STM SUPERIOR TRIBUNAL MILITAR
DIDOC/COGES/LEGIS
Publicado no BJM nº 49,
de 13/12/2024

026778/24-00.327

PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR

ATO NORMATIVO Nº 808

Institui o Guia de Diretrizes e Boas Práticas no Uso de Soluções de Inteligência Artificial Generativa na Justiça Militar da União.

O MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR, no uso das atribuições que lhe são conferidas pelo inciso XXV do art. 6º do Regimento Interno, e

CONSIDERANDO a Resolução nº 332, de 21 de agosto de 2020, do Conselho Nacional de Justiça (CNJ), que dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário;

CONSIDERANDO as orientações e boas práticas em Inteligência Artificial previstas nas normas ABNT NBR ISO/IEC 22989 (Tecnologia da informação - Inteligência Artificial - Conceitos de Inteligência Artificial e terminologia), ABNT NBR ISO/IEC 23894 (Tecnologia da informação - Inteligência Artificial - Orientações sobre gestão de riscos), ABNT NBR ISO/IEC 38507 (Tecnologia da informação - Governança de TI - Implicações de governança do uso de Inteligência Artificial pelas organizações) e ABNT NBR ISO/IEC 42001 (Tecnologia da informação - Inteligência Artificial - Sistema de gestão);

CONSIDERANDO a Política de Segurança Cibernética da Justiça Militar da União (JMU), instituída pela Resolução nº 350, de 16 de abril de 2024;

CONSIDERANDO a Resolução nº 351, de 16 de abril de 2024, que institui a Política de Segurança da Informação da Justiça Militar da União;

CONSIDERANDO a importância de assegurar o uso legal e ético da Inteligência Artificial generativa, visando maximizar seus benefícios, como ganhos de produtividade, escalabilidade e novas capacidades, mantendo a qualidade e a confiabilidade técnica da atuação da Justiça Militar da União;

CONSIDERANDO que as tecnologias de Inteligência Artificial devem ser utilizadas como ferramentas auxiliares, e nunca substitutas do julgamento humano, sendo indispensável que os textos gerados por essas tecnologias sejam revisados e validados pelos magistrados, garantindo a qualidade e a autonomia das decisões judiciais;

CONSIDERANDO a necessidade de estabelecer diretrizes para o uso responsável da Inteligência Artificial generativa na Justiça Militar da União, visando mitigar riscos relacionados ao tratamento inadequado de dados sensíveis e à exposição de informações não públicas em ferramentas externas;

CONSIDERANDO a caracterização da Inteligência Artificial generativa como uma tecnologia capaz de gerar conteúdo a partir de instruções, envolvendo riscos, como a excessiva dependência de suas sugestões e as potenciais ameaças à segurança cibernética;

R E S O L V E:

Art. 1º Fica aprovado, na forma do Anexo I deste Ano Normativo, o Guia de Diretrizes e Boas Práticas no Uso de Soluções de Inteligência Artificial Generativa na Justiça Militar da União.

Art. 2º Compete à Diretoria de Tecnologia da Informação e Transformação Digital (DITIN) apoiar e monitorar a implementação das diretrizes, boas práticas e orientações estabelecidas pelo Guia de Diretrizes e Boas Práticas no Uso de Soluções de Inteligência Artificial Generativa na Justiça Militar da União.

Art. 3º O Comitê de Governança de Tecnologia da Informação e Comunicação da Justiça Militar da União (CGovTIC/JMU) poderá aprovar, a qualquer tempo, mudanças e atualizações no Guia de Diretrizes e Boas Práticas no Uso de Soluções de Inteligência Artificial Generativa na Justiça Militar da União, de modo a assegurar sua constante adequação e evolução.

Art. 4º Este Ato Normativo entrará em vigor na data de sua publicação.

