JNT FACIT BUSINESS AND TECHNOLOGY JOURNAL
ISSN: 2526-4281 - ANO 2026 - MÊS DE ABRIL
Ed. 73. Vol. 1 - Págs. 290-306
DOI: 10.5281/zenodo.19554464

CAPES

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

QUALIS A2

O USO DO CHAT GPT E GEMINI NA ELABORAÇÃO DE PEÇAS PROCESSUAIS: ANÁLISE DA RESPONSABILIDADE DO ADVOGADO PELO TRATAMENTO DE DADOS PESSOAIS E SENSÍVEIS SOB A ÓTICA DA LEGISLAÇÃO BRASILEIRA[1]

THE USE OF CHATGPT AND GEMINI IN DRAFTING LEGAL DOCUMENTS: ANALYSIS OF THE LAWYER'S RESPONSIBILITY FOR THE PROCESSING OF PERSONAL AND SENSITIVE DATA UNDER BRAZILIAN LAW

João Marcelo Ferreira SILVA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: joaomarceloferreirasilva9@gmail.com
ORCID: http://orcid.org/0009-0001-0057-4480

João Marcos Ferreira SILVA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: ferreirasilvajoaomarcos@gmail.com
ORCID: http://orcid.org/0009-0009-5985-2404

Júlia Feitosa COSTA
Faculdade de Ciências do Tocantins (FACIT)
E-mail: juliafeitosaadvocacia@gmail.com
ORCID: http://orcid.org/0009-0000-2960-5028

RESUMO

A crescente integração da Inteligência Artificial na advocacia, embora proporcione ganhos de eficiência, suscita preocupações quanto ao dever ético de sigilo profissional e à proteção de dados. Este estudo objetiva analisar os desafios éticos e jurídicos enfrentados pelo advogado na utilização de IA, à luz da Lei Geral de Proteção de Dados (LGPD) e do Código de Ética da OAB. A pesquisa identifica as vulnerabilidades no uso dessas tecnologias, examina o dever de sigilo a partir da jurisprudência do STJ e discute a responsabilidade disciplinar, civil e penal do advogado. A metodologia adotada é a revisão bibliográfica e documental, com análise crítica da legislação, doutrina e políticas de privacidade de ferramentas como ChatGPT e Gemini. Os resultados indicam que o dever de sigilo, reforçado pela vedação de revelação de informações a terceiros (art. 27, parágrafo único, do Código de Ética da OAB), entra em conflito direto com os termos de uso de diversas IAs, especialmente em versões

[1] COMO CITAR: (ABNT): SILVA, J. M. F.; SILVA, J. M. F.; COSTA, J. F. O Uso do Chat GPT e Gemini na Elaboração de Peças Processuais: Análise da Responsabilidade do Advogado pelo Tratamento de Dados Pessoais e Sensíveis sob a Ótica da Legislação Brasileira. **JNT Facit Business and Technology Journal.** Qualis A2. ISSN: 2526-4281, Mês de Abril de 2026 - Ed. 73. VOL. 01. Págs. 290-306. Disponível: http://revistas.faculdadefacit.edu.br. Acesso em: ___/___/___.

gratuitas que utilizam dados inseridos para treinamento de algoritmos. Conclui-se que o advogado, na condição legal de controlador de dados, não pode eximir-se de sua responsabilidade, sendo a "culpa na escolha" (*culpa in eligendo*) e a "culpa na vigilância" (*culpa in vigilando*) elementos determinantes para sua responsabilização objetiva em casos de vazamento.

Palavras-chave: Inteligência Artificial. Advocacia. Proteção de dados. LGPD. Responsabilidade civil.

ABSTRACT

The increasing integration of Artificial Intelligence in legal practice, although providing efficiency gains, raises significant concerns regarding the ethical duty of professional confidentiality and data protection. This study aims to analyze the ethical and legal challenges faced by lawyers when using AI, in light of the Brazilian General Data Protection Law (LGPD) and the Brazilian Bar Association (OAB) Code of Ethics. The research identifies vulnerabilities in the use of these technologies, examines the duty of secrecy based on the jurisprudence of the Superior Court of Justice (STJ), and discusses the lawyer's disciplinary, civil, and criminal liability. The methodology adopted is a bibliographic and documentary review, featuring a critical analysis of legislation, legal doctrine, and the privacy policies of tools such as ChatGPT and Gemini. The results indicate that the duty of confidentiality, reinforced by the prohibition of disclosing information to third parties (Art. 27, Sole Paragraph, of the OAB Code of Ethics), directly conflicts with the terms of use of several AIs, especially in free versions that use inputted data for algorithm training. It is concluded that the lawyer, in the legal capacity of a data controller, cannot evade their responsibility, with "fault in choosing" (*culpa in eligendo*) and "fault in supervising" (*culpa in vigilando*) being determining elements for their objective liability in cases of data breaches.

Keywords: Artificial Intelligence. Legal practice. Data protection. LGPD. Civil liability.

INTRODUÇÃO

A prática da advocacia, tradicionalmente alicerçada na análise documental analógica e no rigor formal, vivencia atualmente uma transição paradigmática impulsionada pela Revolução Digital. O advento das *legaltechs* e o aprimoramento da Inteligência Artificial (IA) reconfiguraram as rotinas dos escritórios de advocacia, substituindo métodos morosos por sistemas de automação de alta eficiência. Nesse

cenário de transformação, a Inteligência Artificial Generativa desponta não apenas como uma ferramenta acessória capaz de interpretar comandos complexos em linguagem natural e gerar textos jurídicos com um nível de sofisticação outrora restrito ao intelecto humano.

