RESOLUÇÃO Nº _____

(Aprovada na 9ª Reunião do Grupo de Trabalho, realizada em 12 de dezembro de 2024)

Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário.

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA**, no uso de suas atribuições legais e regimentais,

CONSIDERANDO que a Resolução CNJ nº 332, de 21 de agosto de 2020, estabelece diretrizes sobre a ética, a transparência e a governança na produção e no uso de inteligência artificial no Poder Judiciário;

CONSIDERANDO o acelerado desenvolvimento de tecnologias de inteligência artificial, notadamente por meio de algoritmos que utilizam grandes modelos de linguagem, os quais são capazes de interagir com usuários e oferecer soluções geradas automaticamente;

CONSIDERANDO a imprescindibilidade de regulamentação específica para o emprego de técnicas de inteligência artificial generativa no âmbito do Poder Judiciário, de modo a assegurar que sua utilização esteja em consonância com valores éticos fundamentais, incluindo dignidade humana, respeito aos direitos humanos, não discriminação, transparência e responsabilização;

CONSIDERANDO a importância de promover a autonomia dos tribunais na adoção de tecnologias inovadoras, incentivando práticas que garantam a inovação ética, responsável e segura no uso da inteligência artificial;

CONSIDERANDO os potenciais riscos associados à utilização de inteligência artificial generativa, incluindo ameaças à soberania nacional, à segurança da informação, à privacidade e proteção de dados pessoais, bem como a possibilidade de intensificação de parcialidades e vieses discriminatórios;

CONSIDERANDO que a Resolução CNJ nº 332/2020 foi formulada tendo como foco as soluções computacionais destinadas a auxiliar na gestão processual e na efetividade da prestação jurisdicional disponíveis à época de sua elaboração, e que agora se faz necessário atualizar esse normativo para abarcar novas tecnologias, em especial aquelas conhecidas como inteligências artificiais generativas;

CONSIDERANDO o parecer oferecido pela Comissão Permanente de Tecnologia da Informação e Inovação do Conselho Nacional de Justiça no Procedimento de Controle Administrativo de autos nº 0000416-89.2023.2.00.0000, que destacou a importância da governança adequada no uso de inteligência artificial, em particular a generativa, no Poder Judiciário;

CONSIDERANDO a necessidade de assegurar que o desenvolvimento e a implantação de modelos de inteligência artificial no Poder Judiciário observem critérios éticos de transparência, previsibilidade, auditabilidade e justiça substancial;

CONSIDERANDO que 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;

CONSIDERANDO a relevância de fomentar a colaboração e o compartilhamento de informações sobre o uso de inteligência artificial no Poder Judiciário, com vistas a assegurar a transparência e eficácia na aplicação dessas tecnologias;

CONSIDERANDO a necessidade de respeitar as prerrogativas do Ministério Público, da Defensoria Pública, da Advocacia e dos demais atores do sistema de justiça;

CONSIDERANDO as sugestões recolhidas de magistrados e demais atores do sistema de justiça, da sociedade civil, de especialistas e de instituições públicas e privadas para a atualização da Resolução nº 332/2020 durante audiência pública ocorrida entre os dias 25 e 27 de setembro de 2024;

CONSIDERANDO o relatório do Grupo de Trabalho sobre Inteligência Artificial no Poder Judiciário, instituído pela Portaria CNJ nº 338, de 30 de novembro de 2023, cujo objetivo é realizar estudos e apresentar propostas para a regulamentação do uso de sistemas de inteligência artificial generativa;

CONSIDERANDO a decisão proferida pelo Plenário do Conselho Nacional de Justiça no julgamento do Procedimento de Ato Normativo de autos nº XXXXXXX-XX.XXXX.2.00.0000 na XXª Sessão, realizada em XX de XXXX de XXXX;

RESOLVE:

CAPÍTULO I
DAS DEFINIÇÕES E FUNDAMENTOS PARA O USO DE SOLUÇÕES DE IA NO PODER JUDICIÁRIO

Art. 1º A presente Resolução estabelece normas gerais 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 judiciários de modo seguro, transparente, isonômico e ético, em benefício dos jurisdicionados e com estrita observância de seus direitos fundamentais.

§ 1º A governança das soluções de inteligência artificial (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.

§ 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.

§ 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.

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 judiciários 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;

IX – a curadoria dos dados usados no desenvolvimento e no aprimoramento de inteligência artificial, adotando fontes de dados seguras, rastreáveis e auditáveis, preferencialmente governamentais, permitida a contratação de fontes privadas, desde que atendam aos requisitos de segurança e auditabilidade estabelecidos nesta Resolução ou pelo Comitê Nacional de Inteligência Artificial do Judiciário;

X – a conscientização e a difusão do conhecimento sobre as soluções que adotam técnicas de inteligência artificial, com capacitação contínua dos seus usuários sobre as suas aplicações, os seus mecanismos de funcionamento e os seus riscos;

XI – a garantia da segurança da informação e da segurança cibernética.

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 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.

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 fornecido e gera 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 e assistentes técnicos;

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*;

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.

CAPÍTULO II

DO RESPEITO AOS DIREITOS FUNDAMENTAIS

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 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.

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.

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, com mecanismos adequados de supervisão e 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.

Art. 8º As decisões judiciais apoiadas em ferramentas de inteligência artificial devem preservar a igualdade, a não-discriminação abusiva ou ilícita e a pluralidade, assegurando que os sistemas de IA auxiliem no julgamento justo e contribuam para eliminar ou minimizar a marginalização do ser humano e os erros de julgamento decorrentes de preconceitos.

§ 1º Deverão ser implementadas medidas preventivas para evitar o surgimento de vieses discriminatórios, incluindo a validação contínua das soluções de IA e a auditoria ou monitoramento de suas decisões ao longo de todo o ciclo de vida da aplicação, para garantir que as soluções de IA continuem em conformidade com os princípios da igualdade, pluralidade e não discriminação, com relatórios periódicos que avaliem o impacto das soluções no julgamento justo, imparcial e eficiente.

§ 2º Verificado viés discriminatório ou incompatibilidade da solução de inteligência artificial com os princípios previstos nesta Resolução, deverão ser adotadas as medidas corretivas necessárias, incluindo a suspensão temporária, correção ou, se necessário, eliminação definitiva da solução ou de seu viés.

§ 3º Caso se constate a impossibilidade de eliminação do viés discriminatório, a solução de inteligência artificial deverá ser descontinuada, com o consequente cancelamento do registro de seu projeto no Sinapses, e relatório das medidas adotadas e das razões que justificaram a decisão, que poderá ser submetido à análise independente para realização de estudos, se for o caso.