Ten Brig Ar **FRANCISCO JOSELI PARENTE CAMELO**

Ministro-Presidente

ANEXO I

(Art. 1º do Ato Normativo nº 808, de 9 de dezembro de 2024)

GUIA DE DIRETRIZES E BOAS PRÁTICAS NO USO DE SOLUÇÕES DE INTELIGÊNCIA ARTIFICIAL GENERATIVA NA JUSTIÇA MILITAR DA UNIÃO

1. Introdução

1.1. Bem-vindo ao **Guia de Diretrizes e Boas Práticas no Uso de Soluções de Inteligência Artificial Generativa na Justiça Militar da União**. Este documento tem como objetivo orientar magistrados, servidores, estagiários e prestadores de serviço da Justiça Militar da União (JMU) sobre o uso responsável, seguro, ético e consciente de ferramentas de Inteligência Artificial (IA) generativa, tais como ChatGPT, Gemini e Copilot, destacando-se a importância da governança e supervisão adequadas na adoção dessas tecnologias.

1.2. A utilização de ferramentas de IA generativa no contexto laboral da JMU poderá trazer inúmeros benefícios e oportunidades, como a automação de tarefas repetitivas, pesquisa de jurisprudência e legislação, além de auxiliar na elaboração de documentos. No entanto, é necessário que todos utilizem essas ferramentas com responsabilidade e ética, avaliando as limitações, os potenciais riscos à Segurança da Informação, à privacidade e transparência, além de possíveis vieses nos sistemas de IA. Assim, é fundamental a orientação e a adoção de diretrizes e boas práticas que assegurem a privacidade dos dados, a confiabilidade das informações, a segurança de acesso, a ética e a transparência no uso dessas ferramentas, além de promover a capacitação e a conscientização de todos os envolvidos , bem como a governança e o controle no uso de IA generativa.

1.3. Este guia foi elaborado com base nas melhores práticas de mercado e em conformidade com a Resolução nº 351, de 16 de abril de 2024, que institui a Política de Segurança da Informação da Justiça Militar da União, além de outros normativos relevantes, como a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), as normas da ABNT NBR ISO/IEC e as resoluções do Conselho Nacional de Justiça (CNJ), em especial a Resolução CNJ nº 332, de 21 de agosto de 2020, que dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário.

2. Abrangência

2.1. Este guia se aplica a todos os usuários de ferramentas de IA generativa na JMU, incluindo:

- Magistrados;
- Servidores;

- Estagiários;
- Prestadores de serviço;
- Terceirizados.

2.2. As diretrizes e boas práticas apresentadas neste documento são aplicáveis a dispositivos institucionais ou pessoais, quando estes forem utilizados para fins profissionais ou no manuseio de dados da JMU.

3. Definições

3.1. **Inteligência Artificial generativa (IA generativa):** tecnologia que gera conteúdos, como textos, áudios, imagens ou vídeos, a partir de comandos ou perguntas realizadas pelo usuário. Essa tecnologia pode ser a funcionalidade principal ou ser apenas incorporada a um aplicativo.

3.2. **Modelo de linguagem de grande escala (LLM):** também chamado de grandes modelos de linguagem, é uma grande rede neural artificial, treinada em extensos conjuntos de dados textuais, com o objetivo de entender e gerar texto de maneira natural.

3.3. **Ferramentas externas de IA generativa:** soluções de IA generativa, fornecidas por terceiros, gratuitas ou pagas, que não foram aprovadas oficialmente pela Diretoria de Tecnologia da Informação e Transformação Digital (DITIN), como, por exemplo, o ChatGPT e o Gemini, dentre diversas outras disponíveis no mercado.

3.4. **Alucinação:** termo usado na IA generativa para descrever respostas fictícias, informações ou fatos falsos, inexistentes ou imprecisos, porém convincentes, que podem ser erroneamente aceitas devido a algum viés no conjunto de dados usados para treinamento do modelo de IA, por escaparem a uma revisão superficial por quem não conhece profundamente do assunto.

3.5. **Prompt:** comando de texto fornecido a um modelo de linguagem de IA a fim de gerar uma resposta ou realizar uma tarefa específica. A qualidade e precisão da resposta podem variar significativamente de acordo com a formulação do prompt.

