REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

LGPD E LAI NA ERA DA INTELIGÊNCIA ARTIFICIAL: DA COMPATIBILIZAÇÃO ABSTRATA AOS PARÂMETROS DE GOVERNANÇA DE SISTEMAS PÚBLICOS

LGPD AND LAI IN THE AGE OF ARTIFICIAL INTELLIGENCE: FROM ABSTRACT HARMONIZATION TO GOVERNANCE PARAMETERS FOR PUBLIC SYSTEMS

Ciências Sociais Aplicadas • 12/11/2026

REGISTRO DOI: 10.70773/revistatopicos/794524753

Jadir Rafael Bolanha de Aguiar[1]

Luiz Antonio Mendonça Alves da Costa[2]

Marcelle Alencar Urquiza[3]

RESUMO

O uso de inteligência artificial no acesso à informação desafia a compatibilização, pensada para a análise humana, entre a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD). A pesquisa justifica-se pela expansão de assistentes virtuais no setor público enquanto o marco legal da IA permanece em tramitação. O objetivo é propor parâmetros de governança com base nas normas vigentes. De abordagem qualitativa, bibliográfico-documental e método dedutivo, o trabalho examina quatro cenários hipotéticos de risco baseados em casos documentados. Os resultados indicam que a automação pode revelar dados pessoais por reidentificação, favorecer o reuso indevido de dados abertos, gerar negativas sem motivação individualizada e produzir informações falsas. Conclui-se que a compatibilidade entre LAI e LGPD persiste e que a gestão pública pode adotar oito parâmetros auditáveis para assegurar transparência e proteção de dados sem depender de nova lei.

Palavras-chave: Acesso à informação; Proteção de dados pessoais; Inteligência artificial; Decisões automatizadas; Administração pública.

ABSTRACT

The use of artificial intelligence in access to information challenges the harmonization, designed for human analysis, between the Access to Information Law (LAI) and the General Personal Data Protection Law (LGPD). The study is justified by the expansion of virtual assistants in the public sector while Brazil's AI legal framework remains under debate. The objective is to propose governance parameters based on current law. Adopting a qualitative, bibliographic and documentary approach and a deductive method, the paper examines four hypothetical risk

scenarios based on documented cases. Results indicate that automation can reveal personal data through re-identification, enable improper reuse of open data, generate refusals without individualized reasoning, and produce false information. It concludes that the compatibility between LAI and LGPD persists and that public administration can adopt eight auditable parameters to ensure transparency and data protection without new legislation.
Keywords: Access to information; Personal data protection; Artificial intelligence; Automated decisions; Public administration.

1. INTRODUÇÃO

A presente pesquisa delimita-se à relação entre a Lei de Acesso à Informação (LAI, Lei nº 12.527/2011) e a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018) no âmbito do poder público, especificamente quando o atendimento a pedidos de informação passa a ser feito por sistemas de inteligência artificial e assistentes virtuais. A doutrina e a Controladoria-Geral da União (CGU) consolidaram o entendimento de que as duas leis são sistematicamente compatíveis e devem ser aplicadas em conjunto (Brasil, 2022b; Limberger, 2022). Esse entendimento segue a linha do Supremo Tribunal Federal (STF), que, antes mesmo da LGPD, reconheceu que nome, cargo e remuneração de servidores são informação pública (Brasil, 2015). O consenso, contudo, foi construído sob o pressuposto de que uma pessoa analisa o pedido e assina a resposta. A triagem e a decisão automatizadas enfraquecem esse pressuposto e geram tensões normativas em que as garantias de transparência e de privacidade correm o risco de se esvaziar diante do processamento de dados em escala.

