

INTELIGÊNCIA ARTIFICIAL (IA) NA ADVOCACIA BRASILEIRA: ÉTICA, LGPD, RESPONSABILIDADE E O DEVER ÉTICO DO PROFISSIONAL PERANTE A JUSTIÇA MILITAR E JUSTIÇA EM GERAL

ARTIFICIAL INTELLIGENCE (AI) IN THE BRAZILIAN LEGAL PROFESSION: ETHICS, THE GENERAL DATA PROTECTION LAW (LGPD), LIABILITY, AND THE PROFESSIONAL'S ETHICAL DUTY TOWARDS MILITARY JUSTICE AND JUSTICE IN GENERAL

Ary Sergio Dib Dias Filho¹

RESUMO

Este artigo analisa o impacto da inteligência artificial na prática jurídica, com foco nos limites éticos, legais e na responsabilidade profissional inerentes à sua adoção. Explora-se o arcabouço normativo brasileiro (Recomendação nº 001/2024 da Ordem dos Advogados do Brasil e Resolução nº 615/2025 do Conselho Nacional de Justiça) em paralelo com a experiência da advocacia nos Estados Unidos, destacando as diretrizes da American Bar Association e precedentes, como o caso Mata v. Avianca. O estudo avalia a intersecção do uso dessas ferramentas com os deveres fundamentais de competência, diligência e sigilo. É dada atenção especial à "alucinação jurídica", que resulta na geração de falsas jurisprudências, e às implicações frente à Lei Geral de Proteção de Dados Pessoais ao expor dados em plataformas de nuvem, fato ilustrado pelo caso Grok. Por fim, examinam-se os riscos sensíveis na atuação perante a Justiça Militar. Conclui-se que o uso responsável da inteligência artificial exige do profissional rigorosa governança e supervisão humana, não sendo a ignorância tecnológica aceita como atenuante para falhas.

Palavras-chave: inteligência artificial; advocacia brasileira; Estados Unidos; ética profissional; alucinação jurídica; LGPD; Justiça Militar.

ABSTRACT

This article analyzes the impact of artificial intelligence on legal practice, focusing on the ethical and legal limits, as well as professional responsibility inherent to its adoption. The Brazilian regulatory framework (Ordem dos Advogados do Brasil Recommendation No. 001/2024 and Conselho Nacional de Justiça Resolution No. 615/2025) is explored in parallel with the comparative experience of legal practice in the United States, highlighting the American Bar

¹ Advogado inscrito na OAB/RJ sob o nº 82.116. LL.M. em Direito de Segurança Nacional pela George Washington University Law School (Washington, D.C., 2015). AAS em Segurança Cibernética e Computação em Nuvem pelo Northern Virginia Community College, Magna Cum Laude (2020). E-mail: dibdias@law.gwu.edu.

Association guidelines and precedents like the Mata v. Avianca case. The study evaluates the intersection of using these tools with the fundamental duties of using these tools with the fundamental duties of competence, diligence, and confidentiality. Special attention is given to "legal hallucination," which results in the generation of false case law, and the implications concerning the Lei Geral de Proteção de Dados Pessoais (General Data Protection Law) regarding data exposure on cloud platforms, a fact illustrated by the Grok case. Finally, the sensitive risks of operating within the Military Justice system are examined. It concludes that the responsible use of artificial intelligence demands strict governance and human supervision from professionals, with technological ignorance not being accepted as a mitigating factor for failures.

Keywords: artificial intelligence; Brazilian legal practice; United States; professional ethics; legal hallucination; LGPD; Military Justice.

1 INTRODUÇÃO

Como registro de experiência profissional do autor, da época, por volta de 1994, foi contratado um pacote RENPAC da Embratel, que possibilitava, em uma conexão de 9.600 bps, comunicação com os tribunais situados no Rio de Janeiro. Na época, muitos escritórios resistiam ao uso de transmissão de dados, sendo as máquinas de escrever elétricas e os aparelhos de fax predominantemente usados, aparelhos que hoje são relíquias de um passado não tão distante.