3.6. **Viés:** tendências presentes nos conjuntos de dados usados para treinar ferramentas de IA generativa, que podem influenciar os resultados gerados, introduzindo preconceitos ou distorções.

4. Diretrizes e Boas práticas

4.1. Privacidade de dados

É importante que o usuário esteja ciente de que as ferramentas externas de IA generativa registram e armazenam todas as suas conversas, incluindo informações pessoais ou sensíveis. Essas informações podem ser utilizadas para o aprendizado contínuo da IA, tornando-se, assim, públicas e acessíveis a terceiros. A LGPD exige que os dados pessoais, especialmente os sensíveis, sejam tratados de acordo com as finalidades especificadas e que sua coleta, uso e armazenamento sejam realizados com o **consentimento explícito** do titular dos dados. Em resumo, é preciso levar em consideração que os dados coletados podem servir como insumo para aprimorar a ferramenta, mas que existe o risco de que dados internos ou sensíveis sejam disponibilizados em interações com outros usuários que não possuam qualquer vínculo com a JMU.

4.1.1. Não divulgue informações restritas

É proibido inserir qualquer informação não pública, produzida ou custodiada pela JMU, em ferramentas externas de IA generativa. Isso inclui e-mails, minutas, relatórios, dados processuais sob segredo de justiça, decisões ainda não publicadas, informações relacionadas à segurança dos magistrados, dados pessoais e sensíveis, sobretudo dados corporativos cuja divulgação comprometa a integridade administrativa desta Corte. A plataforma pode armazenar as conversas e compartilhar os dados coletados, portanto, mantenha as informações confidenciais em ambientes seguros e restritos.

4.1.2. Atenção com dados pessoais e dados sensíveis

O usuário deverá considerar que os dados pessoais deverão ser tratados com extrema cautela. Os dados sensíveis não deverão ser inseridos, em nenhuma hipótese, em ferramentas externas. Lembre-se de que o usuário tem o dever de garantir a segurança, e o sigilo dessas informações, bem como o tratamento

adequado, de acordo com a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018), a Política de Governança Arquivística, da Informação, dos Dados e do Conhecimento, no âmbito da Justiça Militar da União (Resolução nº 340, de 27 de novembro de 2023) e o Plano Operacional de Gestão e de Privacidade de Dados Pessoais da Justiça Militar da União (Ato Normativo nº 692, de 22 de dezembro de 2023).

4.1.3. Use redações genéricas

Ao fazer perguntas ou redigir textos, não forneça detalhes específicos que possam identificar indivíduos ou informação não pública. Utilize termos genéricos para proteger a privacidade dos envolvidos.

4.1.4. Anonimize os dados pessoais e dados sensíveis

Se necessário, anonimize os dados antes de inseri-los nas ferramentas externas de IA generativa, substituindo nomes, números de identificação ou quaisquer outros detalhes identificáveis por informações fictícias.

4.1.5. Informações Classificadas

Toda informação classificada, que seriam as consideradas ultrassecretas, secretas ou reservadas, tem caráter restrito e não poderá ser utilizada nas ferramentas externas de IA generativa.

4.1.6. Atenção à Política de Privacidade da IA utilizada

É essencial que ao utilizar ferramentas de IA generativa o usuário esteja atento à política de privacidade da plataforma ou serviço em questão. Esse documento define as regras sobre como seus dados pessoais serão coletados, armazenados, utilizados e protegidos durante a interação com a IA. O usuário, portanto, deverá verificar atentamente os seguintes pontos da política de privacidade: finalidade do uso dos dados, bases legais do tratamento, direitos do titular e medidas de segurança que garantam a proteção dos dados pessoais.

