

Sigilo fiscal e proteção de dados no uso de inteligência artificial generativa pela administração tributária municipal: limites jurídicos e condições de conformidade

Paulo Roberto Moraes Barreto
Auditor Fiscal - Prefeitura de Garanhuns

Resumo

A difusão de ferramentas de inteligência artificial generativa de uso geral, como ChatGPT, Gemini e NotebookLM, alcançou a rotina das administrações tributárias municipais, inclusive no tratamento de dados protegidos por sigilo fiscal, entre eles a DIMP, o PGDAS-D, a NFS-e do padrão nacional, o IPTU e os cadastros de contribuintes. Por meio de abordagem qualitativa, analítico-normativa e documental, fundada na leitura sistemática do art. 198 do Código Tributário Nacional, da Lei Geral de Proteção de Dados Pessoais e dos convênios que regem as bases fiscais compartilhadas, na jurisprudência do Supremo Tribunal Federal sobre o traslado do dever de sigilo e na análise dos termos de uso vigentes dos principais fornecedores, verificados em agosto de 2026, o artigo demonstra que a licitude do uso não depende da ferramenta, mas do destinatário do dado. A informação fiscal circula licitamente apenas dentro da esfera do dever de sigilo, integrada pelos sistemas próprios do ente, pelos operadores contratados com garantias formais e pelo intercâmbio entre Fazendas. A conta pessoal, gratuita ou paga, está fora dessa esfera, porque o fornecedor trata o conteúdo para finalidades próprias, com treinamento de modelos, revisão humana e retenção que pode sobreviver à exclusão e ceder a ordens judiciais estrangeiras. E a assinatura corporativa só altera esse quadro quando acompanhada de contratação formal firmada pelo ente; sem ela, o vício permanece. Conclui-se que o uso com dado protegido em contas pessoais é ilícito e que a mera assinatura corporativa não o legitima; que a via legítima é a contratação formal com adendo de tratamento de dados e cláusulas-padrão da ANPD; que o uso sem dado protegido é livre e desejável; e propõe-se uma rota de governança em três fases para as administrações tributárias municipais.

Palavras-chave: Sigilo fiscal; Proteção de dados pessoais; Inteligência artificial generativa; Administração tributária municipal; NFS-e; DIMP; Transferência internacional de dados; Governança de dados.

Tax Secrecy and Data Protection in the Use of Generative Artificial Intelligence by Municipal Tax Administrations: Legal Limits and Compliance Conditions

Abstract

General-purpose generative artificial intelligence tools such as ChatGPT, Gemini, and NotebookLM have reached the daily routine of municipal tax administrations, including the processing of data protected by tax secrecy, such as DIMP payment reports, PGDAS-D returns, the national-standard NFS-e, property tax records, and taxpayer registries. Through a qualitative, analytical-normative, and documentary approach, grounded in a systematic reading of article 198 of the Brazilian National Tax Code, of the Brazilian Data Protection Law (LGPD), and of the agreements governing shared tax databases, in the case law of the Brazilian Supreme Court on the transfer of the duty of secrecy, and in the analysis of the currently effective terms of service of the main providers, verified in August 2026, this article demonstrates that the lawfulness of use does not depend on the tool, but on the recipient of the data. Tax information may lawfully circulate only within the sphere of the duty of secrecy, formed by the entity's own systems, by contracted processors bound by formal safeguards, and by the exchange between tax authorities. Personal accounts, whether free or paid, fall outside that sphere, because the provider processes the content for its own purposes, with model training, human review, and retention that may survive deletion and yield to foreign court orders. A corporate subscription changes this picture only when accompanied by formal contracting executed by the public entity; without it, the defect remains. The article concludes that using protected data in personal accounts is unlawful and that a mere corporate subscription does not legitimize it; that the legitimate path is formal contracting with a data processing addendum and the ANPD's standard contractual clauses; that use without protected data is free and desirable; and it proposes a three-phase governance roadmap for municipal tax administrations.

Keywords: Tax secrecy; Personal data protection; Generative artificial intelligence; Municipal tax administration; NFS-e; DIMP; International data transfers; Data governance.

1 Introdução

A inteligência artificial generativa deixou de ser novidade experimental e passou a integrar a rotina de trabalho das administrações tributárias municipais. Auditores fiscais utilizam ChatGPT, Gemini, NotebookLM e ferramentas congêneres para resumir relatórios, cruzar planilhas, redigir minutas e explorar bases de dados. Em paralelo, multiplicam-se cursos e capacitações que estimulam exatamente esse uso, muitas vezes com exercícios sobre dados reais de contribuintes: extratos da Declaração de Informações de Meios de Pagamento (DIMP), declarações do PGDAS-D, documentos fiscais do padrão nacional da NFS-e, cadastros imobiliários e lançamentos de IPTU.

Esse quadro suscita uma dúvida jurídica precisa. Considerando que tais sistemas retêm, ainda que temporariamente, os dados que processam, o seu emprego com informações protegidas por sigilo fiscal e por dados pessoais de contribuintes seria compatível com o art. 198 do Código Tributário Nacional (Brasil 1966) e com a Lei Geral de Proteção de Dados Pessoais (Brasil 2018)?

A tese central deste artigo é que a pergunta usual, formulada em torno da ferramenta, está mal posta. A pergunta juridicamente relevante não é “posso usar inteligência artificial?”, e sim “a quem estou entregando este dado, e esse destinatário está vinculado ao dever de sigilo?”. Usar inteligência artificial não é o mesmo que entregar dados: há modalidades de uso que não envolvem dado protegido algum e são plenamente legítimas, e há modalidades que consistem, na sua essência jurídica, na entrega de informação sigilosa a uma empresa privada estrangeira que a tratará para finalidades próprias. A distinção estrutura todo o desenvolvimento que segue. O exame alcança as contas pessoais, gratuitas e pagas, e também as assinaturas corporativas: como se demonstrará, o rótulo do plano não define o regime jurídico; o que o define é a existência de contratação formal que vincule o fornecedor ao dever de sigilo.

A análise documental dos termos de uso vigentes revela, ademais, que a premissa da retenção meramente temporária é falsa em pontos decisivos. Conversas do Gemini em conta pessoal selecionadas para revisão humana são retidas por até três anos e não são apagadas quando o usuário exclui sua atividade (Google 2026). No Claude em conta de consumidor, autorizado o treinamento, a retenção alcança cinco anos (Anthropic 2026). E o litígio entre o The New York Times e a OpenAI demonstrou que o prazo contratual de trinta dias cede a ordens judiciais estrangeiras, sem aviso ao titular do dado (OpenAI 2025).

O artigo está organizado da seguinte forma. A seção 2 apresenta a metodologia. A seção 3 constrói o critério jurídico central, a esfera do dever de sigilo. A seção 4 examina o regime da LGPD aplicável ao Poder Público. A seção 5 analisa o regime específico das bases fiscais municipais compartilhadas. A seção 6 verifica o que os termos de uso dos fornecedores efetivamente estabelecem. A seção 7 demonstra a convergência das orientações oficiais brasileiras. A seção 8 realiza a subsunção por

cenário de uso. A seção 9 mapeia as responsabilidades. A seção 10 propõe uma rota de governança em três fases, e a seção 11 conclui.