CAPÍTULO III
DA CATEGORIZAÇÃO DOS RISCOS

Art. 9º Os tribunais deverão realizar avaliação das soluções que utilizem técnicas de inteligência artificial, com a finalidade de definir o seu grau de risco, baseando-se na categorização e nos critérios previstos neste Capítulo e no Anexo de Classificação de Riscos, com base em fatores como o potencial impacto nos direitos fundamentais, a complexidade do modelo, a sua sustentabilidade financeira, os usos pretendidos e potenciais e a quantidade de dados sensíveis utilizados.

§ 1º A avaliação deverá ser realizada pelo Tribunal desenvolvedor ou contratante da solução, preferencialmente durante o período de testes e homologação, ou, no caso de aplicações de baixo risco, no início da entrada em produção interna da solução de IA, de acordo com diretrizes claras e critérios objetivos que garantam uniformidade na avaliação de risco, previamente à disponibilização da solução na PDPJ-Br.

§ 2º O Comitê Nacional de Inteligência Artificial do Judiciário poderá fixar as diretrizes e critérios de avaliação de risco a que se refere o § 1º, ouvidos os tribunais, desenvolvedores e a sociedade civil.

§ 3º O Comitê Nacional de Inteligência Artificial do Judiciário poderá, de ofício ou mediante provocação fundamentada, determinar a reclassificação do grau de risco de determinada solução, bem como determinar, de forma justificada, a realização de avaliação de impacto algorítmico, quando tal medida se demonstrar proporcional, respeitada tanto quanto possível a autonomia dos tribunais.

Art. 10. São vedados ao Poder Judiciário, por acarretarem risco excessivo à segurança da informação, aos direitos fundamentais dos cidadãos ou à independência dos magistrados, o desenvolvimento e a utilização de soluções:

I – que não possibilitem a revisão humana dos dados utilizados e dos resultados propostos ao longo de seu ciclo de treinamento, desenvolvimento e uso, ou que gerem dependência absoluta do usuário em relação ao resultado proposto, sem possibilidade de alteração ou revisão;

II – que valorem traços da personalidade, características ou comportamentos de pessoas naturais ou de grupos de pessoas naturais, para fins de avaliar ou prever o cometimento de crimes ou a probabilidade de reiteração delitiva na fundamentação de decisões judiciais;

III – que classifiquem ou ranqueiem pessoas naturais, com base no seu comportamento ou situação social ou ainda em atributos da sua personalidade, para a avaliação da plausibilidade de seus direitos, méritos judiciais ou testemunhos;

IV – a identificação e a autenticação de padrões biométricos para o reconhecimento de emoções.

§ 1º Os tribunais deverão implementar mecanismos de monitoramento contínuo para garantir o cumprimento dessas vedações e monitorar o desenvolvimento de soluções de IA a fim de prevenir o uso inadvertido das tecnologias proibidas.

§ 2º Qualquer solução de IA que, ao longo de seu uso, se enquadrar nas vedações deste artigo, deverá ser descontinuada, com registro no Sinapses das razões e providências adotadas, para análise pelo Comitê Nacional de Inteligência Artificial do Judiciário, com fins de buscar prevenir outros casos.

Art. 11. Consideram-se de alto ou baixo risco, conforme o caso, as soluções que utilizem técnicas de inteligência artificial desenvolvidas e utilizadas para as finalidades e contextos descritos no Anexo de Classificação de Riscos desta Resolução.

§ 1º As soluções de alto risco 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.

§ 2º A categorização disposta no Anexo de Classificação de Riscos para soluções de alto risco será revista pelo menos anualmente pelo Comitê Nacional de Inteligência Artificial do Judiciário, na forma do art. 16, I, desta Resolução, para assegurar que a classificação de contextos de alto risco permaneça atualizada e continue adequada às exigências legais e éticas.

§ 3º As soluções de baixo risco deverão ser monitoradas e revisadas periodicamente, para assegurar que permanecem dentro dos parâmetros de baixo risco e que eventuais mudanças tecnológicas ou contextuais não alteraram essa categorização.

CAPÍTULO IV
DAS MEDIDAS DE GOVERNANÇA

Art. 12. O Tribunal desenvolvedor ou contratante deverá estabelecer processos internos aptos a garantir a segurança dos sistemas de inteligência artificial, incluindo, ao menos:

I – medidas de transparência quanto ao emprego e à governança dos sistemas de IA, com a publicação de relatórios que detalhem o funcionamento dos sistemas, suas finalidades, dados utilizados e mecanismos de supervisão;

II – a mitigação e prevenção 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;

III – 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;

IV – 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;

V – 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.

VI – 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.

Art. 13. Antes de ser colocada em produção, a solução que utilize modelos de inteligência artificial de alto risco deverá adotar as seguintes medidas de governança:

I – 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*), 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;

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.

Art. 14. O Tribunal desenvolvedor ou contratante deverá promover avaliação de impacto algorítmico da solução classificada na avaliação como de alto risco, nos termos do art. 11 desta Resolução.

§1º A avaliação de impacto algorítmico consistirá em processo contínuo e executado conforme as diretrizes técnicas e os requisitos formulados previamente pelo Comitê Nacional de Inteligência Artificial do Judiciário, incluindo auditorias regulares, monitoramento contínuo, revisões periódicas e a adoção de ações corretivas quando necessário.

§2º 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.

CAPÍTULO V
DA SUPERVISÃO E IMPLEMENTAÇÃO

Art. 15. Fica instituído o Comitê Nacional de Inteligência Artificial do Judiciário.

§ 1º O Comitê será formado por 13 membros titulares e 13 suplentes, divididos por categoria e designados por ato do Presidente do CNJ, a partir das seguintes indicações:

I – dois Conselheiros do CNJ, sendo ao menos um deles membro da Comissão Permanente de Tecnologia da Informação;

II – dois juízes auxiliares e dois servidores com experiência na área do CNJ;

III – dois magistrados, sendo um representante do Conselho da Justiça Federal e um representante do Conselho Superior da Justiça do Trabalho

IV – quatro desembargadores, sendo um representante de tribunal de justiça, um representante de tribunal regional federal, um representante de tribunal regional do trabalho e um representante de tribunal eleitoral;

V – quatro magistrados, escolhidos a partir de indicações da AMB, ANAMATRA e AJUFE;

VI – dois representantes das escolas da magistratura, sendo um da Escola Nacional de Formação e Aperfeiçoamento de Magistrados (ENFAM) e um da Escola Nacional de Formação e Aperfeiçoamento de Magistrados do Trabalho (ENAMAT);

VII – dois representantes da Ordem dos Advogados do Brasil;

VIII – dois representantes do Ministério Público;

IX – dois representantes da Defensoria Pública;

X – dois especialistas em inteligência artificial e tecnologia da informação, com notório saber e atuação reconhecida em desenvolvimento ou sustentação de IA.