4.2. Confiabilidade das informações

As ferramentas de IA generativa podem vir a produzir respostas que aparentam ser precisas e confiáveis, mas que não refletem a realidade. Devido à natureza probabilística desses modelos, existe o risco de "alucinações", nas quais a IA gera informações incorretas ou fictícias, que podem parecer verdadeiras para não especialistas no assunto. Portanto, é fundamental que todo conteúdo produzido por IA Generativa seja submetido à análise minuciosa do usuário, a fim de garantir que as informações apresentadas sejam verídicas, precisas, livres de vieses e que não haja violação de propriedade intelectual ou direitos autorais de terceiros.

4.2.1. Revise as informações geradas

O usuário deverá sempre confirmar as informações geradas pela IA, consultando fontes oficiais ou especialistas na área, e será o responsável por qualquer documento que tenha produzido, com ou sem o uso de IA generativa. Eventuais falhas produzidas pelo uso inadequado de IA generativa não afastam a responsabilidade do autor, que deverá revisar a produção da IA e assumir a autoria do resultado.

4.2.2. Cuidado com alucinações

O usuário deverá analisar criticamente as informações fornecidas, especialmente quando se tratar de questões delicadas ou controversas, a fim de assegurar que o conteúdo produzido seja justo, imparcial, ético e livre de preconceitos, tendo em vista que os algoritmos de IA generativa podem conter viéses em seu treinamento, o que pode afetar a objetividade e precisão de suas respostas.

4.2.3. Evite riscos de violação de propriedade intelectual

O usuário deverá ter cautela antes de reproduzir o conteúdo gerado por IA (textos, imagens, etc), verificando sempre se há indícios de plágio ou violação de propriedade intelectual ou direitos autorais de terceiros, tendo em vista que a base de dados usada para treinamento das ferramentas de IA generativa poderá conter elementos que não são de domínio público.

4.2.4. Evite automatizações sem revisão humana

A adoção de decisões automatizadas criadas pela IA generativa e o uso de IA generativa para tomada de decisões estratégicas ou fornecimento de informações diretamente ao público externo, sem revisão

humana, deverão ser evitados.

4.2.5. Não implemente código sem revisão especializada

São proibidas a implementação e a utilização de código de programação gerado por IA generativa, nos sistemas da JMU, sem a revisão por especialista de TI.

4.3. Segurança no acesso

Garantir a segurança no acesso às ferramentas externas de IA generativa é fundamental para proteger os sistemas da JMU contra ameaças cibernéticas. O uso inadequado ou descuidado poderá expor dados e comprometer a integridade das informações institucionais.

4.3.1. Use senhas fortes

Proteja o acesso às ferramentas externas de IA generativa com senhas fortes e altere-as regularmente ou sempre que houver indícios de comprometimento. Nunca compartilhe suas senhas com terceiros, nem as reutilize em outros serviços. Em nenhuma hipótese utilize a mesma senha dos sistemas internos da JMU.

4.3.2. Habilite a autenticação de múltiplos fatores

A autenticação de múltiplos fatores (MFA) deverá ser habilitada sempre que disponível, a fim de adicionar uma camada extra de segurança ao acesso.

4.3.3. Não utilize credenciais institucionais

As credenciais institucionais, por exemplo, endereços de e-mail ou números de telefone da JMU, não deverão ser utilizadas como *login* para ferramentas externas de IA generativa, evitando, assim, a criação de vínculo entre o uso pessoal dessas plataformas e a relação de trabalho na instituição. Nesse caso, recomenda-se o uso de contas pessoais ao criar contas em plataformas externas de IA generativa.

4.4. Ética e Transparência

O uso de ferramentas de IA generativa deverá ser pautado pela ética e transparência, em conformidade com a Resolução nº 159, de 4 de fevereiro de 2009, que aprova o Código de Ética dos servidores da Justiça Militar da União, e com a Resolução n° 333, de 22 de agosto de 2023, que estabelece a Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação para a Justiça Militar da União.

4.4.1. Atenda aos princípios éticos da instituição

Certifique-se de que o uso de IA generativa esteja alinhado com o Código de Ética da JMU.

4.4.2. Seja transparente no uso de IA generativa

Utilize a transparência em relação ao uso de IA generativa nas atividades profissionais, informando quando as decisões ou conteúdos forem produzidos com o auxílio dessas ferramentas.