2 Metodologia e abordagem analítica

O presente artigo adota abordagem qualitativa, de natureza analítico-normativa, documental e propositiva. Não se trata de mensuração estatística nem de estudo de caso de um Município específico, mas do exame, a partir do direito posto e de documentos públicos verificáveis, das condições de licitude do emprego de ferramentas de inteligência artificial generativa sobre dados protegidos na administração tributária municipal.

A análise desenvolve-se em três eixos complementares. O primeiro é a leitura sistemática do marco normativo: o art. 198 do Código Tributário Nacional e suas exceções, a Lei Geral de Proteção de Dados Pessoais, em especial o regime do tratamento pelo Poder Público (arts. 23 a 32) e da transferência internacional (arts. 33 a 36), a Lei de Acesso à Informação, o Marco Civil da Internet e os convênios que instituem as bases fiscais compartilhadas com os Municípios, com apoio na jurisprudência do Supremo Tribunal Federal sobre o traslado do dever de sigilo.

O segundo eixo é a análise documental dos termos de uso, políticas de privacidade e contratos de tratamento de dados dos quatro principais fornecedores de ferramentas generativas de uso geral: OpenAI, Google, Anthropic e Microsoft. Foram examinadas exclusivamente fontes primárias, isto é, os documentos publicados pelos próprios fornecedores, nas versões vigentes em 23 de agosto de 2026, com registro da data de cada documento. A opção metodológica é relevante porque esses textos são alterados unilateralmente com frequência, o que, como se verá, constitui em si um dado juridicamente significativo.

O terceiro eixo é propositivo: a partir da análise normativa e documental, o artigo organiza os cenários de uso em uma matriz de licitude e propõe uma rota de governança em fases progressivas, aproveitando a experiência normativa já disponível no Poder Judiciário, no controle externo e interno federal e em administrações tributárias que já disciplinaram a matéria. O resultado esperado é um quadro analítico capaz de orientar gestores tributários, auditores fiscais e formuladores de políticas públicas, evitando tanto a proibição indiscriminada, que desperdiça ganhos reais de produtividade, quanto a liberação ingênua, que expõe servidores e Municípios a responsabilização.

Registre-se uma limitação de escopo: o artigo é documento técnico de apoio à decisão e não substitui a manifestação da Procuradoria de cada Município nem a avaliação do encarregado de proteção de dados designado nos termos do art. 41 da LGPD.

3 O critério jurídico central: a esfera do dever de sigilo

O sigilo fiscal decorre da proteção constitucional à intimidade e à vida privada (CF, art. 5º, X) e convive, desde a Emenda Constitucional nº 115, de 2022, com o direito fundamental autônomo à proteção dos dados pessoais, inclusive nos meios digitais (CF, art. 5º, LXXIX). No campo tributário, a Constituição qualifica as administrações tributárias como atividades essenciais ao funcionamento do Estado e determina que atuem de forma integrada, inclusive com o compartilhamento de cadastros e de informações fiscais, na forma da lei ou convênio (art. 37, XXII). A ressalva final é decisiva: o compartilhamento constitucionalmente autorizado ocorre entre administrações tributárias e mediante instrumento formal.

O núcleo legal está no art. 198 do Código Tributário Nacional, com a redação da Lei Complementar nº 104/2001:

Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.

A norma pede leitura atenta em três pontos. O dever vincula simultaneamente a Fazenda Pública e cada um de seus servidores, que respondem em nome próprio. O objeto protegido é amplo: alcança faturamento declarado, movimentação por meios de pagamento, valores e tomadores de serviços, características e valor venal de imóveis e o próprio cadastro de contribuintes. E a proteção não se limita a pessoas naturais, pois o dado de faturamento de uma sociedade empresária não é dado pessoal para a LGPD, mas é informação sob sigilo fiscal; suprimir os identificadores das pessoas físicas não libera o dado da pessoa jurídica.

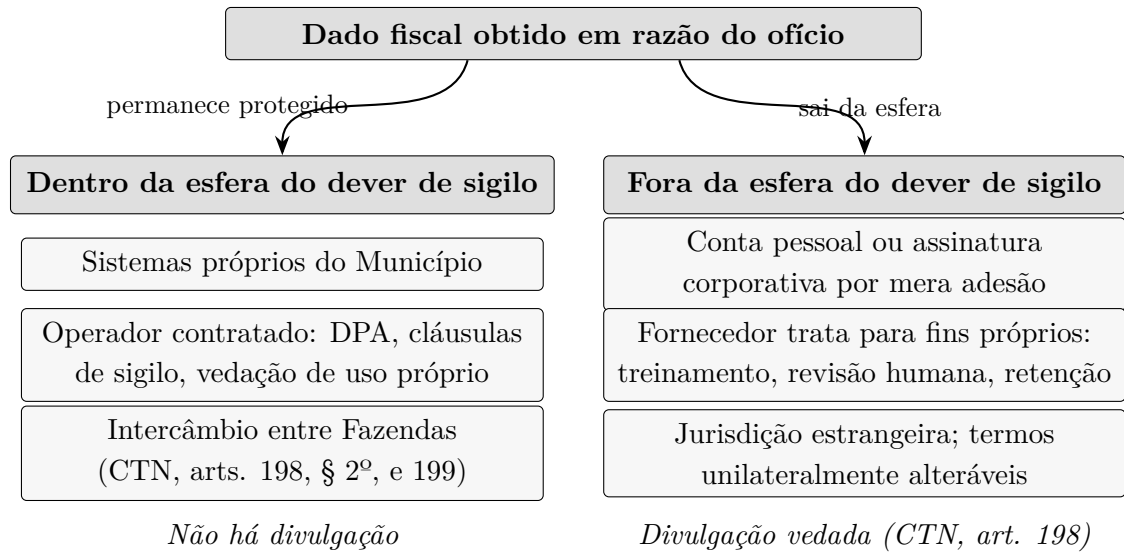
As exceções são taxativas, formais e endereçadas. O § 1º do art. 198 excetua, além das hipóteses do art. 199, a requisição de autoridade judiciária no interesse da justiça e a solicitação de autoridade administrativa mediante processo regularmente instaurado para investigar o próprio sujeito passivo. O § 3º retira do sigilo apenas quatro categorias de informação. E o § 2º disciplina a forma do intercâmbio lícito: processo regularmente instaurado e entrega formalizada por instrumento que assegure a preservação do sigilo. Se a norma exige protocolo documentado até para o compartilhamento entre dois órgãos públicos, é insustentável a tese de que o mesmo dado poderia seguir, sem instrumento algum, para uma empresa privada sediada no exterior.

