrícia Medeiros**

**Ana Amelia Menna Barreto**

**Valéria Ribeiro**

**Pedro Trovão**