4.4.3. Evite danos à reputação da JMU

A IA generativa deverá ser utilizada em conformidade com a Política de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação para a JMU (Resolução nº 333, de 22 de agosto de 2023), a fim de proteger magistrados, servidores, estagiários, prestadores de serviço, terceirizados, cidadãos e a JMU de danos à reputação e prevenir a ocorrência de possíveis vieses. Nesse sentido, o conteúdo inapropriado, discriminatório, incorreto, ou que possa ser prejudicial aos servidores ou cidadãos, criado pela IA generativa devido a alucinações ou vieses, não deverá ser utilizado para fins de trabalho.

4.5. Governança e controle no uso de IA generativa

A governança e o controle no uso de IA generativa são essenciais para garantir que essas ferramentas sejam utilizadas de forma alinhada aos objetivos, missão, visão e valores da JMU, além de permitir o monitoramento e a mitigação de riscos associados.

4.5.1. Reporte o uso corporativo de IA generativa

O uso corporativo e contínuo de funcionalidades providas por ferramentas externas de IA generativa deverá ser reportado à DITIN, a fim de permitir a manutenção de um registro centralizado do uso de

soluções de IA externas, conforme previsto na Política de Gestão de Ativos de Tecnologia da Informação e Comunicação da Justiça Militar da União (PGATIC/JMU), regulamentada pelo Ato Normativo nº 743, de 26 de abril de 2024. A medida visa ajudar a organização a proteger os ativos de TIC, identificando riscos e vulnerabilidades e implementando mecanismos de segurança para assegurar sua integridade.

4.5.2. Colabore com a DITIN na avaliação de riscos

A DITIN poderá avaliar e mitigar os riscos associados ao uso de IA, como a dependência excessiva de fornecedores externos ou a introdução de vulnerabilidades nos sistemas. O usuário poderá colaborar com a avaliação de riscos, fornecendo as informações necessárias para essa avaliação e seguindo as orientações recebidas.

4.6. Capacitação e conscientização

A educação contínua é vital para acompanhar a evolução das tecnologias de IA e compreender seus impactos no ambiente de trabalho. A capacitação permite que os usuários utilizem as ferramentas de forma eficaz e segura, enquanto a conscientização promove uma cultura de responsabilidade e ética no uso da IA.

4.6.1. Esteja atento aos normativos

Mantenha-se informado sobre mudanças nas políticas, normas e regulamentações relacionadas à IA, tanto internas quanto externas à JMU.

4.6.2. Participe de programas de capacitação

Engaje-se regularmente em programas de treinamento e *workshops* oferecidos pela JMU sobre o uso seguro e ético da IA.

4.6.3. Compartilhe boas práticas

Colabore com colegas para disseminar conhecimentos e experiências positivas no uso de IA, promovendo um ambiente de aprendizagem colaborativa.

5. Responsabilidades dos usuários

5.1. As disposições da Política de Segurança da Informação da Justiça Militar da União, instituídas pela Resolução nº 351, de 16 de abril de 2024, também se aplicam no uso de IA generativa.

5.2. Os usuários, elencados no item 2.1 do Anexo I deste Ato Normativo, que não observarem o disposto neste guia e causarem dano patrimonial, moral, individual ou coletivo poderão ser responsabilizados pelo dano, sem prejuízo, nos termos da lei, das sanções administrativas, civis ou penais cabíveis.

5.3. As empresas terceirizadas só receberão informações sigilosas após concordância expressa com as disposições deste guia para IA generativa, e a ciência de que sua violação, por parte de terceiros contratados, poderá ser considerada quebra de contrato.

5.4. É vedado o desenvolvimento de aplicativos baseados em IA generativa, voltados para o público externo, que não sejam produzidos ou validados pela DITIN.

5.5. O STM poderá acessar e monitorar o uso dos aplicativos de IA generativa em qualquer dispositivo da instituição, ou que apareça nas redes gerenciadas pela instituição, a fim de garantir o uso compatível desses sistemas.