O Supremo Tribunal Federal consolidou a chave interpretativa dessa disciplina em três momentos. Em 2016, ao julgar as ADIs 2.386, 2.390, 2.397 e 2.859 e o RE 601.314 (Tema 225), assentou que o acesso do Fisco a dados bancários não configura quebra de sigilo, mas traslado do dever de sigilo da esfera bancária para a fiscal (STF 2016). Em 2019, no RE 1.055.941 (Tema 990), autorizou o compartilhamento

com órgãos de persecução penal, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados (STF 2019). Em 2024, na ADI 7.276, validou a sistemática da DIMP justamente porque nela ocorre transferência do sigilo das instituições financeiras à administração tributária, subsistindo o dever legal de preservar a inviolabilidade dos dados compartilhados (STF 2024).

Dessa jurisprudência decorre o critério que organiza este artigo. O dado fiscal chega ao Município acompanhado do dever de sigilo: o ente e seus servidores são depositários de sigilo alheio, não proprietários da informação. A divulgação vedada pelo art. 198 não consiste em fazer o dado transitar por infraestrutura de terceiro, pois, se assim fosse, seriam ilícitos o correio eletrônico institucional em nuvem, o sistema tributário hospedado em datacenter privado e toda a computação contratada pela Administração. A divulgação consiste em fazer o dado sair da esfera do dever de sigilo, o que ocorre quando o destinatário não está juridicamente vinculado a esse dever e passa a tratar a informação para finalidades próprias. A Figura 1 representa o critério.

Figura 1. O critério da esfera do dever de sigilo



Fonte: elaboração do autor com base no CTN, na LGPD e na jurisprudência do STF.

Disso resulta um teste operacional simples, aplicável antes de submeter qualquer informação a uma ferramenta: verificar se o destinatário do dado está obrigado a guardar o sigilo por instrumento que o Município possa exibir e fazer valer. Nos cenários que motivaram este estudo, nenhum instrumento dessa natureza existe.

4 A LGPD e a vedação de transferência a entidades privadas

A LGPD aplica-se integralmente às pessoas jurídicas de direito público (arts. 1º, parágrafo único, e 23). O Município, ao tratar dados de contribuintes, é controlador: a ele competem as decisões referentes ao tratamento (art. 5º, VI). O servidor que decide, por iniciativa própria, submeter uma base a ferramenta externa exerce de fato, e sem competência, uma decisão de controlador. A Autoridade Nacional de Proteção de Dados registrou expressamente, em seu Radar Tecnológico sobre inteligência artificial generativa, que o usuário que compartilha dados pessoais de terceiros com um sistema dessa natureza poderá, a depender do contexto, ser considerado um agente de tratamento (ANPD 2024).

É comum a alegação de que, havendo base legal para o tratamento, como a execução de políticas públicas (art. 7º, III) ou o cumprimento de obrigação legal (art. 7º, II), estaria autorizado o uso de qualquer ferramenta. O raciocínio confunde operações distintas. A LGPD define o uso compartilhado de dados como operação autônoma (art. 5º, XVI) e submete a comunicação de dados pelo Poder Público a disciplina própria. O art. 26, § 1º, é a norma central: é vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, ressalvadas apenas quatro hipóteses, das quais interessa a do inciso IV, a transferência respaldada em contratos, convênios ou instrumentos congêneres, comunicados à autoridade nacional na forma do § 2º. O Guia Orientativo da ANPD sobre o tratamento de dados pelo Poder Público confirma a leitura restritiva do dispositivo (ANPD 2023).

A aplicação ao caso exige uma distinção técnica que decide todo o problema: a posição do fornecedor na relação de tratamento. Operador é quem trata dados em nome do controlador e segundo suas instruções (arts. 5º, VII, e 39). Quando o Município contrata uma solução sob termos comerciais que vedam ao fornecedor qualquer uso próprio do conteúdo, o fornecedor é operador, e a relação se acomoda no art. 26, § 1º, IV. Nos produtos de consumidor ocorre o inverso: o fornecedor define finalidades próprias para o conteúdo recebido, como treinar e aperfeiçoar modelos, desenvolver produtos e alimentar sistemas de segurança, e quem define finalidades é controlador. O uso de conta pessoal não é, portanto, a contratação de um prestador; é a transferência de dados pessoais do Poder Público a uma entidade privada que os tratará para fins próprios, exatamente a operação que o caput do § 1º proíbe e que nenhuma de suas exceções socorre.

A mesma lógica esclarece o papel das contas corporativas. Os planos corporativos oferecem, em regra, o regime técnico adequado, sem treinamento por padrão e com adendo de tratamento de dados disponível; esse regime, porém, não produz efeito jurídico automático em favor da Administração. Se o ente simplesmente adquire assinaturas por adesão eletrônica, com cartão corporativo ou nota de empenho, sem processo de contratação, sem adendo firmado em seu nome, sem cláusulas-padrão da

ANPD e sem a comunicação do art. 26, § 2º, o vício permanece, pois o instrumento exigido pelo inciso IV não se presume do pagamento. A assinatura corporativa é, portanto, condição necessária, mas não suficiente: ela somente reconduz o fornecedor à posição de operador quando inserida na contratação formal descrita no cenário C da seção 8.

Acrescem-se dois obstáculos autônomos. O primeiro é a transferência internacional: todos os fornecedores examinados processam os dados fora do Brasil, o que atrai o art. 33 da LGPD e o Regulamento aprovado pela Resolução CD/ANPD nº 19/2024, que instituiu as cláusulas-padrão contratuais. Não há decisão de adequação que ampare os Estados Unidos, onde estão sediados os quatro fornecedores; o único reconhecimento até agosto de 2026 é o da União Europeia, pela Resolução CD/ANPD nº 32/2026. Sem contrato, não há cláusula-padrão; sem cláusula-padrão nem outra garantia do art. 33, a transferência é ilícita também por esse fundamento. O segundo é o Marco Civil da Internet: o art. 11 da Lei nº 12.965/2014 impõe o respeito à legislação brasileira e ao sigilo mesmo quando o provedor é sediado no exterior, desde que oferte serviço ao público brasileiro. A eleição contratual de foro estrangeiro, presente nos termos de consumidor, não afasta a lei brasileira; apenas torna mais custoso fazê-la valer, o que é razão para evitar o arranjo, não para considerá-lo neutro.

Convém desfazer, neste ponto, um equívoco comum: a LGPD não exige que os dados sejam armazenados ou processados em território brasileiro. Diferentemente de legislações que impõem localização de dados, a lei brasileira admite a transferência internacional, desde que apoiada em um dos mecanismos do art. 33; para fornecedores sediados nos Estados Unidos, na prática, as cláusulas-padrão contratuais da ANPD. A localização no Brasil não é, portanto, requisito legal do cenário contratado, mas é diferencial relevante de mitigação de risco, porque reduz a exposição do dado a ordens de autoridades estrangeiras, como demonstra o litígio examinado na seção 6.1, e nada impede que o Município a exija como critério em seu processo de contratação. Cumpre registrar, contudo, que nos planos corporativos das empresas examinadas essa localização é hoje limitada: o Microsoft 365 Copilot mantém no Brasil apenas os dados em repouso, com inferência no exterior; o Azure OpenAI processa no país somente em implantação regional, com oferta reduzida de modelos; o Vertex AI dispõe da região de São Paulo com compromisso de processamento restrito a um único modelo; e ChatGPT Enterprise, Gemini no Workspace e Claude Enterprise não oferecem residência brasileira de qualquer natureza.