A relevância da pesquisa está na crescente adoção de assistentes virtuais e sistemas de automação na prestação de serviços públicos, enquanto o marco legal da inteligência artificial (PL nº 2.338/2023) permanece em tramitação no Congresso Nacional (Zanatta; Rielli, 2024). O tema ganha urgência porque sistemas automatizados tendem a reproduzir os padrões dos dados que os alimentam, inclusive os erros já documentados nas negativas de acesso, como se verá na seção 4.3. Embora a literatura examine amplamente a aplicação conjunta da LAI e da LGPD (Limberger, 2022; Fujita; Oliveira, 2023; Crivelatti; Silva, 2025), os estudos brasileiros sobre decisão automatizada concentraram-se em outros objetos: no direito à explicação e à revisão das decisões automatizadas previsto no art. 20 da LGPD (Monteiro, 2018) e nos fundamentos e riscos do uso de big data e de inteligência artificial na administração pública de modo geral (Araújo; Zullo; Torres, 2020). Nenhum deles trata especificamente do atendimento a pedidos de acesso à informação, fluxo em que quem pede normalmente não é titular dos dados e a resposta é, ela própria, o objeto do direito. Por isso, mostra-se oportuna a proposição de salvaguardas viáveis a partir do ordenamento jurídico vigente.

Diante desse cenário, o objetivo geral deste trabalho é propor parâmetros práticos de governança para o uso de inteligência artificial no atendimento a pedidos de acesso à informação, fundamentados nas normas já em vigor. Como objetivos específicos, busca-se: a) identificar as condições em que se formou o entendimento atual sobre a compatibilização entre LAI e LGPD; b) examinar cenários de risco em que a automação enfraquece essas condições; c) apontar tensões normativas e lacunas operacionais ainda pouco discutidas; e d) transformar essas conclusões em parâmetros verificáveis pelos órgãos de controle.

Para alcançar esses objetivos, a pesquisa adota abordagem qualitativa, de caráter bibliográfico e documental, com método dedutivo aplicado por análise de cenários, conforme detalhado na seção 2.

Pretende-se demonstrar que a administração pública não precisa aguardar uma nova lei de inteligência artificial para estruturar um atendimento automatizado transparente e seguro. Para isso, o artigo explica o método (seção 2), apresenta o entendimento atual sobre as duas leis (seção 3), examina quatro cenários de risco (seção 4) e as tensões normativas que deles decorrem (seção 5), discute o marco legal (seção 6) e propõe oito parâmetros de governança (seção 7).

2. METODOLOGIA

A pesquisa é de natureza qualitativa, de caráter bibliográfico e documental, e adota o método dedutivo, operacionalizado por análise de cenários. Parte-se de premissas extraídas das normas em vigor — a Constituição, a LAI, a LGPD e os entendimentos consolidados pela Controladoria-Geral da União (CGU) e pela Autoridade Nacional de Proteção de Dados (ANPD), atual Agência Nacional de Proteção de Dados, redesignada pela Lei nº 15.352/2026 (Brasil, 2026b) — e se testa a suficiência dessas premissas diante de situações hipotéticas de atendimento automatizado de pedidos de acesso à informação. A conclusão decorre logicamente das premissas: se a compatibilidade entre LAI e LGPD depende de condições que a automação não garante, a governança deve recriá-las sem esperar nova legislação.

O levantamento de fontes cobriu quatro tipos de material. As fontes normativas foram pesquisadas no texto compilado do site do

Planalto. As fontes jurisprudenciais, no portal do STF, a partir do andamento processual e do inteiro teor do acórdão do Tema 483 da repercussão geral. Os atos e orientações da CGU e da ANPD foram localizados no Diário Oficial da União e nos sítios oficiais dos órgãos. A literatura jurídica especializada foi buscada no Google Acadêmico com os termos de busca que combinavam “acesso à informação” a “LGPD”, “art. 31”, “decisão automatizada”, “direito à explicação”, “reidentificação” e “retrieval-augmented generation”. Os relatórios da sociedade civil (Transparência Brasil e Fiquem Sabendo) foram localizados nos sítios das próprias organizações. O levantamento foi realizado até setembro de 2026.