O uso prático de Grandes Modelos de Linguagem (LLMs), notadamente o Chat GPT, desenvolvido pela OpenAI, e o Gemini, operado pelo Google, tem se tornado cada vez mais onipresente na rotina jurídica. A atratividade dessas plataformas reside na sua capacidade de otimizar o tempo e potencializar a capacidade analítica do profissional do Direito. Na prática diária, os advogados têm submetido a esses sistemas comandos interativos (*prompts*) para finalidades altamente estratégicas. Destaca-se, primordialmente, a elaboração de petições, onde a IA é alimentada com os fatos do caso concreto para redigir peças processuais estruturadas e fundamentadas. Soma-se a isso a revisão de contratos, modalidade em que minutas, acordos extrajudiciais e documentos corporativos extensos são inseridos na plataforma para o mapeamento de riscos jurídicos, detecção de cláusulas abusivas e sugestão de melhorias redacionais. Por fim, as ferramentas são amplamente empregadas na criação de teses jurídicas, atuando como um assistente de pesquisa que cruza bilhões de dados para sugerir estratégias de defesa ou teses de acusação.

Contudo, a premissa técnica para que a Inteligência Artificial generativa entregue resultados precisos e úteis ao caso concreto é a necessidade incontornável de o operador fornecer um contexto fático detalhado. É neste exato ponto de intersecção entre a eficiência tecnológica e a deontologia jurídica que emerge o núcleo de tensão desta pesquisa. Para redigir uma petição de divórcio, analisar um contrato de fusão empresarial ou elaborar uma tese de defesa criminal, o advogado é compelido a inserir nos campos de *prompt* informações que englobam o nome de clientes, dados financeiros, diagnósticos médicos e confissões íntimas. Tais informações são classificadas pelo ordenamento jurídico pátrio como dados pessoais e dados pessoais sensíveis, submetidos ao rigor protetivo da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018).

A inserção de tais dados em plataformas operadas por empresas de tecnologia terceirizadas (*big techs*) acarreta repercussões imediatas sobre um dos pilares mais sagrados e antigos da profissão: o sigilo profissional, consagrado no Estatuto da Advocacia e da OAB (Lei nº 8.906/1994) e no Código de Ética e Disciplina da OAB. Diante das complexas políticas de privacidade dessas plataformas, que frequentemente preveem o uso dos dados inseridos para o treinamento de novos algoritmos e até mesmo a revisão do conteúdo por humanos, a adoção acrítica da IA

deixa de ser uma mera questão de inovação operacional para se tornar um iminente risco jurídico.

Diante deste cenário, a presente pesquisa é norteada com a problemática central sobre possibilidade na inserção de dados de clientes em ferramentas de IA generativa, violando o dever de sigilo profissional? Ademais existe a possibilidade da responsabilidade civil ao advogado dentro das normas da Lei geral de proteção de dados?

Para responder tais questionamentos, o estudo adota como hipótese preliminar a confirmação de que a utilização indiscriminada e acrítica dessas tecnologias, especialmente em suas versões de consumo (gratuitas ou de baixo custo), configura uma violação objetiva do dever ético de sigilo profissional. Sustentando-se que o advogado, ao decidir unilateralmente inserir informações sigilosas nessas plataformas, atrai para si a condição jurídica de controlador de dados, assumindo a responsabilização civil perante o titular dos dados por eventuais danos materiais e morais, além de sujeitar-se a graves sanções disciplinares e, em tese, penais, decorrentes da quebra de confidencialidade (*culpa in eligendo* e *culpa in vigilando*).

Para esgotar a problemática apresentada, delineou-se como objetivo geral analisar a responsabilidade civil do advogado pelo uso de ferramentas como Chat GPT e Gemini na elaboração de peças processuais e revisão de documentos, sob a ótica do tratamento de dados pessoais e sensíveis regulamentado pela legislação brasileira.

O USO DE IA GENERATIVA NA ELABORAÇÃO DE PEÇAS JURÍDICAS

A Inteligência Artificial no cenário atual, não é apenas mais uma ferramenta, mas um agente transformador. Conforme destacam Queiroz et al. (2024, p. 2706), a principal vantagem da IA na advocacia é o aumento da eficiência, pois ela permite a automação de tarefas rotineiras e repetitivas, como a revisão de documentos e a pesquisa jurídica. Isso libera o tempo do profissional para que ele possa se dedicar a questões estratégicas e complexas o que proporciona maior celeridade na tramitação processual e que exigiram dias de pensamento críticos para verificação do caso concreto com a legislação ou com a jurisprudência atual.

Segundo levantamento setorial conduzido pela OAB São Paulo em parceria com instituições de tecnologia, mais da metade dos profissionais jurídicos (55,1%) já atua como usuário frequente de inteligência artificial generativa. Destaca-se, contudo, que essa incorporação tem se dado majoritariamente por iniciativa dos próprios profissionais, sem uma política institucional definida pelas organizações em que atuam (OAB SP *et al*, 2025). Esse cenário de uso autônomo e despadronizado

corrobora a preocupação de que a ferramenta venha sendo utilizada sem a exata compreensão e mitigação dos perigos ético-jurídicos envolvidos.