Atualmente, a inteligência artificial (IA) já está presente na prática jurídica brasileira. Não como possibilidade futura, mas como realidade cotidiana. Advogados utilizam ferramentas de IA generativa para pesquisa jurisprudencial, elaboração de peças processuais, análise de contratos, organização de documentação e comunicação com clientes. Plataformas como ChatGPT, Claude, Gemini e suas versões especializadas para o mercado jurídico já são ferramentas de trabalho, não curiosidades tecnológicas.

A questão não é se o advogado deve ou não utilizar essas ferramentas, mas, sim, como utilizá-las dentro dos limites éticos e legais que regem a profissão — e com plena consciência das responsabilidades que esse uso implica. A velocidade do avanço tecnológico, em especial, não suspende os deveres profissionais, torna-os mais complexos de cumprir.

Este artigo examina o quadro normativo atual para o uso de IA na advocacia brasileira, as obrigações éticas específicas do uso ativo dessas ferramentas, a experiência comparada dos Estados Unidos e as implicações

particulares para advogados que atuam na área da Justiça Militar.

2 O QUADRO NORMATIVO BRASILEIRO

O marco normativo para o uso de IA na advocacia brasileira está em construção, mas já apresenta contornos suficientemente definidos para estabelecer obrigações concretas. Cabe notar que, como a União Europeia, o Brasil tem uma regulamentação e resposta nacional uniforme, através de legislação federal aplicável em todo o país de forma homogênea. Igualmente, a analogia civil se aplica completamente em casos de indenização por mau uso.

O Conselho Federal da Ordem dos Advogados do Brasil (OAB) aprovou a Recomendação nº 001, em novembro de 2024, estabelecendo diretrizes para o uso de IA generativa na prática jurídica (Ordem dos Advogados do Brasil, 2024). O documento foi elaborado pelo Observatório Nacional de Cibersegurança, Inteligência Artificial e Proteção de Dados da OAB Nacional e organiza-se em quatro eixos principais: legislação aplicável; confidencialidade e privacidade; prática jurídica ética; e comunicação sobre o uso de IA generativa.

A citada Recomendação, no seu número 3.2, exige que o advogado que utilize IA na elaboração de peças processuais faça a verificação rigorosa das informações produzidas, em cumprimento ao art. 77 do CPC (Brasil, 2015). No número 4 da mesma Recomendação, é estabelecida a obrigação de comunicação escrita ao cliente, que deve contemplar o propósito do uso da IA, os benefícios e limitações da tecnologia, os riscos envolvidos — incluindo exposição de dados — as medidas de segurança adotadas e a possibilidade de revisão humana. O consentimento genérico no contrato de honorários não é suficiente, deve ser explícito.

Em março de 2025, o Conselho Nacional de Justiça (CNJ) publicou a Resolução nº 615, estabelecendo diretrizes para o uso de IA no Poder Judiciário. A norma criou o Comitê Nacional de Inteligência Artificial do Judiciário, regulamentou especificamente os modelos de linguagem generativa, estabeleceu classificação de riscos com revisão anual obrigatória e proibiu expressamente o uso de dados sigilosos ou protegidos por segredo de justiça na produção de peças processuais, art. 19, § 3º, IV, em LLMs comerciais e treinamento de sistemas de IA, art. 20, parágrafo único (Brasil, 2025). Para os advogados, a Resolução CNJ nº 615/2025 não é diretamente vinculante, mas

define como os sistemas de IA utilizados pelos tribunais devem funcionar, o que afeta diretamente como as peças são processadas eletronicamente.

O Projeto de Lei nº 2.338/2023, Marco Legal da Inteligência Artificial, foi aprovado pelo Senado em dezembro de 2024 e encaminhado à Câmara, onde está em tramitação (Brasil, 2023). O projeto estabelece regime de responsabilidade civil para sistemas de IA que causem danos, com responsabilidade objetiva para sistemas de alto risco. Para o advogado que utiliza ferramentas de IA no exercício da profissão, o regime de responsabilidade subjetiva, já previsto no Código Civil, aplica-se integralmente: a culpa *in vigilando*, a negligência na supervisão do resultado produzido pela ferramenta é suficiente para caracterizar ato ilícito.