Os casos documentados que fundamentam os cenários foram selecionados por três critérios: 1 - existência de levantamento sistêmico, e não de caso isolado, sobre negativas indevidas, o que levou aos relatórios da Transparência Brasil (2022) e da Fiquem Sabendo (2021); 2 - recorrência documentada de respostas falsas prestadas por assistente virtual público oficial, registrada nas reportagens do The Markup (2024a; 2024b) sobre o assistente da cidade de Nova York; e 3 - existência de decisão judicial sobre responsabilidade civil por resposta de chatbot, no caso Moffatt v. Air Canada (Canadá, 2024).

Os quatro cenários de risco que serão apresentados são hipotéticos e foram construídos por composição. Cada um empresta de um caso documentado o elemento fáctico relevante (negativa indevida em escala, o pedido de registros de visitantes de órgão oficial, a orientação ilegal dada por assistente público e a resposta falsa atribuída a instituição oficial) e acrescenta elementos construídos para dar contorno jurídico à situação, como o vínculo prévio entre as partes, a sequência de perguntas, o tipo de dado sensível atribuído

por erro e o desenho do sistema. Nenhuma das situações retrata pessoa ou órgão determinado.

O método dedutivo mostra-se adequado ao problema porque a questão não é de fato, mas de suficiência normativa: discute-se se as normas vigentes bastam para uma situação nova. A análise de cenários funciona como teste das premissas, assim cada cenário isola uma condição de funcionamento do atendimento humano (análise individualizada, finalidade controlada, motivação e exatidão) e verifica se as normas a preservam quando a decisão passa a ser automatizada. Dos resultados do teste decorrem os oito parâmetros de governança da seção 7, cada um ancorado em norma já em vigor.

São limites do método: os cenários não permitem medir a frequência dos riscos, apenas demonstrar sua plausibilidade normativa; a análise restringe-se ao direito brasileiro, com comparação pontual com o direito da União Europeia; e a tramitação do marco legal da inteligência artificial torna a discussão institucional suscetível de atualização, o que não afeta os parâmetros propostos, todos fundados em leis vigentes.

3. O ENTENDIMENTO ATUAL SOBRE LAI E LGPD

Um dos casos mais conhecidos sobre o choque entre transparência e privacidade envolveu uma servidora do Município de São Paulo que encontrou seu nome e seu salário no site "De Olho nas Contas", da prefeitura, e pediu na Justiça a retirada das informações e indenização por dano moral. Depois de perder em primeira instância, ela obteve em recurso a retirada dos valores, mas não a indenização. O município levou o caso ao Supremo Tribunal Federal (STF), que decidiu em abril de 2015, por unanimidade, ser legítimo

publicar em site oficial os nomes dos servidores e o valor de seus vencimentos e vantagens (Brasil, 2015). Julgada com repercussão geral, a decisão, conhecida como Tema 483, passou a orientar os casos semelhantes em todo o país.

O Tribunal não negou que o salário seja um dado pessoal. Entendeu que, por estar ligado ao cargo, ele também é informação pública, e assim traçou uma linha entre o que pertence à função e o que pertence à vida privada. A LGPD só seria aprovada três anos depois, mas essa linha continua sendo a base do entendimento sobre a relação entre as duas leis.

3.1. Fundamentos Constitucionais e Legais

A Constituição garante, ao mesmo tempo, o acesso a informações dos órgãos públicos (art. 5º, XXXIII), a proteção da intimidade e da vida privada (art. 5º, X) e a proteção dos dados pessoais (art. 5º, LXXIX). Esta última foi incluída pela Emenda Constitucional nº 115/2022 (Brasil, 1988; 2022a). Nenhum desses direitos está acima dos outros e, quando entram em conflito, é preciso harmonizá-los no caso concreto. A harmonização se opera pela ponderação, orientada pelos postulados da razoabilidade e da proporcionalidade, que definem o peso de cada princípio diante das circunstâncias do caso (Ávila, 2018).