O Funcionamento da Inteligência Artificial Generativa

O conceito de Inteligência Artificial (IA) reflete uma longa evolução histórica e filosófica. Conforme aponta Alencar (2022, p. 8), a compreensão de uma máquina inteligente foi delineada em 1950 por Alan Turing, que estabeleceu que um algoritmo seria considerado "inteligente" quando conseguisse simular o comportamento e a linguagem humana de forma convincente.

Atualmente, essa ambição se materializa na IA generativa. Alimentadas por um volume colossal de dados (*big data*), essas tecnologias operam a partir de uma arquitetura conhecida como Grandes Modelos de Linguagem (LLMs - *Large Language Models*), fundamentada em redes neurais artificiais profundas. Diferentemente dos *softwares* tradicionais de gestão jurídica, a IA generativa utiliza o aprendizado de máquina (*machine learning*) para realizar cálculos matemáticos altamente complexos, mapeando bilhões de conexões probabilísticas entre fragmentos de texto (chamados de *tokens*). O sistema não "pensa", mas prevê qual é o próximo termo mais provável de aparecer em uma frase, e no final de tudo a resposta aparece quase que impecável ao olho humano, sem erros de português, uso de gramáticas avançadas e até se adaptando de acordo com o usuário que faz os comandos por meios dos prompts.

Para alcançar essa sofisticada capacidade de geração de respostas em texto, é necessário que os dados sejam extraídos da internet, incluindo livros e códigos. Também serão utilizados os dados que os próprios usuários inserem nas plataformas de inteligência artificial. Essa realidade gera uma preocupação relevante no âmbito da advocacia, especialmente quando o profissional, por desconhecimento sobre o funcionamento e as implicações dessas ferramentas, insere dados sensíveis de seus clientes nas plataformas. Embora não haja intenção de causar prejuízo, a falta de conhecimento técnico pode resultar na exposição indevida de informações confidenciais, afetando diretamente os interesses do cliente. Dessa forma, observa-se a existência de um paradoxo: ao mesmo tempo em que o profissional do Direito utiliza a inteligência artificial para aprimorar seus serviços e aumentar a eficiência de seu trabalho, o uso inadequado dessas ferramentas pode comprometer significativamente o dever de sigilo profissional que rege a advocacia.

A Prática dos Prompts e o Tratamento de Dados Pessoais

A interação entre o controlador, no caso, o advogado, e a inteligência artificial ocorre por meio de um mecanismo relativamente simples: os *prompts*. Os *prompts* consistem nos comandos ou instruções fornecidas pelo usuário à inteligência artificial, seja para obter uma resposta objetiva, seja para aprimorar um texto que será utilizado, por exemplo, em uma peça jurídica. Na prática, a precisão do *prompt* vai influenciar diretamente na qualidade das informações geradas pela inteligência artificial. Quanto mais claro e específico for o comando, maior será a qualidade do resultado obtido. Entretanto, é justamente nessa busca por respostas mais precisas que reside um dos principais riscos. Para produzir textos cada vez mais específicos e contextualizados, a inteligência artificial depende da inserção de dados igualmente detalhados, o que pode envolver informações sensíveis ou confidenciais dos clientes.

A seguir, demonstramos as três principais formas de utilização dessas ferramentas e como elas expõem dados sensíveis:

A) Elaboração de Petições

Exemplo de Prompt: *"Atue como um advogado. Elabore uma petição inicial de indenização contra a companhia aérea [Nome], baseada no cancelamento do voo em [Data]. O autor, [Nome do Cliente], portador do CPF[Número], perdeu uma reunião crucial, o que agravou seu quadro de ansiedade clínica crônica. Utilize jurisprudência recente do STJ e também todos os documentos em anexos que enviei.*

A Inserção de Dados: Neste comando, o advogado forneceu dados de identificação direta e expôs uma informação sobre a saúde mental do cliente, o que a LGPD classifica expressamente como dado pessoal sensível (Art. 5º, II).

O perigo de vazamento não é hipotético, mas um evento já concretizado em incidentes de segurança de grande repercussão. Em reportagem de 1º de agosto de 2025, o portal G1 noticiou uma grave falha que expôs dados de usuários do ChatGPT:

> Conversas de usuários com o ChatGPT estavam sendo indexadas e exibidas no Google. Pelo menos 4.500 links apareciam no buscador, muitos com informações pessoais e de identidade, segundo o site Fast Company [...]. Em um dos casos identificados, uma pessoa detalhava ao ChatGPT sua vida sexual, comentava sobre a infelicidade de morar em outro país e buscava apoio para lidar com transtorno de estresse pós-traumático. A exibição de conversas foi confirmada por Dane Stuckey, chefe de segurança da OpenAI, dona do ChatGPT, em uma publicação no X. Segundo o executivo, um novo recurso que torna os bate-papos públicos em buscadores pode explicar o ocorrido (Helder, 2025, s/p).

Um erro desse tipo é fatal para a advocacia. O vazamento de informações de clientes, expondo dados que podem prejudicar o processo, além de dados sensíveis,

viola o Estatuto da OAB. O artigo 34, inciso VII, prevê que tal conduta configura infração disciplinar, podendo resultar em penalidade de suspensão, além de outras sanções previstas na Lei Geral de Proteção de Dados. Dessa forma, entende-se que, ao inserir dados de clientes em plataformas de inteligência artificial, como ChatGPT ou Gemini, o advogado corre sérios riscos de comprometer tanto o processo do cliente quanto a própria profissão.