3 OS DEVERES ÉTICOS DO ADVOGADO E A INTELIGÊNCIA ARTIFICIAL

O uso de IA na prática jurídica ativa três deveres fundamentais previstos no Código de Ética e Disciplina da OAB que, apesar de o código não fazer nenhuma menção específica ao uso de IA, não significa que não sejam diretamente aplicáveis: competência, diligência e sigilo profissional. Cada um deles é afetado de forma específica (Conselho Federal da Ordem dos Advogados do Brasil, 2015).

O art. 49, VII, do Código de Ética estabelece o dever de atualização permanente do advogado ao exigir competência profissional (Conselho Federal da Ordem dos Advogados do Brasil, 2015). No contexto da IA, esse dever passa a incluir a obrigação de compreender o funcionamento das ferramentas utilizadas, incluindo suas limitações estruturais. Um advogado que utiliza um sistema de IA generativa sem compreender o fenômeno da alucinação, a produção de conteúdo plausível, mas factualmente incorreto, e possíveis erros em função de bancos de dados desatualizados não está exercendo a competência que o cargo exige. Competência tecnológica não é opção: é obrigação profissional.

O dever de diligência exige que o advogado empregue os meios necessários para a defesa dos interesses do cliente com atenção e cuidado, e é explicitado na responsabilidade que o advogado tem com o seu cliente e perante os tribunais. No contexto da IA, isso significa verificar independentemente, pessoalmente, toda fonte científica, doutrina, jurisprudência ou argumentação produzida por ferramentas automatizadas an-

tes de utilizá-la em documento jurídico. O texto produzido pela ferramenta de IA é um ponto de partida, não uma conclusão. A velocidade e a aparência de confiança do resultado não substituem a verificação.

O Capítulo VII do Código de Ética estabelece o sigilo profissional como direito e dever do advogado (Conselho Federal da Ordem dos Advogados do Brasil, 2015). O uso de ferramentas de IA baseadas em nuvem coloca em risco esse dever de forma que muitos profissionais ainda não dimensionaram adequadamente. Ao inserir informações confidenciais do cliente em uma plataforma de IA generativa, o advogado pode estar transferindo dados protegidos pelo sigilo para servidores de terceiros, sujeitos a políticas de privacidade que autorizam o uso dessas informações para treinamento de modelos. O consentimento do cliente para esse uso específico é obrigatório.

A saída da ferramenta de IA é um ponto de partida, não uma conclusão. A velocidade e a aparência de confiança do resultado não substituem a verificação independente.

4 O PROBLEMA DA ALUCINAÇÃO JURÍDICA

A alucinação é uma propriedade estrutural dos modelos de linguagem de grande porte, não um defeito corrigível. O modelo gera texto que corresponde ao padrão estatístico de uma resposta correta, sem mecanismo interno de verificação da veracidade, que só seria possível se o modelo tivesse uma memória ativa que lhe permitiria evitar tais falhas e, mesmo assim, um nível residual iria sempre existir. Uma citação jurisprudencial produzida por IA pode ter a forma exata de um acórdão real (ementa, número do processo, órgão julgador, data) sem que o julgado exista. O modelo não estaria errado, mas cumprindo exatamente o que a IA foi projetada para fazer: gerar texto que corresponde ao padrão aprendido. O resultado é um documento falso com aparência de verdadeiro.

Vale lembrar que não se trata sequer de hipótese de “edição seletiva”, na qual colegas apresentam uma ementa apenas em parte, e não em sua totalidade. Na experiência profissional cotidiana, esse “fenômeno” foi observado algumas vezes, sendo recorrente a necessidade de apresentação do acórdão completo, o qual, em vez de favorecer a parte contrária, apenas confirmava os argumentos anteriormente sustentados. A diligência, portanto, não constitui um problema novo; contudo, com a utilização da inteli-

gência artificial, o fenômeno adquire nova dimensão, pois, nos casos de “alucinação”, são criadas jurisprudências que simplesmente não existem, em volume sem precedentes.