§ 2º A presidência do Comitê, que terá voto de desempate, caberá ao Conselheiro designado pelo Plenário do CNJ, cabendo ao outro Conselheiro a vice-presidência.

§ 3º Em casos de comprovada urgência, poderão ser exaradas medidas pelo Presidente do Comitê Nacional de Inteligência Artificial do Judiciário *ad referendum* da composição plena do Comitê.

§ 4º As decisões, manifestações ou processos do Comitê Nacional de Inteligência Artificial do Judiciário poderão ser submetidos ao Plenário do Conselho Nacional de Justiça, nos termos do art. 98 de seu regimento interno, que, no exercício de sua competência originária, poderá decidir, ratificar, reformar, avocar ou arquivar atos, processos ou expedientes relativos às competências atribuídas ao Comitê nesta Resolução.

Art. 16. Compete ao Comitê Nacional de Inteligência Artificial do Judiciário:

I – avaliar a necessidade de atualização das hipóteses de categorização de riscos referidas no art. 11 e dispostas no Anexo de Classificação de Riscos desta Resolução, com base em critérios objetivos e conforme as melhores práticas internacionais;

II – reclassificar determinados sistemas contratados ou desenvolvidos pelos tribunais, nos termos do § 3º do art. 9º desta Resolução, com a devida justificativa e a publicação de relatório técnico de reclassificação, mediante provocação.

III – estabelecer normas e diretrizes negociais para o sistema Sinapses, incluindo normas de governança, transparência, auditoria e monitoramento;

IV – consolidar padrões de governança e mapeamento de riscos conhecidos e não conhecidos que permitam a definição e a reavaliação contínua do grau de risco adequado para cada hipótese de aplicação, ouvidos os tribunais, especialistas externos e a sociedade civil;

V – recomendar que o CNJ celebre e realize convênios e acordos de cooperação com outros órgãos nacionais e internacionais, visando à melhoria contínua dos sistemas de IA e à incorporação das melhores práticas globais;

VI – vedar ou limitar o uso, de ofício ou mediante provocação, de soluções de IA disponíveis no mercado, gratuitas ou não, que poderão ser utilizadas pelos magistrados e servidores do Poder Judiciário, por meio de licença privada, considerando em particular as condições de uso dos dados pessoais e dos dados para treinamento, os critérios de segurança e o grau de risco das aplicações, estabelecendo regras adicionais de governança e monitoramento, caso necessário, nos termos desta Resolução;

VII – monitorar a oferta pelos tribunais de capacitação e treinamento em inteligência artificial aos seus magistrados e servidores, bem como solicitar ou sugerir à Escola Nacional de Formação e Aperfeiçoamento de Magistrados (ENFAM) e à Escola Nacional de Formação e Aperfeiçoamento de Magistrados do Trabalho (ENAMAT) que desenvolvam parâmetros curriculares e ações voltadas à capacitação e ao treinamento em inteligência artificial.

§ 1º A avaliação periódica de que trata o inciso I, que poderá ser feita no relatório previsto no art. 18 e publicada, deverá contemplar, além de outros pontos que se mostrem relevantes para a administração da justiça, para a razoável duração do processo e para a garantia de direitos fundamentais:

I – a análise geral das soluções cadastradas no Sinapses e das soluções descontinuadas, descartadas ou vedadas no ano corrente, com a publicação de relatórios que poderão trazer conclusões e recomendações;

II – a necessária harmonização com a legislação e com os atos normativos do Conselho Nacional de Justiça, em especial as normas relativas à proteção de dados e ao uso da inteligência artificial;

III – a análise das novas tecnologias e inovações que possam influenciar a eficácia e a adequação das normas existentes, com a inclusão de recomendações para ajustes normativos;

IV – a verificação de situações em que as regras vigentes se mostrarem insuficientes para o controle dos riscos associados ao uso de inteligência artificial no âmbito do Poder Judiciário, com encaminhamentos para correção das lacunas identificadas.

§ 2º A vedação ou limitação para o uso de soluções baseadas em modelos de linguagem de larga escala (LLMs) e outros sistemas de inteligência artificial generativa (IAGen) a que se refere o inciso VI do *caput* deste artigo terá como critério eventual descumprimento ou fundado receio de risco de descumprimento das diretrizes dispostas no § 3º do art. 19 desta Resolução, e poderá limitar o uso de determinada ferramenta apenas a soluções de baixo risco ou determinar providências relativas ao uso de dados, assegurada a possibilidade de rever eventual decisão previamente tomada, se as condições ou os termos de uso da solução forem modificados.

Art. 17. Para embasar a avaliação de atualização das hipóteses de categorização de riscos, o Comitê Nacional de Inteligência Artificial do Judiciário considerará as diretrizes dispostas nesta Resolução, além dos seguintes critérios:

I – impacto negativo comprovado no exercício de direitos e liberdades fundamentais ou na utilização de serviços essenciais;

II – alto potencial danoso de ordem material ou moral, devidamente mensurado, incluindo discriminação ilegal ou abusiva, direta ou indireta;

III – repercussão significativa sobre pessoas pertencentes a grupos vulneráveis, levando em conta suas condições sociais, econômicas e culturais;

IV – irreversibilidade ou difícil reversão de possíveis resultados prejudiciais da solução, especialmente em casos que afetem diretamente direitos materiais ou processuais, ou que provoquem movimentação automática relevante em processos judiciais;

V – histórico de responsabilização civil ou administrativa em decorrência da potencial violação a direitos morais ou materiais dos usuários externos pela solução de inteligência artificial, devidamente documentado e analisado em relatórios técnicos;

VI – baixo grau de transparência, de explicabilidade e de auditabilidade da solução, com critérios objetivos que dificultem ou impossibilitem seu controle, supervisão e revisão pelas partes eventualmente interessadas;

VII – alto nível de identificabilidade dos titulares dos dados, especialmente quando o tratamento envolve combinação, correspondência ou comparação de dados de várias fontes, com impacto direto na privacidade e na proteção dos dados pessoais.