Duas precisões completam o quadro. A primeira: em bases como o PGDAS-D e a DIMP, povoadas por microempreendedores individuais, empresários individuais e autônomos, o dado do negócio é dado de pessoa natural identificada, e portanto dado pessoal para todos os efeitos da LGPD (art. 5º, I). A segunda: a anonimização, quando efetiva, retira o dado do regime da lei (art. 12), mas em bases municipais a reidentificação costuma ser trivial, pois poucos contribuintes compartilham o mesmo porte, atividade e localização; e mesmo a anonimização perfeita quanto a pessoas

naturais não libera a informação da pessoa jurídica, que permanece sob o art. 198 do CTN. Para desenvolvimento de análises e testes de fluxo, o caminho seguro é o dado sintético, não o dado real mascarado.

5 O regime das bases fiscais municipais compartilhadas

As bases mencionadas ao longo deste artigo não estão em igualdade de condições: uma delas conta com vedação convencional expressa, e as demais se submetem ao regime geral. A Tabela 1 sintetiza o quadro.

O acesso do Município ao Ambiente de Dados Nacional da NFS-e decorre do convênio celebrado em 2022 entre a Receita Federal, os Municípios e o Distrito Federal, com a participação de ABRASF, CNM e FNP, fundado no art. 199 do CTN e no art. 37, XXII, da Constituição (Brasil 2022). Sua cláusula nona obriga os Municípios a zelar pelo sigilo e pela confidencialidade dos dados e a utilizá-los somente nas atividades que lhes compete exercer em virtude de lei. O parágrafo único é a norma mais diretamente violada pela prática aqui examinada:

Os acessos realizados às informações da NFS-e de padrão nacional deverão ser restritos àquelas indispensáveis à ação fiscalizadora ou arrecadadora dos municípios convenientes, não podendo ser transferidas a terceiros, seja a título oneroso ou gratuito, ou de qualquer forma divulgadas.

Carregar um arquivo de NFS-e do padrão nacional em uma ferramenta de consumidor é transferi-lo a terceiro a título gratuito. Não há leitura alternativa disponível. E, como a adesão ao ambiente nacional é condição do próprio acesso municipal à base, o descumprimento expõe não apenas o servidor, mas a continuidade do acesso do ente.

A DIMP foi instituída pelo Convênio ICMS nº 134/2016 do CONFAZ, com alterações posteriores, e recebida no plano municipal por normas locais que adotam o mesmo leiaute (CONFAZ 2016). O convênio não traz cláusula de sigilo dirigida ao ente receptor, o que não fragiliza a proteção: o regime aplicável é integralmente o do art. 198 do CTN, na exata leitura da ADI 7.276, que qualificou o fluxo como traslado de sigilo com dever de preservação da inviolabilidade. No Simples Nacional, a LC nº 123/2006 (art. 25-A, incluído pela LC nº 214/2025) e a Resolução CGSN nº 140/2018 (art. 38, § 2º, III) estabelecem o compartilhamento das informações do PGDAS-D entre as administrações tributárias, e apenas entre elas; as informações têm caráter declaratório e constituem confissão de dívida, sendo, por definição, retrato da situação econômica do sujeito passivo. O cadastro imobiliário e o lançamento do IPTU, por fim, reúnem informação sob sigilo fiscal e dados pessoais do proprietário; quando a isenção decorre de doença grave ou de invalidez, o dado revela estado de saúde e passa a ser dado pessoal sensível, atraindo o regime mais

restritivo do art. 11 da LGPD. Registre-se a precisão: a condição de aposentado ou pensionista, isoladamente, não é dado sensível, pois o rol do art. 5º, II, é taxativo; sensível é a informação que permite inferir a saúde do titular.

Tabela 1. Bases fiscais municipais compartilhadas e seu regime de sigilo

Base	Instrumento de acesso	Cláusula própria de sigilo	Consequência prática
NFS-e do padrão nacional	Convênio NFS-e de 2022 (CTN, art. 199; CF, art. 37, XXII)	Sim: cláusula 9ª e parágrafo único	Vedação expressa de transferência a terceiros, onerosa ou gratuita, e de divulgação
DIMP	Convênio ICMS nº 134/2016, recebido por norma local	Não: regime geral do CTN	Traslado de sigilo reconhecido pelo STF na ADI 7.276, com dever de preservação
PGDAS-D (Simples Nacional)	LC nº 123/2006, art. 25-A; Resolução CGSN nº 140/2018, art. 38, § 2º, III	Não: regime geral do CTN	Compartilhamento restrito às administrações tributárias; confissão de dívida
IPTU e cadastro imobiliário	Base própria municipal	Não: regime geral do CTN	Sigilo fiscal e dados pessoais; sensíveis quando revelam saúde do titular

Fonte: elaboração do autor.

6 O que os termos de uso efetivamente estabelecem

A análise que segue baseia-se exclusivamente em documentos oficiais dos fornecedores, nas versões vigentes em 23 de agosto de 2026. A data importa: esses documentos são alterados unilateralmente e com frequência, de modo que o regime jurídico a que o dado ficaria submetido não é estável nem negociável pelo usuário individual. A Tabela 2 sintetiza os resultados.

No ecossistema da OpenAI, o ChatGPT em conta de consumidor (Free, Plus e Pro) usa o conteúdo do usuário para treinamento por padrão, admite exclusão de conversas com remoção definitiva em até trinta dias, não oferece contrato de tratamento de dados nem residência de dados, e elege foro na Califórnia (OpenAI 2026). Os planos corporativos (Business, antigo Team, Enterprise e Edu) não treinam com dados do cliente por padrão e contam com contrato de tratamento; a revisão humana subsiste em hipóteses delimitadas, e no plano Business pode ser feita inclusive por

terceiros contratados. A API não treina com os dados e admite regime de retenção zero para casos elegíveis. Nenhuma modalidade processa em território brasileiro.

No ecossistema do Google, o Gemini em conta pessoal é o caso mais grave do levantamento: com a atividade ativa, o conteúdo é usado para treinar modelos; um subconjunto das conversas é lido por revisores humanos, inclusive prestadores de serviço; a retenção padrão é de dezoito meses; e as conversas revisadas por humanos são mantidas por até três anos, mesmo que o usuário exclua a atividade. A própria página de suporte adverte, em texto expresso, que o usuário não insira informação confidencial que não queira ver revisada ou usada pelo Google (Google 2026). A assinatura paga não altera esse regime. O NotebookLM em conta de consumidor não usa o conteúdo para treinamento, salvo envio de feedback, hipótese em que há revisão humana e retenção de até três anos. Já as versões no Google Workspace, incluindo o NotebookLM corporativo, não treinam nem submetem o conteúdo a revisão humana e contam com contrato de tratamento; as regiões de dados disponíveis, porém, limitam-se a Estados Unidos e União Europeia.