O ADVOGADO COMO CONTROLADOR DE DADOS NA LGPD

Para compreender a dinâmica da responsabilidade civil e ética no tratamento de informações sigilosas, é imperativo definir o agente central dessa cadeia: o controlador. Conforme leciona Garcia (2020, p. 126), a Lei Geral de Proteção de Dados (LGPD) estabelece o controlador como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". No escopo da prática jurídica contemporânea, o advogado ou o escritório de advocacia assume inequivocamente esta posição. Ao optar por utilizar ferramentas de inteligência artificial generativa, como o Chat GPT ou o Gemini, para a redação de peças ou revisão documental, é o profissional do direito quem determina a finalidade e os meios do processamento dos dados de seus clientes. Sendo assim, o papel do controlador atrai para si o dever primordial de governança e segurança, uma vez que a decisão unilateral de inserir informações confidenciais nos *prompts* dessas plataformas dita o risco de exposição e a consequente violação da privacidade e do sigilo profissional.

A figura principal, contudo, recai sobre o advogado e seu escritório. Ao recolher as informações de seu cliente e decidir inseri-las em uma ferramenta de Inteligência Artificial para otimizar a elaboração de uma tese de defesa, o profissional do Direito assume integralmente a posição de controlador de dados (Art. 5º, inciso VI), pois é a ele que competem "as decisões referentes ao tratamento de dados pessoais". É desta premissa legal que deriva o seu dever de vigilância e a sua responsabilização civil, uma vez que o controlador atrai para si o risco e o dever primário de garantir a segurança cibernética dos fatos que lhe foram confiados sob a égide do sigilo.

Essa posição de controlador impõe uma série de obrigações. Conforme aponta Soler (2022, p. 14), o princípio da segurança (Art. 6º, VII) exige a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas". Isso significa que o advogado não pode simplesmente adotar uma ferramenta de IA sem antes realizar uma análise

criteriosa de suas políticas de segurança, seus termos de serviço e sua adequação à LGPD. A responsabilidade é clara no Art. 42, que estabelece que o controlador ou operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar dano a outrem, é obrigado a repará-lo.

Este novo panorama transforma a responsabilidade civil do advogado na era da IA em um campo fértil para litígios. Conceitos clássicos como a "culpa na escolha" (*culpa in eligindo*) ou a "culpa na vigilância" (*culpa in vigilando*) sobre as ferramentas tecnológicas adotadas podem agora ser invocados para fundamentar a responsabilização do profissional. Um incidente de segurança que exponha dados de clientes não pode mais ser visto como uma fatalidade imprevisível, mas como uma possível falha no dever de diligência imposto tanto pelo Código de Ética quanto pela LGPD.

A falha na diligência na proteção de dados de clientes, especialmente quando resulta em um vazamento de informações, expõe o advogado a um complexo espectro de responsabilidades que se desdobram em múltiplas esferas: disciplinar, civil, administrativa e até mesmo criminal. Cada uma dessas áreas impõe sanções específicas, demonstrando a gravidade com que o ordenamento jurídico trata a quebra da confidencialidade.

No âmbito disciplinar, a responsabilidade é direta e está prevista no Estatuto da Advocacia e da OAB (Lei nº 8.906/1994). A violação do sigilo é classificada como uma infração grave, que atenta contra um dos pilares da profissão, conforme estabelece o diploma: “Art. 34. Constitui infração disciplinar: VII – violar, sem justa causa, sigilo profissional” (Brasil, 1994, s/p).

O fundamento ético para essa infração é detalhado de forma contundente pelo Código de Ética e Disciplina da OAB. O Art. 25 estabelece o sigilo como "inerente à profissão", mas para o contexto tecnológico, a norma mais incisiva encontra-se no Art. 27, Parágrafo Único, que proíbe expressamente a revelação de comunicações a terceiros: “Parágrafo único. Presumem-se confidenciais as comunicações epistolares entre advogado e cliente, as quais não podem ser reveladas a terceiros” (OAB, 2015, s/p).

A aplicação deste dispositivo ao cenário digital é direta e inequívoca. Uma plataforma de Inteligência Artificial, operada por uma empresa de tecnologia como a OpenAI ou o Google, é, por definição, um "terceiro" na relação jurídica cliente-advogado. Portanto, o ato de inserir dados confidenciais em tais sistemas, especialmente em versões que utilizam o conteúdo para treinamento de algoritmos,

configura uma revelação a terceiro, violando frontalmente o dever ético e, consequentemente, incorrendo na infração disciplinar.

Finalmente, a Lei Geral de Proteção de Dados (LGPD) estabelece o mais robusto e, talvez, o mais temido regime de responsabilidade. Primeiramente, na esfera civil, o Art. 42 impõe o dever de reparação integral dos danos causados aos titulares dos dados:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (Brasil, 2018, s/p).

ANÁLISE DOS TERMOS DE USO DO CHATGPT E GEMINI

A adoção de ferramentas de Inteligência Artificial pelo advogado não pode ser dissociada de uma análise rigorosa dos termos contratuais que regem essas plataformas. As Políticas de Privacidade e os Termos de Serviço não são meras formalidades, mas sim documentos jurídicos que delimitam o escopo do tratamento dos dados inseridos, as responsabilidades das partes e os riscos assumidos pelo usuário. Para o advogado, que atua como controlador dos dados de seus clientes sob a ótica da LGPD, a compreensão desses termos é um componente indissociável de seu dever de diligência e sigilo profissional. A seguir, será realizada uma análise crítica das políticas de privacidade de duas das mais proeminentes IAs generativas: o ChatGPT, da OpenAI, e a API Gemini, do Google.