A LAI adota a publicidade como regra e o sigilo como exceção (Brasil, 2011, art. 3º, I). Seu art. 31 restringe, por até cem anos, o acesso a informações pessoais ligadas à intimidade, à vida privada, à honra e à imagem, mas admite exceções: a informação pode ser liberada quando houver previsão legal ou consentimento expresso da pessoa (Brasil, 2011, art. 31, §1º, II). O consentimento é dispensado, entre

outras hipóteses, quando a informação for necessária à proteção do interesse público e geral preponderante (Brasil, 2011, art. 31, §3°, V). Por isso, o órgão não pode negar o acesso sem antes examinar o pedido.

A LGPD, por sua vez, permite ao poder público tratar dados pessoais para atender à sua finalidade pública (Brasil, 2018, art. 23). Quando o titular exerce seus direitos perante o poder público, valem os prazos e procedimentos da legislação específica, entre eles os da LAI (Brasil, 2018, art. 23, §3°). A lei de proteção de dados reconhece, portanto, a lei de transparência em seu próprio texto.

3.2. Os Consensos Doutrinários e Administrativos

Com base nessas normas, a doutrina e os órgãos de controle chegaram a quatro pontos de acordo. Cada um tem consequências diretas para quem responde a um pedido de acesso.

O primeiro é que o conflito entre as duas leis é apenas aparente: o gestor não precisa escolher qual lei vale, porque as duas se aplicam ao mesmo pedido, cada uma com sua função. Para Limberger (2022), o diálogo entre elas é possível porque nenhum dos dois direitos é absoluto e o peso de cada um deve ser medido no caso concreto. A CGU adotou o mesmo entendimento ao afirmar que as leis são "sistematicamente compatíveis entre si" e que não há "antinomia entre seus dispositivos" (Brasil, 2022b, p. 152).

O segundo ponto define qual lei orienta a decisão. A CGU entende que, quando um pedido envolve dados de pessoas naturais, a resposta deve se fundamentar nos arts. 3° e 31 da LAI, a norma mais específica para esse tipo de processo (Brasil, 2022b). Decorre desse entendimento que a LGPD, por si só, não justifica a negativa: uma

resposta que diga apenas “negado com base na LGPD” está mal fundamentada. O órgão precisa demonstrar que a informação diz respeito à intimidade, à vida privada, à honra ou à imagem de alguém, como exige o art. 31, e explicar por que isso se aplica àquele caso.

O terceiro ponto é que, entre entregar tudo e negar tudo, deve-se buscar uma solução intermediária: quando só uma parte do documento é protegida, a LAI garante o acesso ao restante "por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo" (Brasil, 2011, art. 7°, §2°). Um contrato administrativo, por exemplo, pode ser entregue com o CPF e o endereço residencial do contratado cobertos por tarja, sem perder o que interessa ao controle social: o objeto, o valor e o prazo (Brasil, 2023a).

O quarto ponto separa o que pertence ao cargo do que pertence à pessoa. Nome, cargo e remuneração do servidor podem ser divulgados porque se ligam ao exercício da função pública, como decidiu o STF no Tema 483 (Brasil, 2015). Informações sobre saúde, família ou vida doméstica continuam protegidas pelo art. 31 da LAI, mesmo quando aparecem em documentos funcionais (Crivelatti; Silva, 2025).

3.3. Os Pressupostos Fáticos da Compatibilização

Como já visto no caso que deu origem ao Tema 483, a decisão de publicar a lista de salários tinha data e responsável e, por isso, pôde ser contestada até chegar ao STF. O conteúdo publicado era conhecido e fixo, o que permitia saber exatamente o que ele revelava. O acordo entre LAI e LGPD depende dessas condições: uma pessoa que analise cada caso, uma decisão concreta que possa

ser contestada e o conhecimento exato do que está sendo divulgado.