No ecossistema da Anthropic, o Claude em conta de consumidor passou, desde agosto de 2025, a regime de treinamento por padrão, com possibilidade de recusa; quem autoriza o treinamento tem os dados retidos, de forma desidentificada, por até cinco anos, e quem recusa permanece na retenção de trinta dias (Anthropic 2026). Nos planos corporativos e na API há vedação contratual expressa de treinamento e contrato de tratamento de dados; a política de privacidade da Anthropic é a única, entre os quatro fornecedores, que menciona expressamente o Brasil, declarando apoiar-se em cláusulas-padrão aprovadas pela ANPD para as transferências.

No ecossistema da Microsoft, o Copilot de consumidor apresenta uma particularidade favorável: usuários no Brasil estão expressamente excluídos do treinamento de modelos generativos. Ainda assim, a retenção é de dezoito meses e há revisão humana obrigatória, sem possibilidade de recusa, na apuração de suspeita de violação do código de conduta (Microsoft 2026). O Microsoft 365 Copilot, corporativo, não treina com dados do cliente, não submete conteúdo a revisão humana e opera sob o contrato de tratamento da Microsoft; o Brasil, contudo, é região local apenas para armazenamento, e a inferência ocorre no exterior. O Azure OpenAI é a arquitetura mais próxima das necessidades de uma administração tributária: dados sob controle do cliente, possibilidade de suprimir o monitoramento com revisão humana para dados altamente sensíveis e região Brasil Sul disponível, desde que a implantação seja regional, e não global.

6.1 A premissa da retenção temporária não se sustenta

A dúvida que motivou este estudo partiu da hipótese de que os sistemas retêm os dados apenas temporariamente. A análise documental mostra que essa hipótese é generosa com os fornecedores.

O caso mais eloquente é judicial. Em 13 de maio de 2025, no litígio movido

Tabela 2. Síntese comparativa dos regimes de dados, por produto (agosto de 2026)

Produto	Treina por padrão	Retenção	Revisão humana	DPA	Processa no Brasil
ChatGPT consumidor (Free, Plus, Pro)	Sim	30 dias após exclusão; indefinida enquanto ativa	Não declarada em cláusula específica	Não	Não
ChatGPT Business e Enterprise	Não	Definida pelo administrador	Sim, restrita; inclui terceiros	Sim	Não
OpenAI API	Não	Até 30 dias; retenção zero possível	Se sinalizado	Sim	Não
Gemini pessoal (gratuito e pago)	Sim	18 meses; até 3 anos após exclusão, se revisada	Sim	Não	Não
Gemini e NotebookLM no Workspace	Não	Definida pelo administrador	Não	Sim	Não (EUA ou UE)
NotebookLM consumidor	Só com feedback	Até 3 anos, com feedback	Com feedback	Não	Não
Claude consumidor	Sim	30 dias sem treinamento; até 5 anos com	Se sinalizado	Não	Não
Claude corporativo e API	Não (vedação contratual)	30 dias	Se sinalizado	Sim	Não
Copilot consumidor	Sim; Brasil excluído	18 meses	Sim; sem recusa na apuração de abuso	Não	Não
Microsoft 365 Copilot	Não	Definida pelo administrador	Não	Sim	Parcial: repouso sim, inferência não
Azure OpenAI	Não	Controlada pelo cliente	Eliminável mediante aprovação	Sim	Sim, em implantação regional

Fonte: elaboração do autor, a partir dos documentos oficiais dos fornecedores listados nas referências.

pelo The New York Times contra a OpenAI perante o Distrito Sul de Nova York, determinou-se que a empresa preservasse e segregasse todos os registros de saída que de outro modo seriam excluídos. A obrigação vigorou até 26 de setembro de 2025. Nesse período, a política de exclusão em trinta dias simplesmente não valeu para as contas de consumidor, para o plano Team e para a API sem retenção zero. Em 7 de novembro de 2025, determinou-se ainda a produção de vinte milhões de conversas de contas de consumidor, em amostra do período de dezembro de 2022 a novembro de 2024, desidentificadas e sob ordem de proteção; a OpenAI produziu o material em dezembro de 2025, sob objeção, e a decisão foi confirmada pelo juízo em 5 de janeiro de 2026 (OpenAI 2025). O prazo de retenção anunciado em termos de uso, portanto, não é garantia oponível a terceiros. É política interna, derogável por ordem judicial de outra jurisdição, sem aviso ao titular e sem que o Município disponha de meio algum de resistência.

Tampouco a exclusão pelo usuário encerra o ciclo de vida do dado. No Gemini em conta pessoal, as conversas selecionadas para revisão humana são mantidas por até três anos e não são apagadas quando o usuário exclui sua atividade: a exclusão remove o histórico visível, não a cópia retida. A leitura por pessoas, por sua vez, nem sempre pode ser recusada. O Copilot de consumidor declara indisponível a recusa da revisão humana na apuração de abuso; o ChatGPT Business admite revisão por terceiros contratados; o Gemini pessoal, por prestadores de serviço. Sigilo fiscal e revisão de conteúdo por terceiros são conceitos incompatíveis.

Por fim, não há processamento em território brasileiro nos produtos de consumidor, e há menos do que o marketing sugere nos corporativos, pois residência de armazenamento não se confunde com residência de inferência. Somam-se, como elementos de risco, incidentes documentados pelos próprios fornecedores, como a falha que em março de 2023 expôs títulos de conversas e dados parciais de cobrança de assinantes do ChatGPT e o incidente de novembro de 2025 em fornecedor de análise de dados da OpenAI.

7 A convergência das orientações oficiais brasileiras

Não há, em agosto de 2026, lei geral de inteligência artificial em vigor no Brasil: o PL nº 2.338/2023 foi aprovado pelo Senado em dezembro de 2024 e aguarda parecer em comissão especial da Câmara dos Deputados. A ausência de marco específico não cria vazio normativo; cria o contrário, pois na falta de norma especial aplicam-se integralmente as normas gerais, o CTN, a LGPD, a Lei de Acesso à Informação, o Código Penal e as cláusulas dos convênios. E as orientações oficiais já editadas convergem, sem exceção relevante, no ponto que interessa a este artigo.

O Guia de IA Generativa da Secretaria de Governo Digital, elaborado no âmbito do Plano Brasileiro de Inteligência Artificial, orienta expressamente: não inserir in-

formações internas da instituição em aplicativos que não sejam solução aprovada; não inserir dados pessoais de servidores, cidadãos ou terceiros; não usar credenciais institucionais para criar contas em plataformas externas; e conclui que a ferramenta externa que salva, reutiliza ou compartilha os dados recebidos para treinar seu modelo não deve ser usada para tratar dados protegidos, sob pena de responsabilização legal e disciplinar dos agentes envolvidos (Brasil 2025a). O Tribunal de Contas da União, em guia aprovado pela Portaria-CGTI nº 1/2024, define ChatGPT e Gemini nominalmente como plataformas externas não aprovadas, determina que apenas dados públicos da instituição sejam a elas enviados e sujeita o descumprimento a medidas disciplinares (Brasil 2024). A Controladoria-Geral da União adota orientação equivalente em seu guia de uso responsável (Brasil 2025b).