No Brasil, uma advogada foi condenada ao pagamento de multa de dez salários mínimos por ter apresentado em juízo petição com julgados e dispositivos legais inexistentes gerados por IA (Advogada [...], 2025). O caso é ilustrativo porque a advogada ignorou que as citações eram falsas, o que é precisamente o ponto, e colocou a culpa no estagiário. A alucinação produz respostas convincentes que não se distinguem externamente de respostas corretas, e apenas a verificação independente pode detectar o problema. Responsabilizar o estagiário é particularmente grave, já que estagiários de Direito estão sob direta supervisão dos advogados.

Os arts. 77 e 78 do CPC estabelecem os deveres das partes e procuradores perante o juízo, incluindo a proibição de produzir provas falsas ou alterar a verdade dos fatos (Brasil, 2015). A apresentação de citações inexistentes, ainda que produzidas por ferramenta tecnológica sem dolo do advogado, pode configurar violação desse dispositivo, com as sanções processuais correspondentes. A ignorância sobre as limitações da ferramenta não elide a responsabilidade, constitui, ela própria, falta de competência.

5 A EXPERIÊNCIA NORTE-AMERICANA: OAB, ABA E OS PRIMEIROS CASOS

A experiência dos Estados Unidos oferece um referencial útil para a advocacia brasileira, não porque o sistema jurídico seja o mesmo, não é; mas porque os problemas são estruturalmente idênticos, e os Estados Unidos começaram a enfrentá-los alguns anos antes.

Em 29 de julho de 2024, a *American Bar Association* (ABA) publicou o *Formal Opinion 512*, sua primeira orientação ética formal sobre o uso de IA generativa na prática jurídica. A opinião aborda seis áreas principais: competência (*Model Rule 1.1*), confidencialidade (*Model Rule 1.6*), comunicação com clientes (*Model Rule 1.4*), candura perante o tribunal (*Rules 3.1 e 3.3*), responsabilidades de supervisão (*Rules 5.1 e 5.3*) e honorários razoáveis. A estrutura é notavelmente paralela à da Recomendação OAB nº 001/2024 — o que sugere que os desafios éticos colocados pela IA transcendem os sistemas jurídicos e são inerentes à tecnologia (American Bar Association, 2024; Ordem dos Advogados do Brasil, 2024).

O *Formal Opinion 512* estabelece que o consentimento genérico para usar IA em contratos de prestação de serviços não é suficiente. O advogado deve obter consentimento informado específico antes de inserir informações confidenciais do cliente em plataformas de IA (American Bar Association, 2024). Vários estados americanos — Califórnia, Flórida, Nova Jersey, Nova York e Pensilvânia — publicaram orientações específicas em antecipação ao posicionamento federal da ABA.

Um caso ilustrativo nos Estados Unidos é o *Mata v. Avianca*, julgado no Distrito Sul de Nova York em 2023 (Estados Unidos da América, 2023). Dois advogados submeteram peça processual citando seis precedentes judiciais gerados pelo ChatGPT, mas nenhum dos seis casos existia. O juízo não aceitou a defesa de que os advogados não sabiam que a ferramenta poderia produzir citações falsas. A ignorância sobre as limitações de uma ferramenta que o advogado escolheu utilizar foi tratada como falta de competência profissional, não como circunstância atenuante. Ambos foram punidos e, ironicamente, esse alerta não foi suficiente para evitar novos casos.

A comparação entre os dois sistemas revela uma convergência significativa: tanto a OAB quanto a ABA tratam a competência tecnológica como obrigação profissional, exigem consentimento informado específico para uso de dados confidenciais em plataformas de IA e atribuem ao advogado responsabilidade plena pelo conteúdo que submete ao tribunal, independentemente da fonte tecnológica que o produziu. A diferença principal está no grau de maturidade dos mecanismos sancionatórios, que nos Estados Unidos já geraram jurisprudência documentada, enquanto no Brasil ainda estão em fase de consolidação jurisprudencial.

A ignorância sobre as limitações de uma ferramenta que o advogado escolheu utilizar não é circunstância atenuante, é, ela própria, falta de competência profissional.

6 LGPD E O SIGILO NA ERA DA INTELIGÊNCIA ARTIFICIAL

A Lei Geral de Proteção de Dados (LGPD) — Lei nº 13.709/2018 — cria obrigações específicas para o tratamento de dados pessoais que se intersectam de forma complexa com o uso de ferramentas de IA na prática jurídica (Brasil, 2018).