§ 1º A avaliação de risco deverá ser acompanhada de indicadores de desempenho e relatórios de auditoria ou de monitoramento, a fim de garantir a efetividade das medidas de mitigação de riscos.

§ 2º Sempre que constatada a baixa transparência ou explicabilidade de uma solução de IA, medidas corretivas deverão ser adotadas assim que possível, incluindo eventualmente a descontinuidade da solução, caso as correções não sejam viáveis.

Art. 18. O Comitê Nacional de Inteligência Artificial do Judiciário confeccionará relatório circunstanciado de sua avaliação anual, contendo:

I – as metodologias e critérios utilizados na avaliação das soluções de inteligência artificial;

II – os resultados das auditorias, monitoramentos e avaliações de impacto algorítmico realizadas;

II – a atualização das hipóteses de categorização de riscos dispostas no Anexo de Classificação de Riscos desta Resolução, quando for o caso;

IV – recomendações para a correção de falhas ou a melhoria das soluções de inteligência artificial em uso, conforme identificado nas auditorias, monitoramentos ou avaliações;

V – panorama do estado da utilização de inteligência artificial generativa no Judiciário brasileiro.

§ 1º O relatório será publicado e disponibilizado ao público em geral, garantindo a transparência do processo de avaliação e acompanhamento das soluções de IA utilizadas no Judiciário.

§ 2º O Comitê poderá propor revisões extraordinárias a qualquer momento, caso sejam identificadas mudanças tecnológicas significativas ou novas informações que justifiquem uma reavaliação dos riscos associados às soluções de IA em uso.

CAPÍTULO VI
DO USO E DA CONTRATAÇÃO DE MODELOS DE LINGUAGEM DE LARGA ESCALA (LLMs) E DE OUTROS SISTEMAS DE IA GENERATIVA (IAGen)

Art. 19. Os modelos de linguagem de larga escala (LLMs), de pequena escala (SLMS) e outros sistemas de inteligência artificial generativa (IAGen) disponíveis na rede mundial de computadores poderão ser utilizados pelos magistrados e pelos servidores do Poder Judiciário

em suas respectivas atividades como ferramentas de auxílio à gestão ou de apoio à decisão, em obediência aos padrões de segurança da informação e às normas desta Resolução.

§ 1º Os modelos e soluções a que se refere o caput poderão ser utilizados pelos magistrados e pelos servidores do Poder Judiciário, preferencialmente, por meio de acesso que seja habilitado, disponibilizado e monitorado pelos tribunais.

§ 2º Quando o Tribunal não oferecer solução corporativa de inteligência artificial especificamente treinada e personalizada para uso no Poder Judiciário, será facultado ao magistrado, servidor ou colaborador do Poder Judiciário a contratação direta de solução mediante assinatura ou cadastro de natureza privada, desde que atendidas as diretrizes do § 3º deste artigo.

§ 3º A contratação direta para uso privado ou individual dos modelos de linguagem de larga escala (LLMs) e outros sistemas de inteligência artificial generativa (IAGen) disponíveis na rede mundial de computadores, deverá observar as seguintes condições:

I – os usuários deverão realizar capacitação e treinamentos específicos sobre as limitações, os riscos e o uso ético, responsável e eficiente de LLMs e dos sistemas de IA generativa para a utilização em suas atividades, ficando a cargo dos tribunais e de suas escolas a promoção dos treinamentos continuados aos magistrados e servidores;

II – 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;

III – 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;

IV – é vedado o uso de LLMs e sistemas de IA generativa de natureza privada ou externos ao Judiciário para processar, analisar, gerar conteúdo ou tomar 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;

V – 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.

§ 4º O Comitê Nacional de Inteligência Artificial do Judiciário elaborará e atualizará periodicamente um manual de boas práticas para orientar magistrados e servidores sobre o uso correto, ético e eficiente de LLMs e de sistemas de IA generativa, abordando aspectos como suas potencialidades, limitações, configurações recomendadas, riscos, casos de uso adequados e vedados, orientações para interpretação crítica dos resultados e correção de eventuais erros ou inconsistências.

§ 5º Caberá aos tribunais e às suas escolas, em consonância com as diretrizes do Conselho Nacional de Justiça, da Escola Nacional de Formação e Aperfeiçoamento de Magistrados (ENFAM) e da Escola Nacional de Formação e Aperfeiçoamento de Magistrados do Trabalho (ENAMAT), promover capacitação e treinamentos continuados para assegurar o uso adequado e responsável de LLMs e sistemas de IA generativa pelos magistrados e servidores, bem como para mantê-los atualizados quanto à evolução dessas tecnologias e suas implicações para o sistema de Justiça.

§ 6º Quando houver emprego de IA generativa para auxílio à redação de ato judicial, tal situação poderá ser mencionada no corpo da decisão, a critério do magistrado, sendo porém devido o registro automático no sistema interno do Tribunal, para fins de produção de estatísticas, monitoramento e eventual auditoria.

§ 7º Na hipótese do § 2º deste artigo, o magistrado ou gestor que contratar solução de mercado de inteligência artificial para uso em suas atividades no Poder Judiciário, ou que tiver em sua equipe servidor ou colaborador que utilize essas soluções, deverá prestar informações periodicamente à Corregedoria local sobre sua utilização, na forma do regulamento.

§ 8º As Corregedorias 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.

Art. 20. A contratação de modelos de linguagem de larga escala (LLMs) e outros sistemas de inteligência artificial generativa (IAGen) pelos tribunais deverá cumprir as seguintes diretrizes:

I – a empresa contratada deve se comprometer a respeitar a legislação vigente no Brasil, entre elas, a Lei Complementar nº 35, de 14 de março de 1979 (Lei Orgânica da

Magistratura Nacional – LOMAN), a Lei Geral de Proteção de Dados Pessoais, a Lei nº 9.279, de 14 de maio de 1996 (Lei de Propriedade Intelectual – LPI) e esta Resolução;

II – o uso dos dados fornecidos pelos usuários do Poder Judiciário para treinamento fica condicionado às bases legais da Lei Geral de Proteção de Dados Pessoais e não poderá ser utilizado para quaisquer outros fins não expressamente autorizados, com realização de monitoramento contínuo para assegurar a conformidade com as diretrizes de proteção de dados e de propriedade intelectual;