O precedente normativo mais detalhado é a Resolução CNJ nº 615/2025, que disciplina a inteligência artificial no Poder Judiciário. Ela torna a anonimização obrigatória para dados sigilosos (art. 7º, § 2º), veda o uso de modelos de linguagem privados para processar documentos ou dados sigilosos, salvo anonimização na origem ou mecanismos técnicos equivalentes (art. 19, § 3º, IV), e exige que o fornecedor não trate os dados dos usuários para treinamento ou quaisquer fins não autorizados (art. 19, § 3º, III). É digno de nota que a mesma resolução faculta a assinatura individual de soluções privadas quando o tribunal não oferecer solução corporativa (art. 19, § 2º): o CNJ não proíbe a conta pessoal, proíbe o seu uso com dado sigiloso. A distinção reforça, em vez de enfraquecer, o critério defendido neste artigo, pois na administração tributária incidem cumulativamente o art. 198 do CTN e o art. 26, § 1º, da LGPD, que disciplinam o destino do dado, e não apenas a conduta do usuário (CNJ 2025).

Nas administrações tributárias, a Receita Federal editou a Portaria RFB nº 647/2026, política institucional de inteligência artificial estruturada em supervisão humana, rastreabilidade e responsabilidade (Brasil 2026). E o precedente diretamente municipal é a Portaria SF nº 22/2026, da Secretaria Municipal da Fazenda de São Paulo, cujo art. 4º restringe dados pessoais e fiscais a sistemas sob controle da Secretaria ou formalmente contratados, proibindo o armazenamento em plataformas externas não autorizadas, e cujo art. 6º veda a decisão administrativa final tomada de forma autônoma por sistema de inteligência artificial (São Paulo 2026). A ANPD, por sua vez, além do Radar Tecnológico, já demonstrou disposição fiscalizatória concreta sobre plataformas de inteligência artificial, com medidas preventivas e multa diária, e mantém a regulamentação do tratamento automatizado em sua agenda regulatória, o que recomenda que os Municípios estruturem sua governança antes da norma, e não depois dela.

8 Seis cenários de uso e seus enquadramentos

O uso de inteligência artificial na rotina de uma Secretaria de Finanças não é uma situação única, e sim um conjunto de situações juridicamente distintas, cuja

licitude varia caso a caso. Seis cenários cobrem a prática e estão sintetizados na Tabela 3.

No cenário A, o servidor emprega conta pessoal, gratuita ou paga, com dado fiscal identificado. É o cenário que motivou este estudo e o mais frequente. A conduta viola o art. 198 do CTN, fora de suas exceções taxativas; viola o art. 26, § 1º, da LGPD, sem amparo em qualquer de suas hipóteses; realiza transferência internacional sem instrumento do art. 33; e, quando o dado provém do padrão nacional da NFS-e, viola diretamente o parágrafo único da cláusula nona do convênio. A conclusão é de ilicitude, insuscetível de regularização por termo de responsabilidade individual, por configuração de privacidade ou por exclusão posterior da conversa.

No cenário B, o Município paga assinaturas sem contratação formal de tratamento, inclusive planos corporativos como ChatGPT Business ou Enterprise e Gemini no Workspace: adquire os planos por adesão, com cartão corporativo ou nota de empenho, sem processo de contratação, sem adendo de tratamento de dados firmado pelo ente, sem cláusulas-padrão e sem comunicação à ANPD. O pagamento, isoladamente, não supre o requisito do art. 26, § 1º, IV, quando o instrumento aceito é termo de adesão firmado por servidor; e a aquisição sem processo regular contraria a Lei nº 14.133/2021, cujo art. 92, § 1º, exige cláusula de foro da sede da Administração, enquanto os termos de consumidor elegem foro estrangeiro. O cenário é irregular e insuficiente para legitimar o tratamento de dado sigiloso; sua correção natural é a migração para o cenário C.

No cenário C, o Município contrata formalmente solução corporativa, com processo regular, adendo de tratamento de dados, cláusulas-padrão da ANPD, vedação contratual de treinamento, retenção controlada, trilhas de auditoria, relatório de impacto e ato normativo interno. A transferência passa a respaldar-se em contrato (art. 26, § 1º, IV), a transferência internacional no art. 33, II, e o fornecedor assume a posição de operador (art. 39). Quanto ao art. 198 do CTN, o instrumento que vincula o fornecedor ao dever de sigilo mantém o dado dentro da esfera de proteção, como a mantém o datacenter contratado e o correio institucional em nuvem. O cenário é admissível sob condições cumulativas, com uma ressalva de direito: para a NFS-e do padrão nacional, a literalidade da cláusula nona alcança até o cenário contratado, e a via adequada para superá-la é a consulta formal à Receita Federal, não a interpretação unilateral do Município. Recomenda-se que a primeira contratação exclua a NFS-e nacional e a DIMP até que sobrevenha essa manifestação.

No cenário D, empregam-se dados anonimizados, sintéticos ou agregados, sem sujeito passivo identificável: não há dado pessoal (art. 12 da LGPD) nem informação sob sigilo fiscal. A ressalva é que a anonimização precisa ser verificada, e não presumida; em bases municipais, mascarar o identificador e manter valor, atividade e localização normalmente não anonimiza. No cenário E, a ferramenta é usada sem qualquer dado protegido, para redação, pesquisa de legislação, construção de fórmulas, roteiros de auditoria e revisão de minutas sem dados reais: o uso é livre, legítimo e deve constar expressamente da norma interna como permitido,

pois a política que apenas proíbe perde produtividade e empurra a prática para a clandestinidade. No cenário F, o processamento ocorre em solução interna ou em infraestrutura sob controle público, incluindo as soluções de empresas públicas de tecnologia: é a arquitetura de menor risco e a preferencial; para municípios de pequeno e médio porte, o consórcio público e a adesão a soluções compartilhadas são o caminho realista.

Tabela 3. Matriz de licitude por cenário de uso

Cenário	Fundamento normativo	Conclusão
A. Conta pessoal, gratuita ou paga, com dado fiscal identificado	CTN, art. 198; LGPD, arts. 6º, 26, § 1º, e 33; Convênio NFS-e, cláusula 9ª, parágrafo único	Vedado
B. Assinatura, inclusive corporativa, sem contratação formal de tratamento	LGPD, art. 26, § 1º, IV, e § 2º; Lei nº 14.133/2021, art. 92, § 1º	Irregular; migrar para o cenário C
C. Solução corporativa contratada, com DPA e cláusulas-padrão da ANPD	LGPD, arts. 26, § 1º, IV, 33, II, 39 e 46; CTN, art. 198, § 2º	Admissível sob condições; NFS-e nacional depende de consulta à RFB
D. Dados anonimizados, sintéticos ou agregados	LGPD, art. 12	Admissível; anonimização verificada, preferindo-se o dado sintético
E. Uso sem qualquer dado protegido	Fora do âmbito do art. 198 do CTN e da LGPD	Livre e recomendável
F. Solução interna ou em infraestrutura sob controle público	CTN, art. 198, § 2º; LGPD, arts. 46 e 49	Arquitetura preferencial

Fonte: elaboração do autor.