A Política de Privacidade do ChatGPT (OpenAI): O Uso de Conteúdo para Treinamento

A Política de Privacidade da OpenAI, que rege a utilização do ChatGPT, estabelece uma distinção crucial entre as diferentes categorias de dados coletados. De um lado, encontram-se as "Informações da conta" (nome, credenciais, dados de pagamento) e os "Dados de registro e de utilização" (endereço IP, tipo de navegador, interações com a plataforma) (OpenAI, 2026). De outro, e de relevância ímpar para a prática advocatícia, está o "Conteúdo do Usuário", definido expressamente pela empresa como as solicitações (*prompts*) e outros materiais que o usuário carrega no serviço, tais como arquivos, imagens e textos. Na rotina jurídica, isso se traduz no envio de peças processuais, detalhes fáticos de litígios e minutas contratuais.

O ponto de maior sensibilidade e risco para a advocacia encontra-se na seção normativa que disciplina a utilização desses dados. A OpenAI declara expressamente que se utiliza do conteúdo inserido na plataforma para aprimorar seus algoritmos. A

política de privacidade afirma, de forma literal: "Podemos usar o Conteúdo para fornecer, manter, desenvolver e aprimorar nossos Serviços [...] por exemplo, para treinar os modelos que alimentam o ChatGPT" (OpenAI, 2026).

Essa previsão contratual representa um conflito direto e frontal com o dever ético de sigilo do advogado. Ao inserir dados confidenciais de um cliente, como estratégias de defesa criminal, informações financeiras de uma fusão corporativa ou detalhes íntimos de uma disputa familiar, o advogado que utiliza as versões de consumo da plataforma (Gratuita, Plus ou Pro) está, sob os termos padrão, consentindo que essas informações sejam utilizadas para o treinamento de um modelo de Inteligência Artificial global. Embora a OpenAI ofereça a possibilidade de *opt-out* (opção de cancelar a participação no treinamento de modelos), essa não é a configuração padrão da ferramenta para usuários comuns. A responsabilidade de acessar as configurações e desativar ativamente o compartilhamento de dados recai de forma exclusiva sobre o usuário, exigindo um conhecimento técnico e uma proatividade diligente que nem todos os profissionais do Direito possuem. A simples existência de uma opção de *opt-in* por padrão para o uso de dados confidenciais torna o uso irrefletido da plataforma eticamente insustentável para a prática jurídica.

Os Termos de Serviço da API Gemini (Google): termos de uso do Gemini

A abordagem do Google em relação à sua API Gemini apresenta uma nuance contratual fundamental que impacta diretamente a análise de risco pelo advogado, para isso devemos entender a distinção explícita entre "Serviços Não Pagos" e "Serviços Pagos" (Google, 2025), sabendo dessa diferenciação, o advogado entenderá melhor as nuances do uso dessa inteligência artificial no dia a dia da advocacia.

Nos serviços não pagos, que incluem o uso direto da interface do *Google AI Studio* ou a cota gratuita da API, os termos são inequívocos e alarmantes para o uso profissional. O Google afirma expressamente que utiliza o conteúdo enviado (entradas/*prompts*) e as respostas geradas (saídas) para "fornecer, aprimorar e desenvolver produtos, serviços e tecnologias de aprendizado de máquina" (Google, 2025).

Mais criticamente, a política de uso estabelece a revisão humana do conteúdo, alertando que "revisores humanos podem ler, fazer anotações e tratar suas entradas e saídas das APIs". O próprio documento finaliza com uma advertência peremptória: "Não envie informações sensíveis, confidenciais ou pessoais para os serviços não pagos" (Google, 2025). Para o advogado, essa cláusula torna a utilização da versão gratuita da API Gemini eticamente inviável. A submissão de dados de clientes à

revisão humana e o seu uso explícito para o treinamento de modelos configuram violação direta, intencional e indefensável do sigilo profissional.

Em contrapartida, nos serviços pagos, a política muda drasticamente. O Google estabelece que "não usa seus comandos [...] ou respostas para aperfeiçoar os produtos" (Google, 2025). Nesse modelo, a relação jurídica passa a ser regida por um adendo específico de tratamento, no qual a empresa se posiciona de forma mais clara como uma "operadora" de dados, agindo sob as instruções do advogado ("controlador"), nos moldes da LGPD.

No que tange ao armazenamento, a política determina que, nas versões pagas, os comandos e respostas são retidos "por um período limitado, exclusivamente com o propósito de detectar violações da Política de Uso Proibido e quaisquer divulgações legais ou regulatórias necessárias", podendo os dados ser armazenados temporariamente ou mantidos em cache nos servidores do Google (Google, 2025).

