



ALERTAS

Para o uso de IA Generativa

A RESPONSABILIDADE É

SUA



RESPONSABILIDADE DO AUDITOR

Vale mencionar que se **MANTÊM** aplicáveis ao uso de IA generativa todos os normativos que regem as diversas atividades de auditoria ou do serviço público.

Portanto, permanece a plenitude da responsabilidade do **auditor(a)** sobre qualquer documento que tenha produzido, com ou sem uso de IA generativa.

Eventuais falhas introduzidas por uso inadequado de IA generativa não afastam a responsabilidade do autor de **REVISAR** a produção da IA e assumir a autoria plena e exclusiva do resultado

PONTOS QUE MERECEM **ATENÇÃO**

no uso de IA Generativa



**USO DE DADOS SENSÍVEIS
NÃO É RECOMENDADO**

SEM ANONIMIZAÇÃO

<https://chatgpt.com/share/0ca41d02-1130-4103-a471-a017b0221790>
<https://chatgpt.com/share/0cacf7c7-9e91-4552-b02d-a7bac3e86b55>
<https://chatgpt.com/share/0cb30ac3-a496-41e4-9af7-235ed09f6b29>
<https://chatgpt.com/share/0cbb3725-b0d3-42f0-ace8-3990915738bd>
<https://chatgpt.com/share/0cc33d08-788f-4d89-a5ea-f3b5797cbd26>
<https://chatgpt.com/share/0cc667b9-03e4-4fcd-9836-8f88dcb87955>
<https://chatgpt.com/share/0cc7afd5-49c0-4773-8fc1-54054e886632>
<https://chatgpt.com/share/0cce5f60-1bcb-4b30-b288-9af78a45f365>
<https://chatgpt.com/share/0ccf5729-bcb3-4bc6-968f-2614f2ad71f4>
<https://chatgpt.com/share/0ccfb7a5-e3ac-4369-97bb-4139ca6b294d>
<https://chatgpt.com/share/0cd2126b-e7f2-4f5b-8040-4104fca8e3b5>
<https://chatgpt.com/share/0cd77782-13b5-4775-80d0-c77c7749fb9d>
<https://chatgpt.com/share/0ce2c749-fea7-466c-8874-45bf9d067423>
<https://chatgpt.com/share/0ce38fec-9750-4426-b17b-11e9ac9692da>

ChatGPT scrubbed today nearly 50,000 shared conversations from Google's index after our article. They thought they'd solved the problem. But did they?

changed the state to **Not applicable** on google indexes shared chatgpt conversations including PII data (names, phone numbers...

A new Digital Digging investigation, [here is the first one](#), conducted with Belgian researcher [Nicolas Deleur](#), has uncovered 110,000 ChatGPT conversations preserved via Archive.org's Wayback Machine. When users click "share" on a ChatGPT conversation, they think they're creating a temporary link for a friend or colleague. What they don't realize is they were also creating a permanent, searchable record of their thoughts, confessions, and sometimes illegal activities seen by Archive.org.

O recente vazamento de conversas privadas do ChatGPT, amplamente reportado em julho e agosto de 2025, envolveu a exposição de milhares de diálogos de usuários em mecanismos de busca como o Google, devido a uma falha em um recurso experimental da OpenAI chamado "Make this chat discoverable" ("Tornar este chat acessível")

Quando a IA Generativa cita
legislação. “Segundo a Lei 8.666/93
...”

Modelos sem *Reasoning* e sem o uso de **Engenharia de Prompt** e **Engenharia de Contexto** tendem a alucinar ao falar de legislação.

Quando o dado é muito atual.

A implementação de Agentes (busca web) e outras ainda é muito recente.

Os modelos são treinados em períodos específicos de dados (ex.: até dez. 2023)