9 Responsabilidades do servidor e do Município

A exposição pessoal do servidor é maior do que a percepção corrente sugere. No plano penal, o art. 325 do Código Penal tipifica a violação de sigilo funcional, com pena de detenção de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave, e o § 1º, II, pune quem se utiliza, indevidamente, do acesso restrito; o art. 153, § 1º-A, tipifica a divulgação, sem justa causa, de informações sigilosas, contidas ou não nos sistemas da Administração, com detenção de um a quatro anos e multa. O enquadramento concreto depende do elemento subjetivo e da demonstração de desvio de finalidade do acesso, e entre os tipos há relação de

especialidade que tende a afastar o concurso; a discussão, porém, só se trava depois de instaurado o procedimento, e a tese de que não houve intenção de revelar convive mal com a advertência que o próprio fornecedor exibe na tela.

No plano disciplinar, os estatutos de servidores preveem o dever de guarda de sigilo e classificam a revelação de segredo apropriado em razão do cargo entre as infrações mais graves, e a Lei de Acesso à Informação qualifica como conduta ilícita divulgar ou permitir a divulgação de informação sigilosa ou pessoal (art. 32, IV). Na improbidade administrativa, o art. 11, III, da Lei nº 8.429/1992, com a redação da Lei nº 14.230/2021, alcança a revelação de fato que deva permanecer em segredo, exigidos o dolo específico de obter proveito e a lesividade relevante, configuração improvável na hipótese do servidor que buscava eficiência, mas possível na reiteração após advertência formal. No plano civil, o art. 34 da Lei de Acesso à Informação e os arts. 42 e seguintes da LGPD asseguram a reparação ao contribuinte lesado, respondendo o Município diretamente e exercendo o direito de regresso contra o servidor.

O Município, por sua vez, sujeita-se às sanções do art. 52 da LGPD aplicáveis ao Poder Público (§ 3º): advertência, publicização da infração, bloqueio e eliminação dos dados, suspensão do funcionamento do banco de dados, suspensão da atividade de tratamento e proibição parcial ou total do tratamento. Seria um erro medir esse risco pela inaplicabilidade da multa: o bloqueio de uma base fiscal ou a suspensão do seu tratamento paralisa lançamento, cobrança e fiscalização, com efeito operacional muito superior ao pecuniário. Acresce o dever de comunicação de incidente: conhecida a inserção de base protegida em ferramenta não homologada, incide o art. 48 da LGPD, com o prazo de três dias úteis fixado pela Resolução CD/ANPD nº 15/2024 para comunicação à autoridade e aos titulares, e a inércia diante do incidente conhecido constitui descumprimento autônomo.

Uma palavra sobre os cursos e capacitações. O problema não está na técnica ensinada, que é legítima e valiosa, mas no ambiente em que se pratica. O curso que ensina a construir análises fiscais com dados sintéticos, ou sobre solução homologada, é irrepreensível; o curso que instrui o servidor a exportar a base real e colá-la em ferramenta de consumidor está ensinando a praticar o cenário A, e o certificado não funciona como excludente de responsabilidade. Recomenda-se que o custeio e o reconhecimento institucional de capacitações fiquem condicionados à demonstração, no plano de ensino, de que os exercícios usam dados fictícios ou ambiente homologado.

10 Uma rota de governança em três fases

A adaptação das administrações municipais deve ocorrer em fases, porque as providências têm graus distintos de urgência e de complexidade. Nenhuma fase posterior faz sentido sem a anterior minimamente estabelecida.

A primeira fase é de contenção e esclarecimento, executável de imediato e sem custo relevante. Compreende a comunicação interna a todos os servidores com acesso

a bases fiscais, dizendo com igual clareza o que é vedado e o que permanece permitido; o levantamento, sem caráter punitivo inicial, da extensão do uso já ocorrido, insumo indispensável à avaliação de incidente do art. 48 da LGPD; a vedação do uso de e-mail e credenciais institucionais para criar contas em plataformas externas; e o condicionamento das capacitações a exercícios com dados fictícios ou ambiente homologado.

A segunda fase é de normatização e alternativa. Compreende a edição de ato normativo local disciplinando o uso de inteligência artificial, para o qual a Portaria SF nº 22/2026 de São Paulo e a Resolução CNJ nº 615/2025 oferecem modelos maduros; o envolvimento formal do encarregado de proteção de dados e da Procuradoria; a elaboração do relatório de impacto à proteção de dados antes da contratação; e, sobretudo, a disponibilização de uma alternativa homologada, ainda que de escopo inicial modesto, porque proibição sem alternativa não elimina o uso, apenas o torna invisível e inaudível.

A terceira fase é estrutural. Compreende a avaliação das três arquiteturas viáveis, em ordem crescente de proteção: solução corporativa contratada de fornecedor global, com adendo de tratamento e cláusulas-padrão da ANPD; solução em nuvem com processamento em região brasileira, observadas as limitações de modelo e de tipo de implantação; e solução em infraestrutura sob controle público. Para municípios de pequeno e médio porte, a contratação compartilhada por consórcio público ou a adesão a solução de ente maior é o caminho realista, e tema de vocação natural para a articulação federativa no âmbito da Confederação Nacional de Municípios. Completam a fase a capacitação institucional obrigatória sobre sigilo fiscal e proteção de dados aplicados a ferramentas digitais, com registro de participação, e a revisão periódica do ato normativo, imposta pela mutabilidade dos termos dos fornecedores e pela agenda regulatória da ANPD.

11 Conclusão

A principal lição deste estudo é que a ilicitude não está na tecnologia, mas no destinatário do dado. O dado fiscal chega ao Município acompanhado do dever de sigilo, e o servidor é depositário, não proprietário, da informação. Inserir dados de DIMP, PGDAS-D, NFS-e do padrão nacional, IPTU ou cadastros de contribuintes em contas pessoais de ferramentas generativas, gratuitas ou pagas, é conduta vedada pelo art. 198 do CTN e pelo art. 26, § 1º, da LGPD, e, no caso da NFS-e nacional, por cláusula convencional expressa. A análise documental demonstrou que a suposta retenção temporária é, em pontos decisivos, retenção de anos, sujeita a revisão humana e derogável por ordem judicial estrangeira; e que nem a distinção entre conta gratuita e conta paga, nem o rótulo corporativo do plano, alteram o regime jurídico: o que o altera é a contratação formal que vincula o fornecedor, na posição de operador, ao dever de sigilo.

O planejamento das administrações tributárias municipais deve evitar dois equí-

vocos simétricos. O primeiro é a liberação ingênua: tratar a ferramenta como um utilitário neutro e permitir que a base fiscal do Município se disperse por contas pessoais, jurisdições estrangeiras e bases de treinamento de terceiros. O segundo é a proibição cega: vetar toda e qualquer utilização, desperdiçando ganhos legítimos de produtividade nos usos sem dado protegido e empurrando a prática real para a clandestinidade, onde nenhum controle alcança. Entre os dois equívocos há um caminho definido: permitir com clareza o que não envolve dado protegido, contratar formalmente o que envolve, e construir progressivamente a governança que sustenta essa distinção.