Quando o advogado insere dados do cliente em uma plataforma de IA baseada em nuvem, está realizando uma operação de tratamento de dados pessoais sujeita à LGPD. A base legal para esse tratamento precisa ser identificada. Salvo exceções legais, é necessário o consentimento do titular, o cliente, e observar as regras do art. 7º da LGPD. O consentimento genérico para prestação de serviços jurídicos não cobre o tratamento específico por sistemas de IA (Brasil, 2018).

É importante ressaltar a questão de dados pessoais sensíveis, aqueles aos quais a LGPD conferiu uma proteção ainda maior, por estarem diretamente relacionados aos aspectos mais íntimos da personalidade de um indivíduo, o que também se aplica à utilização de IA. De acordo com o art 5º, II, da LGPD são dados pessoais sensíveis aqueles relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (Brasil, 2018).

Há ainda a observância especial ao art. 14 da LGPD, que prevê condições específicas para o tratamento de dados pessoais de crianças e adolescentes. Nesse caso, é necessário consentimento específico e, em destaque, dado por pelo menos um dos pais ou pelo responsável legal. As informações sobre o tratamento dos dados pessoais de crianças e adolescentes, assim como de idosos, devem ser fornecidas de maneira simples, clara e acessível e devem ser adequadas ao seu entendimento (Brasil, 2018).

Tendo isso em consideração, vale citar o caso IA Grok que constitui, até o momento, o exemplo mais bem documentado de violação estrutural à LGPD por um sistema de inteligência artificial generativa no Brasil — e suas implicações para a advocacia são diretas.

Em 14 de janeiro de 2026, a “Coordenação-Geral de Fiscalização (CGF) da Agência Nacional de Proteção de Dados (ANPD) recebeu a Representação nº 01-2026 - (0238713) e sua Petição Complementar de 12/01/2026 (0238714), apresentada pela Deputada Federal Erika Hilton” (Brasil, 2026), denunciando que o sistema Grok — assistente de inteligência artificial integrado à Plataforma X — permitia a geração automatizada de imagens sexualizadas de terceiros, inclusive de crianças e adolescentes, a partir de fotografias reais fornecidas pelos usuários, sem qualquer verificação de consentimento, idade ou finalidade legítima. Denúncias de conteúdo semelhante foram apresentadas simultanea-

mente pelo Instituto Brasileiro de Defesa do Consumidor (Idec), pelo Instituto Alana e pela Secretaria de Políticas Digitais da Presidência da República.

A Coordenação de Fiscalização da ANPD realizou testes próprios entre os dias 9 e 16 de janeiro de 2026, utilizando imagens de seus próprios servidores. Os resultados confirmaram a verossimilhança da denúncia: o Grok, mediante fornecimento de fotografia real pelo usuário, alterou o contexto original da imagem, trocando as roupas da pessoa retratada e inserindo-a em contexto íntimo e sexualizado. A citada Nota Técnica nº 1/2026/FIS/CGF/ANPD, publicada em 20 de janeiro de 2026, concluiu que a integração e operacionalização do Grok na Plataforma X é potencialmente incompatível com os arts. 6º, 11, 14, 46, §2º, e 49 da LGPD (Brasil, 2018; 2026).

A análise jurídica da ANPD estabelece pontos fundamentais para a compreensão do problema. Primeiro, o conteúdo sintético gerado por sistemas de IA constitui dado pessoal nos termos do art. 5º, I, da LGPD sempre que se referir, direta ou indiretamente, a pessoas naturais identificadas ou identificáveis (Brasil, 2018). Segundo, quando esse conteúdo envolver dados biométricos — como imagens faciais —, assume a qualificação de dado pessoal sensível, sujeito ao regime mais restritivo do art. 11 da LGPD (Brasil, 2018). Terceiro, e talvez mais importante para fins de responsabilidade: a ANPD afastou expressamente a tese de neutralidade da plataforma. A funcionalidade foi integrada deliberadamente à infraestrutura tecnológica do X; a materialização do resultado lesivo decorre do design do produto, não apenas da conduta do usuário (Brasil, 2026). Portanto, incumbe à plataforma a responsabilidade integral pelas salvaguardas técnicas e administrativas.