Quando um assistente virtual responde aos pedidos apenas com inteligência artificial, essas condições se enfraquecem. O sistema responde a milhares de perguntas por dia, cada uma para uma pessoa diferente. As respostas não são registradas e assinadas como decisão de alguém, o que torna difícil saber o que contestar e contra quem. Somadas, elas podem revelar mais do que qualquer lista de salários. O limite definido pelo STF continua valendo, mas pode ser ultrapassado sem que ninguém perceba.

4. CENÁRIOS DE RISCO

Os cenários a seguir mostram como a IA pode enfraquecer essas condições.

4.1. Reidentificação por Agregação de Respostas

Um homem quer descobrir a rotina da ex-companheira, fiscal da vigilância sanitária do município. Pelo assistente virtual da prefeitura, ele pergunta quais fiscais atuam na zona norte, quais estabelecimentos foram vistoriados na última semana e em que dias. Por fim, pergunta como funciona a escala de plantões do setor. Cada resposta é lícita e poderia ser dada por qualquer servidor. Somadas, porém, elas dizem onde a fiscal estará na próxima terça-feira à tarde.

Nenhuma pergunta pedia algo sigiloso, mas a rotina que as respostas revelam faz parte da vida privada que o art. 31 da LAI protege, justamente para evitar que alguém seja localizado e exposto a riscos como esse. É improvável que um servidor

entregasse a escala de uma colega a um desconhecido; o sistema entregou a mesma informação em partes, sem perceber que montava um quebra-cabeça.

A pesquisa sobre reidentificação descreve esse mecanismo como uma eliminação em rodadas: parte-se de toda a população e, a cada dado novo, eliminam-se candidatos até restar uma só pessoa. Sweeney (2000) mostrou que três dados triviais (código postal, data de nascimento e sexo) bastavam para identificar 87% da população dos Estados Unidos. Ohm (2010) concluiu que a anonimização, como promessa de proteção, havia fracassado. Estudos posteriores reforçaram essa conclusão. Em uma base de 1,5 milhão de registros de celulares sem nenhum nome, quatro pontos de localização no tempo identificaram 95% das pessoas (De Montjoye *et al.*, 2013). Com quinze atributos demográficos, 99,98% das pessoas se tornam únicas (Rocher; Hendrickx; De Montjoye, 2019).

O assistente virtual faz o mesmo em forma de conversa: cada pergunta acrescenta um atributo, e cada resposta elimina candidatos. A LGPD não considera pessoais os dados anonimizados, salvo quando a anonimização puder ser revertida com esforços razoáveis (Brasil, 2018, art. 12). Essa avaliação, porém, costuma ser feita uma única vez, sobre a base publicada, e não acompanha a identificação construída pergunta a pergunta. Um dado anônimo na primeira consulta pode identificar alguém depois das respostas seguintes.

Se a fiscal for localizada por essa via, o órgão continua sendo, formalmente, o controlador dos dados. Na prática, fica difícil apontar onde ocorreu a falha: o servidor que cadastrou os dados não autorizou a soma das respostas, a empresa que desenvolveu o

sistema não aparece no atendimento e o cidadão que perguntou apenas usou um serviço público. A prestação de contas, que a LGPD exige como princípio (Brasil, 2018, art. 6º, X), torna-se difícil de concretizar.

4.2. Coleta Automatizada e Reuso de Dados Abertos

Uma empresa privada programa um robô para visitar e copiar o portal da transparência de um estado. Em poucas horas, ele extrai contratos, diárias, folha de pagamento e listas de beneficiários de programas sociais. Não há invasão, porque tudo já estava publicado. Esses dados passam a alimentar um sistema comercial de IA que responde a perguntas de qualquer pessoa, para qualquer finalidade, inclusive sobre uma beneficiária de programa social identificada pelo nome.

A LAI facilita essa coleta ao determinar que os portais permitam o acesso automatizado por sistemas externos, em formatos abertos, estruturados e legíveis por máquina (Brasil, 2011, art. 8º, §3º, III). A regra existe para ampliar o controle social do gasto público, por exemplo por jornalistas e pesquisadores, mas também facilita a coleta em massa para fins que nada têm a ver com fiscalização.