O ponto de partida do planejamento, portanto, não é a escolha da ferramenta, que é decisão de mercado e muda com ele. É um inventário jurídico: levantar quais instrumentos o Município possui, hoje, capazes de vincular ao dever de sigilo cada destinatário de seus dados fiscais. Enquanto esse inventário estiver vazio, a única posição compatível com o art. 198 do CTN é não entregar o dado. Feito com honestidade sobre a situação de cada ente, ele define o resto: o que liberar desde logo, o que contratar e o que construir.

Conflito de interesses

O autor declara não haver conflito de interesses relacionado à elaboração, ao conteúdo ou à submissão deste manuscrito.

Declaração de dados da pesquisa

Os dados de pesquisa utilizados neste artigo estão contidos no próprio manuscrito. O trabalho possui natureza qualitativa, analítico-normativa, documental e propositiva, não tendo utilizado base de dados empírica própria, entrevistas ou experimentos. As fontes que fundamentam a análise correspondem a normas jurídicas, decisões judiciais, documentos públicos e documentos oficiais de fornecedores, indicados ao longo do texto e na seção de referências, com as datas de verificação. Desse modo, os dados necessários à compreensão, verificação e reprodução argumentativa do estudo encontram-se descritos e citados no próprio manuscrito.

Referências

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo: tratamento de dados pessoais pelo Poder Público**. 2. ed. Brasília: ANPD, 2023. Disponível em: <https://www.gov.br/anpd>. Acesso em: 23 ago. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Radar Tecnológico nº 3: Inteligência Artificial Generativa**. Brasília: ANPD, 2024. Disponível em: <https://www.gov.br/anpd>. Acesso em: 23 ago. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 15, de 24 de abril de 2024.** Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União, 2024.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 19, de 23 de agosto de 2024.** Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Diário Oficial da União, 2024.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 32, de 26 de janeiro de 2026.** Reconhece a União Europeia como provedora de grau de proteção adequado para fins de transferência internacional de dados. Diário Oficial da União, 2026.

ANTHROPIC. **Privacy Policy; Commercial Terms of Service; Updates to Consumer Terms and Privacy Policy.** San Francisco: Anthropic, 2025-2026. Disponível em: <https://www.anthropic.com/legal>. Acesso em: 23 ago. 2026.

BRASIL. **Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional).** Diário Oficial da União, 1966. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/15172compilado.htm. Acesso em: 23 ago. 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Diário Oficial da União, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 ago. 2026.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001.** Dispõe sobre o sigilo das operações de instituições financeiras. Diário Oficial da União, 2001.

BRASIL. **Lei Complementar nº 123, de 14 de dezembro de 2006.** Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte. Diário Oficial da União, 2006.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).** Diário Oficial da União, 2011.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Diário Oficial da União, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).** Diário Oficial da União, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 23 ago. 2026.

BRASIL. **Lei nº 14.133, de 1º de abril de 2021.** Lei de Licitações e Contratos Administrativos. Diário Oficial da União, 2021.

BRASIL. **Convênio para a instituição do padrão nacional da Nota Fiscal de Serviço eletrônica (NFS-e).** Brasília: Receita Federal do Brasil; Municípios;

Distrito Federal, 2022. Disponível em: <https://www.gov.br/nfse>. Acesso em: 23 ago. 2026.

BRASIL. Tribunal de Contas da União. **Guia de uso de Inteligência Artificial Generativa no TCU**. Portaria-CGTI nº 1, de 11 de julho de 2024. Brasília: TCU, 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Guia IA Generativa**. Brasília: MGI, 2025a. Disponível em: <https://www.gov.br/governodigital>. Acesso em: 23 ago. 2026.

BRASIL. Controladoria-Geral da União. **Guia de Uso Responsável de Inteligência Artificial (Generativa)**. Brasília: CGU, 2025b.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Portaria RFB nº 647, de 5 de fevereiro de 2026**. Dispõe sobre a política de Inteligência Artificial no âmbito da RFB. Diário Oficial da União, 2026.

COMITÊ GESTOR DO SIMPLES NACIONAL. **Resolução CGSN nº 140, de 22 de maio de 2018**. Diário Oficial da União, 2018.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 615, de 11 de março de 2025**. Institui diretrizes para desenvolvimento, utilização e governança de soluções com inteligência artificial no Poder Judiciário. Brasília: CNJ, 2025.

CONSELHO NACIONAL DE POLÍTICA FAZENDÁRIA (CONFAZ). **Convênio ICMS nº 134, de 9 de dezembro de 2016**. Dispõe sobre o fornecimento de informações sobre transações com cartões e demais instrumentos de pagamento eletrônico. Diário Oficial da União, 2016.

GOOGLE. **Gemini Apps Privacy Notice and Activity; NotebookLM Help; Generative AI in Google Workspace Privacy Hub**. Mountain View: Google, 2026. Disponível em: <https://support.google.com/gemini>. Acesso em: 23 ago. 2026.

MICROSOFT. **Privacy FAQ for Microsoft Copilot; Microsoft 365 Copilot Privacy; Azure OpenAI Data, Privacy, and Security**. Redmond: Microsoft, 2026. Disponível em: <https://learn.microsoft.com>. Acesso em: 23 ago. 2026.

OPENAI. **Response to NYT Data Demands; Fighting the NYT User Privacy Invasion**. San Francisco: OpenAI, 2025. Disponível em: <https://openai.com/index/response-to-nyt-data-demands/>. Acesso em: 23 ago. 2026.

OPENAI. **Privacy Policy; Terms of Use; Enterprise Privacy; How Your Data Is Used to Improve Model Performance**. San Francisco: OpenAI, 2026. Disponível em: <https://openai.com/policies>. Acesso em: 23 ago. 2026.

SÃO PAULO (Município). Secretaria Municipal da Fazenda. **Portaria SF nº 22, de 6 de fevereiro de 2026**. Dispõe sobre diretrizes para o uso de sistemas de Inteligência Artificial no âmbito da Secretaria Municipal da Fazenda. Diário Oficial da Cidade, 2026.

SUPREMO TRIBUNAL FEDERAL (STF). **ADIs 2.386, 2.390, 2.397 e 2.859; RE 601.314 (Tema 225)**. Relator: Min. Dias Toffoli. Julgamento em 24 de fevereiro de 2016. Brasília: STF, 2016.

SUPREMO TRIBUNAL FEDERAL (STF). **RE 1.055.941 (Tema 990)**. Relator: Min. Dias Toffoli. Julgamento em 4 de dezembro de 2019. Brasília: STF, 2019.

SUPREMO TRIBUNAL FEDERAL (STF). **ADI 7.276**. Relatora: Min. Cármen Lúcia. Julgamento em 6 de setembro de 2024. Brasília: STF, 2024.