A Nota Técnica documentou, ainda, que, segundo estimativas, o sistema teria gerado uma imagem sexualizada não consensual por minuto durante determinado período. Mesmo após anúncios de atualizações e restrições pela Plataforma X, jornalistas constataram que a produção de conteúdo não consensual continuava possível. A ANPD concluiu que as medidas de mitigação adotadas pela empresa eram insuficientes, caracterizando falha estrutural na arquitetura de governança de dados do modelo — não um evento isolado (Brasil, 2026).

A dimensão internacional do caso é igualmente relevante. A Ofcom britânica abriu investigação formal. A autoridade italiana Garante advertiu sobre violações ao *General Data Protection Regulation* (GDPR). A Comissão Europeia iniciou apuração própria. A Malásia e a Indonésia bloquearam o acesso ao Grok.

A ANPD e a *Commission Nationale de l'Informatique et des Libertés* (CNIL) francesa reforçaram, nesse contexto, sua cooperação bilateral em matéria de proteção de dados e inteligência artificial, sinalizando que a fiscalização de sistemas de IA generativa será progressivamente coordenada em nível internacional (Grok [...], 2026).

Para o advogado brasileiro, o caso Grok tem uma lição direta: não é suficiente verificar se uma plataforma de IA afirma estar em conformidade com a LGPD, é necessário avaliar sua arquitetura de governança, suas políticas efetivas de uso, suas medidas técnicas de prevenção de danos e seu histórico documentado de conformidade. O caso demonstra que declarações de conformidade e políticas internas de uso podem coexistir com falhas estruturais graves que geram responsabilidade legal. A ausência de governança adequada no design de uma ferramenta não é um problema abstrato — é uma violação documentada e sancionável. O advogado que insere dados de clientes em plataformas sem realizar essa avaliação assume um risco que o ordenamento jurídico brasileiro já reconhece, documenta e pune.

7 A JUSTIÇA MILITAR COMO CONTEXTO ESPECÍFICO

Os deveres éticos discutidos nas seções anteriores aplicam-se a toda a advocacia brasileira. Na Justiça Militar — tanto estadual quanto federal, incluindo o Superior Tribunal Militar —, esses deveres operam em um contexto que agrava significativamente as obrigações e os riscos.

A Justiça Militar lida regularmente com informações de natureza restrita ou confidencial: dados funcionais de militares, informações sobre operações, hierarquia e disciplina das Forças Armadas, matérias que podem ter implicações para a segurança nacional. Cabe apontar que, apesar dessas informações não terem normalmente classificação de segurança, quando usadas de forma uniforme, podem dar uma visão bem clara da situação operativa das Forças. O advogado que atua nesse contexto e utiliza plataformas de IA generativa com dados de seus clientes militares pode estar expondo informações cujo vazamento não tem apenas consequências civis ou disciplinares — pode ter implicações para a segurança operacional.

Há ainda a questão da imparcialidade e do sigilo processual, no caso de processos na Justiça Militar que tramitem em sigilo ou com restrições de aces-

so. A inserção de informações de processos sigilosos em plataformas comerciais de IA cria risco de violação do sigilo judicial, além de exposição do conteúdo do processo a terceiros — incluindo potencialmente concorrentes do cliente ou partes adversárias.

A orientação prática para advogados que atuam na Justiça Militar é conservadora: não inserir dados identificadores de clientes, números de processos, informações operacionais ou qualquer dado sensível em plataformas de IA generativa que não ofereçam garantias contratuais explícitas de não utilização dos dados para treinamento e de conformidade com a LGPD. O uso de ferramentas de IA nesse contexto deve limitar-se a tarefas que não envolvam a exposição de dados sensíveis: pesquisa doutrinária genérica, estruturação de argumentos em abstrato, revisão gramatical de textos já anonimizados.