A LGPD admite o uso de dados de acesso público, mas com limites. O tratamento deve considerar a finalidade, a boa-fé e o interesse público que justificaram a disponibilização (Brasil, 2018, art. 7º, §3º). O uso para novas finalidades só é permitido se houver propósito legítimo e específico e se os direitos do titular forem preservados (Brasil, 2018, art. 7º, §7º). A lista de beneficiários foi publicada para que a sociedade pudesse controlar o programa social e usá-la para abastecer um produto comercial configura desvio de finalidade.

Pela LGPD, o cumprimento desses deveres cabe ao controlador, isto é, a quem decide como e para que os dados serão usados (Brasil, 2018, art. 5º, VI). No caso em análise, o controlador é a empresa que copiou o portal, e não o órgão que publicou os dados. O órgão dificilmente sabe quem fez a cópia e não tem como impedir o uso posterior. Resta a fiscalização da ANPD sobre a empresa, mais difícil quando a coleta é automática. Em 2026, ao analisar o caso do Grok, a ANPD entendeu que conteúdo gerado por IA sobre pessoa identificável pode configurar tratamento de dados pessoais (Brasil, 2026a). Esse entendimento indica que a empresa responderia não só pela base copiada, mas também pelo que o sistema afirma sobre as pessoas nas respostas.

A publicação, portanto, não autoriza qualquer uso e a administração não controla quem copia, mas controla o que publica e em que formato.

4.3. Negativas Automatizadas de Acesso

Considere-se o seguinte cenário hipotético: um jornalista pede a um ministério a lista de visitantes do gabinete do ministro e recebe a resposta: “Pedido negado. A informação contém dados pessoais protegidos pela LGPD.” Nenhum servidor leu o pedido: o sistema de triagem encontrou nomes próprios na base e aplicou a regra programada.

A cena é hipotética, mas o padrão que um sistema assim aprenderia já existe nas negativas do poder público. Entre as quase 20 mil negativas do governo federal de 2015 a 2022, a Transparência Brasil identificou 1.379 que invocavam o sigilo de dados pessoais do art. 31 da LAI. Ao analisá-las uma a uma, concluiu que 513 foram indevidas,

cerca de 37% dessas 1.379 negativas, pois tratavam de informações de claro interesse público, sem relação com a intimidade de ninguém (Transparência Brasil, 2022). A Fiquem Sabendo, por sua vez, levantou 79 pedidos negados com base na LGPD que chegaram em recurso à CGU e à Comissão Mista de Reavaliação de Informações até julho de 2021, e 39 negativas foram mantidas (Fiquem Sabendo, 2021), entre eles estão pedidos sobre os registros de visitantes do Palácio do Planalto, o que dá base real ao cenário do jornalista.

Embora essas negativas tenham sido feitas por pessoas, um sistema treinado com esse histórico tenderia a aprender que nome próprio leva à negativa, porque sistemas automatizados reproduzem os padrões dos dados que os alimentam (Barocas; Selbst, 2016). Se reproduzisse a mesma proporção, cerca de uma em cada três negativas fundadas em dados pessoais seria indevida, agora com rapidez, em escala e com aparência de decisão fundamentada.

A LAI exige que a negativa indique as razões de fato ou de direito da recusa (Brasil, 2011, art. 11, §1°, II) e garante recurso à autoridade superior (Brasil, 2011, art. 15). A negativa automática cumpre o prazo, mas sua motivação apenas repete um modelo. O recurso também perde força, pois é difícil contestar um raciocínio que ninguém fez. A análise caso a caso, base do entendimento descrito na seção 3, dá lugar a uma classificação estatística.