III – é dever dos tribunais contratantes e de suas escolas, da magistratura e de servidores, oferecer treinamento aos usuários internos de LLMs e de sistemas de inteligência artificial generativa sobre as limitações, os riscos e o uso ético, responsável e eficiente dessas soluções antes de utilizá-los em suas atividades;

IV – o uso dessas ferramentas será de caráter auxiliar e complementar, 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;

V – é vedado o uso de LLMs e sistemas de IA generativa para processar, analisar, gerar conteúdo ou tomar decisões a partir de documentos ou dados sigilosos ou protegidos por segredo de justiça, exceto quando devidamente anonimizados na origem, em consonância com a Lei Geral de Proteção de Dados Pessoais, nos termos da legislação aplicável;

VI – é vedado o uso de LLMs e sistemas de IA generativa privados 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;

VII – as empresas contratadas devem resguardar o sigilo das informações compartilhadas pelos tribunais contratantes, respeitar e comprovar utilização de normas de segurança atuais e compatíveis com o estado da arte, podendo ser exigida auditoria externa ou relatórios periódicos sobre a segurança dos dados e sua conformidade;

VIII – os sistemas contratados devem oferecer documentação e referências bibliográficas atualizadas, sempre que disponíveis, de acordo com o uso do seu resultado;

IX – os sistemas contratados deverão adotar mecanismos de *privacy by design* (privacidade desde a concepção) e *privacy by default* (privacidade por padrão), incluindo a possibilidade de não-armazenamento ou eliminação do histórico de perguntas e *prompts*, podendo ser exigido relatório com indicadores claros para avaliar sua implementação e cumprimento.

Parágrafo único. É vedada a utilização de dados sigilosos ou protegidos por segredo de justiça para treinamento de modelos de inteligência artificial.

Art. 21. Os sistemas de processo judicial eletrônico que utilizem soluções de inteligência artificial deverão indicar, em sua interface principal, a relação dos modelos em uso, sua versão e código de registro no Sinapses e a data da última atualização dessas informações.

§ 1º A revisão e atualização dessas informações ocorrerão com periodicidade mínima de doze meses ou sempre que houver alteração significativa nos modelos ou em suas versões.

§ 2º Os produtos elaborados de forma automatizada por solução de inteligência artificial deverão registrar a utilização de IA nos *logs* de uso do sistema por meio de rótulos de identificação adequados e compreensíveis, para fins de estatística, monitoramento e eventual auditoria.

CAPÍTULO VII
TRANSPARÊNCIA E REGISTRO NO SINAPSES

Art. 22. Qualquer modelo de inteligência artificial que venha a ser adotado pelos órgãos do Poder Judiciário deverá observar as regras de governança de dados aplicáveis aos seus próprios sistemas computacionais, as Resoluções e as Recomendações do Conselho Nacional de Justiça, a Lei Geral de Proteção de Dados Pessoais, a Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI), a propriedade intelectual e o segredo de justiça.

§ 1º A conformidade com essas regras deverá ser assegurada contratualmente, garantida por meio de monitoramento contínuo e eventual auditoria, com foco na proteção de dados, na propriedade intelectual e na transparência dos modelos de IA adotados.

§ 2º O uso dos modelos de inteligência artificial no âmbito do Judiciário deverá ser acompanhado de relatórios periódicos, que comprovem a conformidade com as diretrizes de governança de dados, em particular os sensíveis, transparência e proteção à propriedade intelectual.

§ 3º Os modelos de inteligência artificial adotados deverão possuir mecanismos de explicabilidade, sempre que tecnicamente possível, de modo que suas decisões e operações sejam compreensíveis e auditáveis pelos operadores judiciais.

Art. 23. Os órgãos do Poder Judiciário envolvidos em projeto de inteligência artificial deverão:

I – informar ao Conselho Nacional de Justiça por meio da plataforma Sinapses a conclusão da pesquisa ou estudo, o início do desenvolvimento e a entrada em produção da solução de inteligência artificial, bem como os respectivos objetivos e os resultados que se pretende alcançar;

II – promover esforços para atuação em modelo comunitário, com desestímulo ao desenvolvimento paralelo por um tribunal quando a iniciativa possuir objetivos e resultados pretendidos idênticos e compatíveis com modelo ou sistema de inteligência artificial já existente em outro tribunal;

III – o depósito do código-fonte, bases de dados e demais partes da solução de IA poderão ser dispensados, sempre que as licenças de proteção ao direito autoral e à propriedade intelectual limitem seu compartilhamento público. Nesse caso, o Tribunal deverá indicar quais sistemas, motores, bases de dados, LLMs e demais elementos utilizados na solução de IA, acompanhados de suas respectivas versões e fornecedores.

Art. 24. As soluções que adotam técnicas de inteligência artificial, tanto em desenvolvimento quanto em uso no Poder Judiciário, deverão ser cadastradas no Sinapses, que manterá um catálogo de sistemas de IA no Judiciário brasileiro e organizado conforme a categorização de risco da solução, na forma do Anexo de Classificação de Riscos desta Resolução.

§ 1º Também deverá ser incluído no Sinapses o sumário público da avaliação de impacto algorítmico a que se refere o 14, quando as soluções forem classificadas como de alto risco.

§ 2º O sumário público poderá omitir dados sensíveis, sigilosos ou protegidos por propriedade intelectual, assegurando a proteção da privacidade e da confidencialidade das informações.

§ 3º Para as soluções de baixo risco, o cadastro no Sinapses deverá ser realizado pelo tribunal responsável antes da entrada em produção da solução, com as informações mínimas necessárias, como finalidade, criação própria ou colaborativa, se a ferramenta é contratada ou desenvolvida internamente e a descrição dos objetivos.

§ 4º Para as soluções de alto risco, o cadastro no Sinapses poderá ser realizado após os estudos preliminares, mas necessariamente antes do início do desenvolvimento.

§ 5º As informações cadastradas deverão ser complementadas e atualizadas conforme a evolução do desenvolvimento da solução, sendo obrigatória a atualização a cada nova fase ou versão relevante das soluções de alto risco.

§ 6º O Conselho Nacional de Justiça deverá prover a Plataforma Sinapses com a estrutura necessária para recepcionar os cadastros realizados pelos tribunais, sendo dispensado o depósito de grandes bases de dados ou de modelos protegidos por propriedade intelectual.

Art. 25. O Conselho Nacional de Justiça publicará, em área própria de seu sítio na rede mundial de computadores, a 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, acompanhada de explicações acessíveis sobre as implicações da classificação de risco.