RESPONSABILIDADE CIVIL DO ADVOGADO PELO USO DE IA

Para comprovar a importância do sigilo profissional o Superior Tribunal de Justiça já decidiu, no julgamento do Recurso em Mandado de Segurança nº 67.105/SP, e com veemência confirmou a inviolabilidade do sigilo profissional. Na decisão, o Relator, Ministro Luis Felipe Salomão, asseverou que o sigilo é uma prerrogativa essencial para a administração da justiça:

> O contrato de prestação de serviços advocatícios está sob a guarda do sigilo profissional, assim como se comunica à inviolabilidade da atividade advocatícia, sendo possível o afastamento daquelas garantias tão somente por meio de ordem judicial expressa e fundamentada e em relação a questões envolvendo o próprio advogado e que sejam relativas a fato ilícito em que ele seja autor (STJ, RMS 67.105/2021, s/p).

A decisão do STJ é de vital importância para a presente análise, pois, em sua fundamentação, o tribunal reforça que "é garantida a inviolabilidade do local de trabalho do advogado, de seus arquivos e dados, de sua correspondência e de suas comunicações" (STJ, RMS 67.105/SP, 2021, item 7 da ementa). Ao utilizar a expressão "arquivos e dados", o tribunal estende a proteção constitucional e legal do sigilo para além dos documentos físicos, abrangendo inequivocamente as informações em formato digital.

Culpa in eligendo e Culpa in vigilando na Era Digital

A responsabilização civil do advogado no contexto da adoção de sistemas de inteligência artificial orbita a clássica teoria da culpa e a prática do ato ilícito. Nesse

sentido, é indispensável a verificação da quebra de um dever legal de cuidado por parte do profissional. Conforme conceitua Carlos Roberto Gonçalves ao analisar o artigo 186 do Código Civil: "[...] não basta, para gerar o dever de indenizar, a prática de um ato lesivo aos interesses de outrem. É indispensável a ilicitude, que constitui a violação de um dever jurídico preexistente" (Gonçalves, 2020, p. 13).

No caso em análise, o dever preexistente violado é exatamente a obrigação de sigilo profissional e de proteção de dados, configurando o comportamento culposo do advogado por negligência ou imprudência no trato das informações sigilosas inseridas em ferramentas tecnológicas não seguras.

O uso incorreto ou negligente de ferramentas de Inteligência Artificial pode gerar a responsabilização do profissional com base no conceito de *culpa in eligendo* (culpa na escolha). A responsabilidade do advogado contemporâneo não se limita mais a contratar um software de gestão com boa reputação no mercado; ela se estende ao dever ativo de ler e compreender os complexos termos de serviço para aferir o nível de proteção contratual oferecido. Ignorar uma advertência explícita, como a que consta nos termos do Google ("Não envie informações sensíveis"), não pode ser tutelada como um mero descuido, mas sim como uma falha grave na eleição da ferramenta de trabalho.

Ademais, essa negligência inicial pode ser agravada pela *culpa in vigilando* (culpa na vigilância). Ainda que utilize uma plataforma dotada de mecanismos de segurança, o advogado incorre nessa modalidade de culpa por omissão quando deixa de gerenciar e configurar corretamente as opções de privacidade, como a desativação do histórico de conversas ou do consentimento para o uso de dados no treinamento de algoritmos, falhando, assim, em sua vigilância tecnológica sobre as informações do cliente.

GUIA DE BOAS PRÁTICAS PARA O USO DE IA NA ADVOCACIA

A análise dos riscos éticos e legais expostos nos capítulos anteriores demonstra que a adoção da Inteligência Artificial na advocacia não é uma questão de "se", mas de "como". A tecnologia, por si só, não é inerentemente boa ou má; sua adequação à prática jurídica depende inteiramente da diligência, da consciência e da conduta do profissional que a utiliza. A percepção de que a IA é apenas um "software" isento de responsabilidades é um equívoco perigoso que ignora o dever de sigilo e as obrigações impostas pela LGPD.

Nesse contexto, a transição para uma prática juridicamente segura no uso de IA exige uma mudança de mentalidade: o advogado deve se enxergar não apenas

como um usuário, mas como um gestor de riscos. Essa perspectiva é fundamental para conciliar inovação com os deveres da profissão. Em webinário intitulado "IA 'do zero'", o Juiz do Trabalho do TRT da 10ª Região e Membro do Comitê Gestor da Segurança Institucional do Poder Judiciário – CNJ, Maximiliano Carvalho (2024), oferece uma visão pragmática e indispensável sobre a segurança de dados. Segundo ele, o primeiro passo para qualquer profissional é a leitura atenta das normas que regem a ferramenta:

> [...] toda inteligência artificial tem uma política de privacidade de dados. Busque ler a política de privacidade de dados dessa inteligência artificial, tente entender se você concorda com aquilo que está escrito lá ou não. E se você concordar, envie, correndo os riscos, porque tudo é gestão de risco e todo mundo está correndo risco, mesmo que digam para você que não tem risco [...] (Carvalho, 2024, s/p).

A premissa de que "tudo é gestão de risco", vinda de uma autoridade com experiência na intersecção entre o Judiciário e a segurança tecnológica, é o ponto de partida para uma advocacia digitalmente responsável. A responsabilidade não pode ser delegada à plataforma; ela é assumida pelo profissional. A partir dessa conscientização, Carvalho (2024) oferece uma diretriz prática e fundamental, que visa mitigar o principal risco associado ao tratamento de dados sensíveis por terceiros.