Cabe ainda diferenciar a anonimização da pseudonimização, distinção de grande relevância prática para o uso de IA na advocacia. A anonimização, nos termos do art. 5º, III, da LGPD, é o processo pelo qual um dado perde a possibilidade de ser associado a um indivíduo direta ou indiretamente, de forma definitiva (Brasil, 2018). Um dado verdadeiramente anonimizado deixa de ser dado pessoal e sai do escopo da LGPD. Já a pseudonimização, prevista no art. 13, § 4º, é o tratamento pelo qual um dado perde a possibilidade de associação direta a um indivíduo, mas mediante uso de informação adicional guardada separadamente (Brasil, 2018). O dado pseudonimizado permanece dado pessoal e continua sujeito à LGPD. Para o advogado que pretende usar ferramentas de IA com informações de clientes, a pseudonimização — substituir nomes e identificadores diretos por códigos antes de inserir o conteúdo na plataforma — é uma medida de mitigação importante, mas não elimina a obrigação de consentimento nem afasta o risco residual de reidentificação por cruzamento de dados. Apenas a anonimização genuinamente irreversível exclui o dado do regime da LGPD — e a ANPD tem sido rigorosa ao analisar se a anonimização é de fato eficaz.

O caso Grok, analisado na seção anterior, ilustra com precisão os riscos específicos que o uso de plataformas inadequadas representa no contexto da Justiça Militar: se dados de usuários comuns foram expostos por falha estrutural de governança, dados operacionais e processuais de natureza militar comportam riscos ainda maiores. Obviamente, quaisquer informações restritas ou confidenciais, dados pessoais, inclusive os sensíveis, inseridos em platafor-

mas de IA públicas passam a integrar o banco de dados dessas plataformas e podem aparecer em resultados de pesquisas realizadas por terceiros.

Tais regras se aplicam também a Sindicâncias, Inquéritos Policiais Militares (IPMs) e Conselhos de Disciplina ou Justificação. Os oficiais responsáveis por tais atos terão que tomar as mesmas precauções para evitar qualquer potencial nulidade de atos essenciais à Justiça Militar.

8 CONSIDERAÇÕES FINAIS

A resposta aos riscos identificados não é a renúncia ao uso de ferramentas de IA, mas em seu uso informado, supervisionado e documentado, dentro de um *framework* de governança adequado.

O advogado que pretende utilizar ferramentas de IA deve compreender como funcionam, quais são suas limitações documentadas — incluindo alucinação, viés de treinamento e deriva de confiança — e quais são as políticas de privacidade e uso de dados das plataformas que utiliza. Ignorar essas informações não é uma opção profissional. O advogado não precisa se tornar um programador, mas precisa saber usar essas ferramentas como, por exemplo, sabe dirigir um carro sem ser mecânico.

Conforme exige a Recomendação OAB nº 001/2024, o cliente deve ser informado por escrito sobre o uso de IA, os riscos envolvidos e as medidas de segurança adotadas. Esse consentimento informado e específico deve ser obtido antes do uso, não formalizado a posteriori. Essa autorização não só tem que estar no contrato, mas com destaque.

Toda jurisprudência, doutrina, legislação ou argumentação produzida por ferramenta de IA deve obrigatoriamente ser verificada antes de ser utilizada em documento jurídico. A verificação não é uma precaução adicional, é o padrão mínimo de diligência.

O advogado deve manter registro do que foi produzido com auxílio de IA, quais verificações foram realizadas e quais foram os resultados. Essa documentação do processo é necessária tanto para fins de responsabilidade profissional quanto para eventual demonstração de diligência perante o cliente ou o tribunal.

Dados confidenciais e sensíveis de clientes, informações processuais sigilosas e qualquer informação que possa comprometer a segurança do cliente

ou de terceiros não devem ser inseridos em plataformas de IA que não ofereçam garantias contratuais explícitas de proteção. Na dúvida, a orientação é ser conservador.