§ 1º As informações deverão ser atualizadas periodicamente, com revisão obrigatória a cada doze meses ou sempre que houver alteração significativa nas aplicações, seja por evolução do software, mudanças no grau de risco ou descontinuidade.

§ 2º A relação deverá indicar de forma clara os critérios utilizados para a classificação de risco, bem como qualquer situação de descontinuidade ou suspensão de uso das aplicações.

§ 3º O Conselho Nacional de Justiça poderá retirar do catálogo aplicações descontinuadas ou suspensas, desde que isso seja comunicado publicamente, com justificativa.

CAPÍTULO VIII
QUALIDADE E SEGURANÇA

Art. 26. Os dados utilizados no processo de desenvolvimento de soluções de inteligência artificial deverão ser preferencialmente provenientes de fontes públicas ou governamentais, e serão objeto de curadoria de qualidade, particularmente quando desenvolvidos internamente, e em qualquer caso, respeitando as diretrizes da Lei Geral de Proteção de Dados Pessoais.

§ 1º Consideram-se fontes seguras para a obtenção de dados aquelas que possuam mecanismos de validação e curadoria de dados, garantindo a sua precisão, equilíbrio, integridade e confiabilidade. Quando dados de fontes não governamentais forem utilizados, deverá ser realizada uma verificação rigorosa da qualidade e segurança dos dados.

§ 2º A utilização de dados provenientes de fontes não governamentais será permitida em casos em que os dados governamentais forem insuficientes ou inadequados para o objetivo específico da solução de inteligência artificial, desde que esses dados sejam validados conforme os critérios estabelecidos neste artigo.

§ 3º No caso de soluções contratadas pelos tribunais, as fornecedoras de serviços devem garantir contratualmente o respeito às diretrizes da Lei Geral de Proteção de Dados Pessoais.

§ 4º Deverão ser coletados apenas os dados estritamente necessários ao treinamento, não devendo ser mantidos conjunto de dados sem uso ou controle quanto ao armazenamento.

Art. 27. O sistema deverá impedir que os dados recebidos sejam alterados antes de sua utilização no fluxo de desenvolvimento de soluções de inteligência artificial, por meio de mecanismos de controle de versões, *tokens* e registros para auditoria e monitoramento que garantam a integridade e rastreabilidade dos dados.

§ 1º Deverá ser mantida uma cópia de cada conjunto de dados (*dataset*) utilizado em versões relevantes dos modelos desenvolvidos, garantindo que os dados possam ser auditados e revisados quando necessário.

§ 2º As cópias dos *datasets* deverão ser armazenadas de forma segura, com a utilização de criptografia e controle de acesso, conforme as diretrizes da Lei Geral de Proteção de Dados Pessoais, para assegurar a proteção contra acessos não autorizados e demais riscos à segurança da informação.

§ 3º Na hipótese de mostrar-se inviável a manutenção por longo prazo de todos os *datasets* das versões relevantes do sistema, em virtude de suas dimensões, o Tribunal poderá estabelecer um plano de eliminação desses arquivos, conforme tabela de temporalidade adequada ao impacto algorítmico da solução, sendo garantida a manutenção de *dataset* anteriormente utilizado por, no mínimo, um ano após sua obsolescência ou modificação.

Art. 28. O armazenamento e a execução das soluções de inteligência artificial, operadas em datacenters próprios, provedores de serviço de nuvem ou por meio de APIs (interfaces de programação de aplicações), devem garantir o isolamento dos dados compartilhados pelo Tribunal, utilizando mecanismos de segurança adequados, como criptografia e segregação de ambientes.

§ 1º O isolamento deverá assegurar que os dados do Tribunal não sejam acessados, manipulados ou utilizados por terceiros sem autorização, garantindo a privacidade e a segurança das informações.

§ 2º Os provedores de serviços de nuvem e APIs deverão estar em conformidade com a legislação brasileira, incluindo a Lei Geral de Proteção de Dados Pessoais, e adotar as melhores práticas de segurança da informação para proteger os dados do Tribunal.

Art. 29. Os dados armazenados no processo de desenvolvimento e execução de soluções de inteligência artificial devem ser protegidos de forma eficaz contra os riscos de destruição, modificação, extravio ou acessos e transmissões não autorizados, por meio de medidas técnicas e administrativas adequadas.

§ 1º A proteção dos dados deve incluir a implementação de criptografia, controle de acesso baseado em permissões, auditorias regulares e monitoramento para identificar e mitigar possíveis ameaças à segurança.

§ 2º As práticas de proteção de dados deverão estar em conformidade com a Lei Geral de Proteção de Dados Pessoais e com as normativas de segurança da informação aplicáveis, assegurando a privacidade e a integridade dos dados.

§ 3º O uso de ferramentas de monitoramento contínuo e proativo e de prevenção de incidentes será adotado para garantir uma resposta ágil a qualquer tentativa de violação da segurança dos dados.

Art. 30. Nos casos em que o uso de soluções de inteligência artificial, se dê diretamente por meio de sítios eletrônicos, aplicativos ou APIs (interfaces de programação de aplicações) que utilizem os dados compartilhados para alimentar o repositório central ou para fins de treinamento ou (re)adequação do modelo, é vedado o compartilhamento de dados custodiados pelo Judiciário, exceto quando esses dados forem anonimizados na origem, em conformidade com a Lei Geral de Proteção de Dados Pessoais, e as melhores práticas de segurança de dados.

§ 1º Considera-se anonimização na origem o processo técnico de eliminação da possibilidade de associação, direta ou indireta, entre os dados pessoais e uma pessoa natural identificável, realizado antes que os dados sejam transmitidos ou processados pela solução de IA.

§ 2º Deverão ser adotados mecanismos de auditoria e controle para verificar e garantir a conformidade das soluções de IA com as normas de proteção de dados,

especialmente no uso de dados para fins de treinamento ou readequação de modelos de inteligência artificial.

Art. 31. O armazenamento e a execução dos modelos de inteligência artificial deverão ocorrer em ambientes que atendam a padrões consolidados de segurança da informação, na forma deste artigo.