Para além do imperativo de desativação do uso comercial dos dados, conforme outrora advertido pelo Juiz Maximiliano Carvalho, a conduta eticamente exigível do advogado na adoção da Inteligência Artificial pressupõe a implementação de um protocolo de *compliance* preventivo. Esse protocolo inicia-se por uma rigorosa auditoria contratual prévia, na qual o profissional deve analisar minuciosamente as Políticas de Privacidade e os Termos de Serviço da plataforma, identificando cláusulas abusivas sobre o compartilhamento e o treinamento de dados. Ato contínuo, a mitigação de riscos exige a preferência por modelos profissionais ou corporativos (*Enterprise*), cujos contratos assumem o papel de "operador" sob a LGPD, garantindo maior grau de confidencialidade. Aliado a isso, impõe-se a gestão ativa das configurações de segurança pelo advogado, bloqueando recursos automáticos de histórico e alimentação de algoritmos que possam comprometer o sigilo fático.

Outra estratégia tecnicamente robusta de mitigação de riscos consiste na adoção de modelos de linguagem de grande escala (LLMs) que operam localmente, ou seja, instalados diretamente na máquina do advogado e sem a necessidade de conexão com a internet. Ferramentas específicas permitem que o profissional baixe e execute modelos de IA de código aberto em seu próprio computador. Essa prática cria um

ambiente de "sandbox" (caixa de areia), no qual os dados sensíveis dos clientes são processados integralmente offline. Ao eliminar a transmissão de informações para servidores de terceiros (*big techs*), o advogado mitiga quase que por completo o risco de vazamentos decorrentes de falhas de segurança na nuvem, de compartilhamento indevido ou de uso de dados para treinamento de modelos, assumindo controle total sobre a cadeia de custódia da informação.

Por fim, é imperativo que o advogado discuta a utilização de ferramentas de Inteligência Artificial na elaboração de teses e documentos, formalizando essa ciência de modo prévio e expresso. Tal prática não apenas atende ao princípio matriz da transparência, entabulado no artigo 6º, inciso VI, da Lei Geral de Proteção de Dados (LGPD), como também encontra regulamentação específica na Recomendação nº 001/2024 do Conselho Federal da OAB. O referido documento determina que "[...] o advogado que optar por utilizar ferramentas ou sistemas de Inteligência Artificial na prestação de serviços advocatícios deve, previamente ao início de sua utilização, formalizar tal intenção ao cliente" (OAB, 2024, p. 14).

Essa formalização deve ultrapassar a mera autorização genérica, consubstanciando-se em uma cláusula de consentimento informado elaborada por meio de documento escrito, em linguagem clara e acessível. Conforme a Recomendação da OAB (2024), o advogado deve explicar o propósito do uso da tecnologia, seus benefícios e limitações, os possíveis riscos de exposição de dados ou imprecisões e, notadamente, garantir que haverá revisão humana sobre os resultados obtidos. Assegura-se, ainda, o direito do cliente de recusar o uso da IA em sua demanda. Essa transparência proativa resguarda o profissional de responsabilizações futuras e garante que a inovação tecnológica não suprima a dignidade e a autodeterminação informativa do titular dos dados.

CONSIDERAÇÕES FINAIS

O presente artigo científico debruçou-se sobre a intrincada interseção entre a inovação tecnológica e os deveres basilares da advocacia, investigando os riscos e as responsabilidades decorrentes do uso de ferramentas de Inteligência Artificial generativa, como o ChatGPT e o Gemini, na elaboração de peças processuais. A pesquisa percorreu um caminho metodológico que partiu da contextualização do uso prático dessas ferramentas, passando pela definição do papel do advogado como controlador de dados à luz da Lei Geral de Proteção de Dados (LGPD), analisando criticamente as políticas de privacidade e termos de serviço das plataformas e, por fim, dissecando a tríplice esfera de responsabilização do profissional. O fio condutor

de toda a análise foi responder ao seguinte problema de pesquisa: a inserção de dados de clientes em ferramentas de IA generativa viola o dever de sigilo profissional e gera responsabilidade civil ao advogado nos termos da LGPD?

Ao final da análise científica, confirma-se a hipótese de que a utilização indiscriminada dessas tecnologias, especialmente em suas versões de consumo (gratuitas ou de baixo custo), configura, de fato, uma violação objetiva do dever de sigilo profissional e atrai a responsabilização civil, disciplinar e, em tese, penal do advogado. Ficou demonstrado que os termos contratuais de plataformas como ChatGPT e Gemini preveem, como regra, a utilização dos dados inseridos pelos usuários (*prompts*) para o treinamento de seus algoritmos, bem como a possibilidade de revisão humana desse conteúdo. Tal prática é frontalmente incompatível com o dever de confidencialidade inerente à advocacia, consagrado no Estatuto da OAB, e com o princípio da segurança, pilar da LGPD.

A premissa de que "tudo é gestão de risco" reforça a conclusão central deste trabalho: a responsabilidade não pode ser delegada à plataforma; ela é integralmente assumida pelo profissional. A falha em gerenciar esse risco materializa a *culpa in eligendo* (culpa na escolha da ferramenta) e a *culpa in vigilando* (culpa na ausência de configuração de privacidade), fundamentos clássicos da responsabilidade civil agora aplicados ao universo digital.

Conclui-se, portanto, que a advocacia não enfrenta uma era de substituição do homem pela máquina, mas sim uma era de responsabilidade amplificada, na qual a inovação deve, obrigatoriamente, caminhar *pari passu* com a excelência ética e a intransigente proteção dos direitos e dados daqueles que lhe são confiados.