Finalmente, cabe ressaltar que muitos desses problemas e questões não são novos e vão desde a edição seletiva de texto de acórdãos citados a uso indevido de imagens em processos. Por volta de 1992, quando ainda lecionava na PUC/RJ, o então professor de Mandado de Segurança e Desembargador Carlos Alberto Menezes Direito, posteriormente Ministro do Supremo Tribunal Federal, comentou o mal-estar instaurado no Tribunal em razão de advogado atuando em causa própria ter promovido a juntada de centenas, ou mesmo milhares, de fotos íntimas de sua esposa, após mais de vinte anos de casamento, no contexto de separação litigiosa. Não cabe discutir o caso substantivo, mas a questão processual foi a declaração imediata de segredo de justiça, que não era a regra aplicada na época, apesar da previsão legal. O advogado fez isso, literalmente, para ferir a moral da sua esposa. O professor alegou, ainda, que era ele quem estava tirando as fotos e, em caso de críticas, teriam que ser feitas a ele e à esposa, em especial a ele, pois tinham fotos da época de namoro e noivado. O ocorrido se deu em uma época sem difusão de internet. Hoje isso é, sem dúvidas, um crime, até porque a possibilidade de difusão é infinita e o dano permanente. O ponto é que as soluções existem, basta serem aplicadas com rigor e atenção à natureza essencial do caso concreto.

A inteligência artificial é uma ferramenta poderosa que chegou para ficar. Como ocorre com toda ferramenta de elevada capacidade operacional, o resultado de seu uso depende da competência, do julgamento e da responsabilidade de quem a utiliza. Os deveres éticos do advogado não foram alterados pelo surgimento da IA, foram maximizados. A exigência de competência, diligência e sigilo continua intacta, o que mudou é o que é necessário para cumpri-la. O advogado que utiliza IA sem governança adequada não está sendo inovador, mas sim negligente.

REFERÊNCIAS

ADVOGADA concorda com multa por mau uso de IA, mas culpa estagiário. **Migalhas**, Ribeirão Preto, 16 maio 2025. Disponível em: <https://www.migalhas.com.br/quentes/435670/advogada-concorda-com-multa-por-mau-uso-de-ia-mas-culpa-estagiario>. Acesso em: 10 maio 2025.

AMERICAN BAR ASSOCIATION. **ABA issues first ethics guidance for AI tools.** Chicago, 29 jul. 2024. Disponível em: <https://www.americanbar.org/news/abanews/aba-news-archives/2024/07/aba-issues-first-ethics-guidance-ai-tools/>. Acesso em: 10 maio 2025.

BRASIL. **Lei nº 13.105, de 16 de março de 2015.** Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 10 maio 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 maio 2025.

BRASIL. Senado Federal. **Projeto de Lei n.º 2.338, de 2023.** Dispõe sobre o uso da inteligência artificial. Brasília, DF: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 10 maio 2025.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 615, de 14 de março de 2025.** Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. Brasília, DF: CNJ, 2025. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/6001>. Acesso em: 10 maio 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Nota Técnica nº 1/2026/FIS/CGF/ANPD.** Brasília, DF: ANPD, 2026. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-1-2026-fis-cgf-anpd.pdf/@@display-file/file>. Acesso em: 10 maio 2025.

CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL. **Código de Ética e Disciplina da OAB.** Brasília, DF: CFOAB, 2015. Disponível em: <https://www.oab.org.br/publicacoes/AbrirPDF?LivroId=0000004085>. Acesso em: 10 maio 2025.

ESTADOS UNIDOS DA AMÉRICA. United States District Court for the Southern District of New York. **Mata v. Avianca, Inc.**, No. 1:22-cv-01461-PKC, Opinion and Order on Sanctions. Relator: Judge P. Kevin Castel. New York, 22 jun. 2023. Disponível em: <https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2022cv01461/575368/54/>. Acesso em: 10 maio 2025.

GROK sexual deepfake scandal. **Wikipedia:** the free encyclopedia, [S. l.], [2026?]. Disponível em: https://en.wikipedia.org/wiki/Grok_sexual_deepfake_scandal. Acesso em: 10 maio 2025.

maio 2025.

ORDEM DOS ADVOGADOS DO BRASIL. Conselho Federal. Recomendação n. 001/2024: apresenta diretrizes para orientar o uso de Inteligência Artificial generativa na prática jurídica. **Diário Eletrônico da OAB**, Brasília, DF, ano VI, n. 1483, p. 1, 14 nov. 2024. Disponível em: <https://diario.oab.org.br/pages/materia/842347>. Acesso em: 10 maio 2025.