Parágrafo único. Consideram-se boas práticas para atendimento ao que dispõe o caput deste artigo:

I – 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;

II – implementação de controles de acesso rigorosos, criptografia de dados em repouso e em trânsito e políticas de gerenciamento de vulnerabilidades nos ambientes de armazenamento e execução;

III – instituição de política de governança de dados que busque:

a) educar continuamente a equipe sobre práticas de segurança da informação e privacidade;

b) ao final do treinamento dos modelos, eliminar os dados pessoais não-anonimizados dos repositórios de dados (*data lake*, *data warehouse* ou *data lakehouse*), observados o art. 26, § 4º, e o art. 27, § 3º, desta Resolução;

c) manter apenas os dados tokenizados estritamente necessários ao modelo, fazendo a guarda dos últimos *datasets* aprovados em local que observe a segurança da informação, observados o art. 26, § 4º, e o art. 27, § 3º, desta Resolução;

d) implementar a governança e curadoria dos dados utilizados, para garantir sua qualidade e segurança;

e) realizar monitoramento contínuo e eventualmente auditorias nos modelos em testes e aprovados para garantir a obediência aos padrões de segurança e privacidade;

f) garantir que modelos fiquem funcionais durante todo o ciclo de vida das soluções de IA, removendo-os quando se identifique sua inutilidade ou obsolescência.

IV – adoção como referência, tanto quanto possível, de normas internacionais reconhecidas, tais como a ISO/IEC (Organização Internacional de Padronização/Comissão Eletrotécnica Internacional) 42001, a série ISO/IEC 27000 e as do NIST (*National Institute of*

Standards and Technology), ou as que vierem a sucedê-las, além das regulamentações locais aplicáveis.

CAPÍTULO IX
DO CONTROLE DO USUÁRIO

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.

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 no § 6º do art. 19 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.

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.

CAPÍTULO X
DA PESQUISA, DO DESENVOLVIMENTO E DA IMPLANTAÇÃO DE SERVIÇOS DE INTELIGÊNCIA ARTIFICIAL

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 de diferentes perfis de gênero e etnia, 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.

Art. 36. A realização de estudos, pesquisas, ensino e treinamentos de inteligência artificial deve ser livre de preconceitos, devendo para tanto:

I – respeitar a dignidade e a liberdade de pessoas ou grupos envolvidos em suas atividades, evitando práticas de discriminação, assédio ou exclusão;

II – coibir atividades que envolvam qualquer forma de risco ou prejuízo aos seres humanos, como testes inseguros ou a manipulação de dados sensíveis sem consentimento,

ou ainda o uso indiscriminado ou malicioso de dados que possam comprometer a equidade das decisões;

III – identificar e evitar sectarismos ou vieses que possam direcionar o curso da pesquisa ou seus resultados, comprometendo a objetividade ou a imparcialidade dos estudos.

Art. 37. Concluída a pesquisa e iniciado o desenvolvimento de soluções que utilizem modelos de inteligência artificial, os tribunais deverão cadastrar a iniciativa no Sinapses, na forma do art. 23 desta Resolução, e velar por sua continuidade enquanto for útil à execução das suas atividades.

§ 1º As atividades descritas no *caput* deste artigo serão encerradas quando, mediante manifestação fundamentada, for reconhecida sua desconformidade com os preceitos estabelecidos nesta Resolução ou em outros atos normativos aplicáveis ao Poder Judiciário e for inviável sua readequação.

§ 2º A utilização de modelos de inteligência artificial que empreguem técnicas de reconhecimento facial ou de análise biométrica que configurem aplicações de alto risco, nos termos do Anexo de Classificação de Risco, item AR5, requererá autorização prévia do Comitê Nacional de Inteligência Artificial do Judiciário para o seu desenvolvimento e implementação, sendo imprescindível a apresentação de um plano que comprove a conformidade com os direitos fundamentais, a proteção de dados pessoais e o tratamento de potenciais vieses discriminatórios, em especial quanto à raça, condição social ou localidade geográfica de moradia.

Art. 38. Os modelos de inteligência artificial poderão utilizar ferramentas de mercado ou soluções de código aberto que:

I – facilitem sua integração ou interoperabilidade entre os sistemas utilizados pelos órgãos do Poder Judiciário, permitindo uma troca de informações eficiente e segura;

II – possibilitem um ambiente de desenvolvimento colaborativo, onde diferentes tribunais e instituições possam contribuir para evolução das soluções adequadas;

III – permitam maior transparência, garantindo que os processos e algoritmos utilizados sejam acessíveis para auditoria, monitoramento e revisão por parte de especialistas autorizados ou por meio da sociedade civil, mediante requerimento;

IV – proporcionem cooperação entre outros segmentos e áreas do setor público e a sociedade civil, promovendo iniciativas conjuntas para o desenvolvimento e a implementação de soluções de inteligência artificial;

V – assegurem a proteção e a segurança dos dados utilizados, em particular os dados por cuja guarda o Poder Judiciário seja responsável, adotando medidas que previnam acessos não autorizados e preservem a integridade das informações;

VI – garantam a não-dependência tecnológica.

CAPÍTULO XI
DA AUDITORIA E DO MONITORAMENTO

Art. 39. 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.

§ 1º A prestação de contas compreenderá:

I – os nomes dos responsáveis pela execução das ações e pela prestação de contas;

II – os custos envolvidos na pesquisa, desenvolvimento, implantação, comunicação e treinamento;

III – a existência de ações de colaboração e cooperação entre os agentes do setor público ou entre esses e a iniciativa privada ou a sociedade civil;

IV – os resultados pretendidos e os que foram efetivamente alcançados;

V – a demonstração de efetiva publicidade quanto à natureza do serviço oferecido, técnicas utilizadas, desempenho do sistema e riscos de erros;

VI – a demonstração da divulgação das informações acima mencionadas em formato acessível e linguagem simples, através de canais adequados, com atualizações regulares, permitindo a interação do público para esclarecimento de dúvidas e sugestões.

§ 2º A prestação de contas deverá ser publicada em canal oficial e poderá ser submetida a auditoria externa por decisão do Tribunal ou do Comitê Nacional de Inteligência Artificial do Judiciário, quando for o caso.

Art. 40. O desenvolvimento ou a utilização de sistemas inteligentes em desacordo com os princípios e regras estabelecidos nesta Resolução e nos demais normativos aplicáveis será monitorado, sem caráter disciplinar, por parte do Comitê Nacional de Inteligência Artificial do Judiciário.

Parágrafo único. O monitoramento poderá indicar necessidade de auditoria sobre práticas inadequadas, uso indevido de dados e falta de transparência e as faltas e discrepâncias eventualmente identificadas poderão ser comunicadas pelo Comitê ao órgão competente para adoção de providências.

Art. 41. 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.

1º A definição da metodologia para a condução de auditorias será realizada pelo Comitê, levando em consideração a identificação dos riscos envolvidos, a definição de salvaguardas (medidas de proteção) e a documentação produzida.