5.6. Os casos em desacordo com as disposições deste guia deverão ser reportados à Ouvidoria da Justiça Militar da União (OUVJMU), ou diretamente à DITIN, que serão responsáveis por consultar as unidades administrativas competentes pelos assuntos relacionados à IA generativa.

5.7. Os casos omissos serão resolvidos pela DITIN, ouvidas as áreas de interesse.

6. Referências

BRASIL. Conselho Nacional de Justiça. **Resolução nº 332, de 21 de agosto de 2020**. Dispõe sobre a ética, a transparência e a governança na produção e no uso de inteligência artificial no Poder Judiciário e dá outras providências. Brasília, DF: Conselho Nacional de Justiça, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3429. Acesso em: 3 nov. 2024.

BRASIL. Superior Tribunal Militar. Ato Normativo nº 743, de 26 de abril de 2024. Institui a política de gestão de ativos de tecnologia da informação e comunicação da Justiça Militar da União (PGATIC/JMU). **Boletim da Justiça Militar**, Brasília, DF, n. 17, p. 1158, 3 maio 2024. Disponível em: https://dspace.stm.jus.br/handle/123456789/185671. Acesso em: 3 nov. 2024.

BRASIL. Superior Tribunal Militar. **Código de ética dos servidores da Justiça Militar da União**. 2. ed. Brasília, DF: Superior Tribunal Militar, 2015. 27 p. (Série Legislação, 4). Publicação organizada pela Diretoria de Documentação e Gestão do Conhecimento (DIDOC). Disponível em: https://dspace.stm.jus.br/handle/123456789/58467. Acesso em 10 nov. 2024.

BRASIL. Superior Tribunal Militar. Resolução n° 333, de 22 de agosto de 2023. Estabelece a política de prevenção e enfrentamento do assédio moral, do assédio sexual e da discriminação para a Justiça Militar da União e institui a Comissão de Prevenção e Enfrentamento do Assédio Moral, do Assédio Sexual e da Discriminação da Justiça Militar da União (COMPREV). **Boletim da Justiça Militar**, Brasília, DF, n. 34, p. 2226, 1 set. 2023. Disponível em: https://dspace.stm.jus.br/handle/123456789/174756. Acesso em: 10 nov. 2024.

BRASIL. Superior Tribunal Militar. Resolução n° 340, de 27 de novembro de 2023. Institui a política de governança arquivística, da informação, dos dados e do conhecimento, no âmbito da Justiça Militar da União. **Boletim da Justiça Militar**, Brasília, DF, n. 47, p. 3140, 1 dez. 2023. Disponível em: https://dspace.stm.jus.br/handle/123456789/179224. Acesso em: 11 nov. 2024.

BRASIL. Superior Tribunal Militar. Resolução nº 351, de 16 de abril de 2024. Institui a política de segurança da informação da Justiça Militar da União. **Boletim da Justiça Militar**, Brasília, DF, n. 16, p. 104, 26 abr. 2024. Disponível em: https://dspace.stm.jus.br/handle/123456789/184747. Acesso em: 11 nov. 2024.

BRASIL. Tribunal de Contas da União. **Guia de uso de inteligência artificial generativa no Tribunal de Contas da União (TCU)**. Brasília, DF: TCU, 2024. Disponível em: https://portal.tcu.gov.br/guia-de-uso-de-inteligencia-artificial-generativa-no-tribunal-de-contas-da-uniao-tcu.htm. Acesso em: 12 nov. 2024.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. **Guia de boas práticas**: ferramentas externas de inteligência artificial generativa. Brasília: TJDFT, 2024. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/imagens-e-arquivos-2024/07_guia-boas-praticas.pdf. Acesso em: 12 nov. 2024.

Documento assinado eletronicamente por **FRANCISCO JOSELI PARENTE CAMELO**, **MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR**, em 09/12/2024, às 19:20 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4084033** e o código CRC **F3D2D52B**.