REFERÊNCIAS

ALENCAR, Ana Catarina de. **Inteligência Artificial, Ética e Direito**: Guia Prático para Entender o Novo Mundo. Rio de Janeiro: Expressa, 2022. E-book. pág.8. ISBN 9786553620339. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786553620339/ . Acesso em: 01 mar. 2026.

BRASIL**.** Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal.** Diário Oficial da União, Brasília, DF, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 15 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União, Brasília**, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 out. 2025.

BRASIL. Lei nº 8.906, de 4 de julho de 1994. Dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB). **Diário Oficial da União**, Brasília, DF, 5 jul. 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: 15 out. 2025.

BRASIL. Superior Tribunal de Justiça. Agravo Interno no Recurso Especial nº 1.954.379 - SP (2021/0253737-9). Relator: Ministro Marco Aurélio Bellizze. Brasília, DF, 17 nov. 2021. **Diário da Justiça Eletrônico**, 17 nov. 2021. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2099217&num_registro=202102537379&data=20211117&formato=PDF. Acesso em: 15 out. 2025.

BRASIL. Superior Tribunal de Justiça (4. Turma). Recurso em Mandado de Segurança nº 67.105 - SP (2021/0246221-5). Recorrente: Luiz Carlos Bellucco Ferreira. Recorrido: Estado de São Paulo. Relator: Ministro Luis Felipe Salomão. Brasília, DF, 21 set. 2021. **Diário da Justiça Eletrônico**, 27 set. 2021. Disponível em: https://scon.stj.jus.br/jurisprudencia/externo/informativo/?livre=@CNOT='018536'. Acesso em: 27 abr. 2026.

CARVALHO, Maximiliano. **Webinário IA 'do zero' - Janeiro de 2025**. [S. l.: s. n.], 2024. 1 vídeo (43 min). Publicado pelo canal Maximiliano Carvalho. Disponível em: https://www.youtube.com/watch?v=eWmhIuzAipI. Acesso em: 16 de out. 2025.

GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD):** Guia de implantação . São Paulo: Editora Blucher, 2020. E-book. pág.126. ISBN 9786555060164. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555060164/ . Acesso em: 05 mar. 2026.

GONÇALVES, Carlos R. **Sinopses Jurídicas v 06 - tomo II - direito civil - direito das obrigações parte especial - responsabilidade civil**. 17. ed. Rio de Janeiro: Saraiva Jur, 2020. E-book. p.13. ISBN 9788553619764. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553619764/ . Acesso em: 07 mar. 2026.

GOOGLE. **Termos de Serviço Adicionais da API Gemini**. [S. l.], 3 abr. 2025. Disponível em: https://ai.google.dev/gemini-api/terms?hl=pt-br. Acesso em: 15 out. 2025.

HELDER, Darlan. **Conversas de usuários com o ChatGPT apareceram por engano no Google; entenda**. G1, 1 ago. 2025. Tecnologia. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/08/01/conversas-de-usuarios-com-o-chatgpt-apareceram-por-engano-no-google-entenda.ghtml. Acesso em**:** 15 out. 2025.

OPENAI. **Política de Privacidade**. [S. l.], 06 fev. 2026. Disponível em: https://openai.com/pt-BR/policies/row-privacy-policy/. Acesso em: 20 mar. 2026.

ORDEM DOS ADVOGADOS DO BRASIL - SEÇÃO SÃO PAULO (OAB SP); TRYBE; JUSBRASIL; INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO (ITS RIO). **Impacto da IA Generativa no Direito:** panorama sobre adoção e percepções**.** 1º relatório setorial. São Paulo, 2025. Disponível em: https://betrybe.com/inteligencia-artificial/relatorio-impacto-ia-no-

direito?utm_medium=referral&utm_source=jota&utm_campaign=jota-exclusiva Acesso em: 13 mar. 2026.

ORDEM DOS ADVOGADOS DO BRASIL. Conselho Federal. **Recomendação nº 001/2024/COP**. Apresenta diretrizes para orientar o uso de Inteligência Artificial generativa na Prática Jurídica. Relator: Conselheiro Federal Francisco Queiroz Caputo Neto. Brasília, DF, 11 de novembro de 2024. Disponível em: https://s.oab.org.br/arquivos/2024/11/7160d4fe-9449-4aed-80bc-a2d7ac1f5d2f.pdf . Acesso em: 11 mar. 2026.

ORDEM DOS ADVOGADOS DO BRASIL. Conselho Federal. **Resolução nº 02/2015.** Aprova o Código de Ética e Disciplina da Ordem dos Advogados do Brasil – OAB. Diário Oficial da União, Brasília, DF, 19 out. 2015. Seção 1, p. 115. Disponível em: https://www.oab.org.br/publicacoes/AbrirPDF?LivroId=0000004085 . Acesso em: 15 out. 2025.

QUEIROZ, Aíla Marques de; et al. O impacto da inteligência artificial na advocacia brasileira: benefícios e desafios no setor jurídico. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 11, p. 2697-2712, nov. 2024. DOI: 10.51891/rease.v10i11.16691**.** Acesso em: 15 out. 2025.

SOLER, Fernanda G**. Proteção de dados:** reflexões práticas e rápidas sobre a LGPD. Rio de Janeiro: Expressa, 2022. E-book. p.14. ISBN 9786553622500. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786553622500/ . Acesso em: 14 out. 2025.