§ 2º Para execução das atividades de auditoria e inspeção, o Comitê poderá propor à Presidência do Conselho Nacional de Justiça a criação de comissões técnicas ou grupos de trabalho, que deverão contar com membros qualificados e com experiência nas áreas relacionadas à auditoria de inteligência artificial.

§ 3º 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.

§ 4º Havendo identificação de desconformidades, o Comitê fixará prazo para correção, que será definido com base na gravidade e impactos da desconformidade.

Art. 42. 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.

§ 1º 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.

§ 2º A comunicação dos eventos adversos deverá ser realizada no prazo de até 72 horas após a sua identificação, contendo descrição do incidente, suas causas e as medidas adotadas para correção.

§ 3º O Comitê analisará as informações recebidas e poderá recomendar ações corretivas, conforme necessário.

CAPÍTULO XII
DAS DISPOSIÇÕES FINAIS

Art. 43. Os órgãos do Poder Judiciário poderão realizar cooperação técnica com outras instituições, públicas ou privadas, ou com a sociedade civil, para o desenvolvimento colaborativo de modelos de inteligência artificial, desde que observadas as disposições contidas nesta Resolução.

§ 1º A cooperação técnica deve incluir a elaboração de acordos que especifiquem as responsabilidades de cada parte no que diz respeito à proteção de dados e à confidencialidade das informações compartilhadas.

§ 2º As instituições parceiras devem garantir que os dados utilizados na colaboração atendam aos requisitos da Lei Geral de Proteção de Dados Pessoais e às normas de segurança estabelecidas pelo Conselho Nacional de Justiça.

§ 3º As soluções de IA do Judiciário devem ser desenvolvidas com a perspectiva de disponibilização de seus aplicativos na PDPJ-Br, ainda que por meio de versão adaptada para as peculiaridades técnicas da Plataforma.

Art. 44. As normas previstas nesta Resolução não excluem a aplicação de outras normas do ordenamento jurídico brasileiro, incluindo, mas não se limitando a, leis federais, estaduais e municipais, assim como tratados e convenções internacionais ratificados pela República Federativa do Brasil.

Art. 45. As disposições desta Resolução aplicam-se também aos projetos e modelos de inteligência artificial já em desenvolvimento ou implantados nos tribunais, respeitados os atos já consolidados.

Parágrafo único. Os tribunais terão um prazo de doze meses para adequar seus projetos e modelos, em desenvolvimento ou já implantados, às novas disposições estabelecidas nesta Resolução, a partir de sua publicação.

Art. 46. Revoga-se a Resolução CNJ nº 332, de 21 de agosto de 2020, a partir do início da vigência desta Resolução.

Art. 47. Esta Resolução entra em vigor após decorridos 120 dias da data de sua publicação.

ANEXO DE CLASSIFICAÇÃO DE RISCOS

Consideram-se de **alto risco** as seguintes finalidades e contextos para o desenvolvimento de soluções baseadas em inteligência artificial destinadas a desempenhar ou apoiar o usuário na realização das seguintes atividades acessórias:

AR1 – identificação de perfis e de padrões comportamentais de pessoas naturais ou de grupos de pessoas naturais, exceto quando enquadradas como situações de risco mínimo ou controlado, conforme critérios objetivos estabelecidos;

AR2 – aferição da adequação dos meios de prova e a sua valoração nos processos de jurisdição contenciosa, sejam documentais, testemunhais, periciais ou de outras naturezas, especialmente quando tais avaliações possam influenciar diretamente a decisão judicial;

AR3 – averiguação, valoração, tipificação e a interpretação de fatos como sendo crimes, contravenções penais ou atos infracionais, ressalvadas as soluções voltadas à mera rotina da execução penal e de medidas socioeducativas;

AR4 – formulação de juízos conclusivos sobre a aplicação da norma jurídica ou precedentes a um conjunto determinado de fatos concretos, inclusive para a quantificação ou a qualificação de danos suportados por pessoas ou grupos, em ações criminais ou não;

AR5 – identificação e a autenticação facial ou biométrica para o monitoramento de comportamento de pessoas naturais, exceto quando utilizada para a mera confirmação da identidade de uma pessoa natural específica ou para atividades de segurança pública devidamente justificadas, sempre garantida a observância dos direitos fundamentais e monitoramento contínuo de tais soluções.

Consideram-se de **baixo risco** as seguintes finalidades e contextos para o desenvolvimento de soluções baseadas em inteligência artificial destinadas a desempenhar ou apoiar o usuário na realização das seguintes atividades acessórias:

BR1 – execução de atos processuais ordinatórios ou de tarefas de apoio à administração judiciária, mediante a extração de informações de sistemas e de documentos,

com a finalidade de classificação e agrupamento de dados e processos, enriquecimento de cadastros, certificação e transcrição de atos processuais, sumarização ou resumo de documentos, entre outras finalidades de gestão processual e operacional, desde que supervisionadas por responsável humano;

BR2 – detecção de padrões decisórios ou de desvios de padrões decisórios, bem como detecção de precedentes qualificados pertinentes, observado o caráter complementar da técnica de inteligência artificial, desde que não haja substituição da avaliação humana sobre processos, sendo seu uso destinado para apoio interno ao tribunal e para uniformização da jurisprudência;

BR3 – fornecimento aos magistrados de subsídios para a tomada de decisão mediante relatórios gerenciais e análises que adotem técnica jurimétrica, com a integração de fontes de informação relevantes ou a detecção de padrões decisórios, desde que não haja substituição da avaliação humana e que a solução não realize valorações de cunho moral sobre provas ou sobre perfis e condutas de pessoas;

BR4 – produção de textos de apoio para facilitar a confecção de atos judiciais, desde que a supervisão e a versão final do documento sejam realizadas pelo magistrado e com base em suas instruções, especialmente as decisões acerca das preliminares e questões de mérito;

BR5 – aprimoramento ou formatação de uma atividade humana anteriormente realizada, desde que não se altere materialmente o seu resultado, ou ainda realização de uma tarefa preparatória para uma outra, considerada como de alto risco;

BR6 – realização de análises estatísticas para fins de política judiciária, sempre com supervisão humana contínua, especialmente para evitar conclusões enviesadas;

BR7 – transcrição de áudio e vídeo para o auxílio das atividades do magistrado, com revisão final realizada por pessoa responsável;

BR8 – anonimização de documentos ou de sua exibição, especialmente para garantir sua conformidade com as normas de privacidade e proteção de dados.