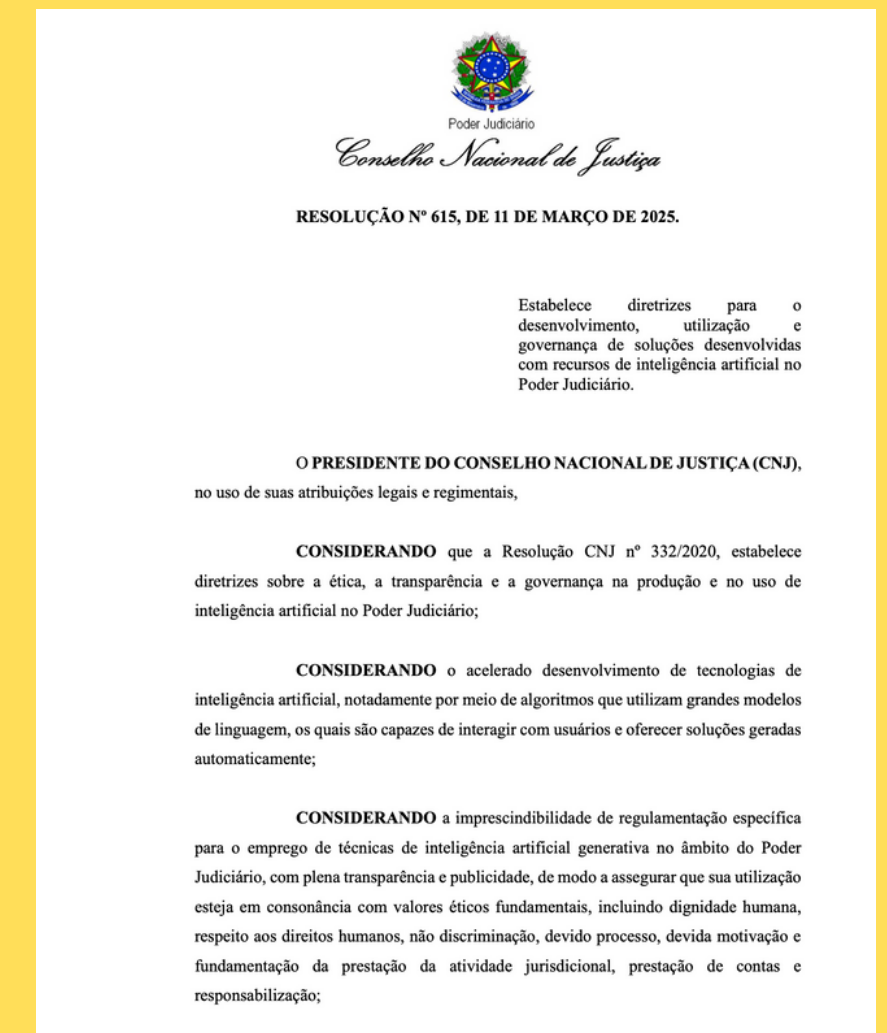
Sem Agentes de busca, ou dados para **contexto** eles não respondem corretamente

Ex.: *“Quem é o atual Secretário Federal de Controle da CGU?”*



REVISAR SEMPRE!

Guias e Orientações



CGU: <https://cgugovbr.sharepoint.com/sites/intracgu-inovacao/SitePages/Proposta-2.aspx?web=1>

TCU: <https://portal.tcu.gov.br/data/files/42/F7/91/4B/B59019105E366F09E18818A8/Guia%20de%20uso%20de%20IA%20generativa%20no%20TCU.pdf>

MGI: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/inteligencia-artificial-1/ia-generativa-no-servico-publico.pdf>

CNJ: <https://atos.cnj.jus.br/files/original1555302025031467d4517244566.pdf>

Utilizar IA apenas como ferramenta auxiliar, nunca como substituto de decisão humana.

Garantir que o uso da IA seja ético, transparente, seguro e não discriminatório.

Evitar o uso de IA para processar dados sigilosos ou protegidos por segredo de justiça, salvo se devidamente anonimizados.

Revisar o conteúdo gerado pela IA



Poder Judiciário

Conselho Nacional de Justiça

RESOLUÇÃO Nº 615, DE 11 DE MARÇO DE 2025.

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

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, para fins de uso em atividades funcionais do Poder Judiciário deverá observar as seguintes condições:

I – 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;

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 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; e

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 desta Resolução.

§ 4º O Comitê Nacional de Inteligência Artificial do Judiciário elaborará e atualizará periodicamente um manual de boas práticas em linguagem simples 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 CNJ, da Enfam e da 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 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.

§ 8º 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.

Art. 20. A contratação de modelos de linguagem de larga escala (LLMs), de pequena escala (SLMS) 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 35/1979 (Lei Orgânica da Magistratura Nacional – Loman), a Lei Geral de Proteção de Dados Pessoais, a Lei nº 9.279/1996 (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 servir de suporte a decisões a partir de documentos ou dados sigilosos ou protegidos por segredo de justiça, exceto nas hipóteses do art. 19, § 3º, IV, desta Resolução;

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 desta Resolução;

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; e

X – a contratação de serviços ou soluções de inteligência artificial pelos tribunais deverá levar em conta seus aspectos financeiros e orçamentários em todo seu ciclo de vida, notadamente no desenvolvimento, implantação e manutenção.

Parágrafo único. É vedada a utilização de dados sigilosos ou protegidos por segredo de justiça para treinamento de modelos de inteligência artificial, salvo prévia anonimização dos dados na origem.

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 12 (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.



AUDITORIA INTELIGENTE

<http://auditoriainteligente.com.br>
[in/andrecorumba](#)