4.4. Alucinação e Produção de Informação Falsa

Considerando o seguinte cenário hipotético: uma servidora municipal pergunta ao assistente virtual da prefeitura quais benefícios existem para quem cuida de um familiar com doença

crônica. O sistema responde com uma lista de programas, alguns reais e outros inexistentes. Na mesma semana, outro usuário pergunta sobre servidores afastados por motivo de saúde. Ao montar a resposta, o modelo gera um nome plausível presente na base funcional (o de outra servidora, sem qualquer relação com as consultas anteriores) e o apresenta, com aparência de dado oficial, como pessoa que vive com HIV. A informação é falsa, mas passou a constar de uma resposta oficial do município.

O fenômeno é chamado de alucinação: os grandes modelos de linguagem não consultam um arquivo de fatos, mas produzem o texto mais provável a partir de padrões estatísticos, o que pode gerar afirmações fluentes, convincentes e falsas (Ji *et al.*, 2023). Mesmo quando o assistente consulta bases oficiais — arquitetura em que o sistema busca trechos em bases confiáveis e os usa como contexto para redigir a resposta, técnica conhecida como geração aumentada por recuperação (Lewis *et al.*, 2020) —, a redação final continua probabilística: o modelo pode atribuir ao dado recuperado informações que não estão nele.

Risco distinto, embora relacionado, é o vazamento de contexto ou de memória entre sessões de usuários diferentes, em que dado confiado por uma pessoa aparece na conversa de outra. Esse fenômeno decorre de falha de segregação de sessões, e não da geração probabilística, e se enfrenta pelos registros e pela segregação de sessões previstos no quinto parâmetro (seção 7.2).

A resposta atinge, ao mesmo tempo, a veracidade e a privacidade. A LAI exige que o Estado garanta informação autêntica, íntegra e atualizada (Brasil, 2011, arts. 6º, II, e 7º, IV). Dados sobre saúde recebem proteção reforçada na LGPD (Brasil, 2018, art. 5º, II), e a

condição de pessoa que vive com HIV tem sigilo protegido por lei própria, que veda a divulgação de informações que permitam identificá-la, inclusive no âmbito da administração pública (Brasil, 2022c, art. 2º, IV). A LGPD também exige que os dados sejam exatos (Brasil, 2018, art. 6º, V) e garante ao titular o direito de corrigi-los (Brasil, 2018, art. 18, III). Essas regras, porém, foram pensadas para dados guardados em uma base, e não para afirmações que o sistema inventa no momento da resposta. A honra e a imagem, garantidas pela Constituição (Brasil, 1988, art. 5º, X), são atingidas de qualquer forma.

Fora do Brasil, danos desse tipo já foram registrados: o assistente virtual da prefeitura de Nova York orientou empreendedores a adotar práticas ilegais na cidade, como recusar inquilinos que recebiam auxílio-moradia ("*housing vouchers*"), aceitar a retenção de gorjetas dos trabalhadores e deixar de aceitar pagamento em dinheiro, obrigatório por lei local (The Markup, 2024a; 2024b). No Canadá, o chatbot de uma companhia aérea informou a um passageiro uma regra de reembolso que a empresa não aplicava. O tribunal rejeitou a alegação de que o chatbot respondia por seus próprios atos e condenou a companhia, por entender que ela responde por todas as informações de seu site (Canadá, 2024).

A mesma lógica vale para o poder público: a resposta do assistente oficial é uma resposta do Estado. Ainda assim, falta um procedimento claro para corrigir o erro. Quem descobre que foi alvo de uma afirmação falsa não sabe a quem reclamar, não tem como provar o que o sistema disse e não tem garantia de que a informação não será repetida a outra pessoa.

5. TENSÕES AINDA POUCO DISCUTIDAS

Os cenários da seção 4 deixam em aberto três questões ainda sem resposta clara nas normas vigentes: o destino dos dados que já cumpriram sua finalidade (5.1), a transparência sobre o próprio sistema (5.2) e a revisão humana das decisões (5.3).

5.1. O Dado Que Já Cumpriu Sua Função

Uma servidora aposentada pesquisa o próprio nome na internet e o encontra no portal do órgão onde trabalhou, em uma lista de fiscais de um programa encerrado em 2014, ao lado da região que supervisionava. A informação é verdadeira, mas o programa acabou, o cargo não existe mais e o nome continua disponível para qualquer busca. Ela pede a retirada. O órgão responde que a informação é pública e que apagá-la seria uma forma de censura.

Os dois lados têm base legal. A LGPD permite ao titular pedir a anonimização, o bloqueio ou a eliminação de dados desnecessários ou excessivos (Brasil, 2018, art. 18, IV). As três medidas têm intensidades diferentes: anonimizar é desvincular o dado da pessoa, bloquear é suspender temporariamente seu uso e eliminar é apagá-lo (Brasil, 2018, art. 5º, XI, XIII e XIV). Em muitos casos, a anonimização basta: a lista continua disponível para consulta, sem o nome da servidora. A LAI, por sua vez, protege a publicidade dos atos do Estado, e a lista de fiscais foi informação de interesse público enquanto o programa existiu.

Divulgada em papel, uma lista como essa acabaria esquecida em um arquivo, mas na internet ela continua sendo encontrada por buscadores e, como mostrou a seção 4.1, pode ser cruzada com informações novas e ganhar um significado que não tinha. A LGPD prevê o fim do tratamento quando a finalidade é alcançada (Brasil,

2018, art. 15, I), mas também permite conservar os dados para cumprir obrigação legal (Brasil, 2018, art. 16, I). Nenhuma das duas leis define como essas regras se aplicam a um dado pessoal publicado em portal de transparência: não há prazo para a retirada, não há critério e não está definido quem decide. A resposta fica a critério de cada gestor, e casos iguais podem receber respostas diferentes. Um rito para esses pedidos, com prazo, motivação e recurso, preservaria a transparência e traria previsibilidade: o cidadão saberia o que pode pedir, e o gestor, o que deve responder.

5.2. O Sistema Também é Informação Pública?

Um pesquisador procura no portal de um órgão informações sobre o assistente virtual, como as bases de dados que o alimentam e os tipos de pergunta que ele se recusa a responder, mas não encontra nada. Ao questionar o órgão, a resposta é que essas informações não constam da lista de itens que a LAI obriga a divulgar. De fato, o art. 8°, §1°, da LAI lista o que deve ser publicado independentemente de pedido, como estrutura do órgão, repasses, despesas, licitações, contratos, programas e respostas às perguntas mais frequentes, e não menciona sistemas (Brasil, 2011). Esse rol, porém, é mínimo, já que a lei diz que "deverão constar, no mínimo", esses itens. Além disso, nada impede que o pesquisador faça um pedido específico sobre o assunto.

A questão tem peso porque é o sistema que define o que o cidadão recebe: quais dados consulta, quais combinações bloqueia e como formula as respostas. Sem conhecer essas escolhas, não há como fiscalizá-las. A transparência necessária aqui não envolve o código-fonte, que poucos cidadãos teriam condições técnicas de interpretar. Ela envolve as decisões que o gestor já conhece: de onde

vêm os dados, quais regras o sistema aplica, qual versão está em uso e quem a aprovou. Por isso, a leitura mais adequada do art. 8º é ampla: se o rol é mínimo, o princípio da publicidade recomenda que ele inclua informações sobre os sistemas que atendem o cidadão.

5.3. A Revisão das Decisões

O jornalista da seção 4.3 recebeu a negativa com o timbre do ministério e acreditou que alguém tinha lido seu pedido. Como não sabia que a decisão havia sido tomada por uma máquina, dificilmente pediria sua revisão.

A LGPD garante ao titular o direito de pedir a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais (Brasil, 2018, art. 20). Na redação original, essa revisão deveria ser feita "por pessoa natural", ou seja, por um ser humano. A exigência foi retirada ainda em 2018, por medida provisória. O Congresso tentou reinseri-la ao converter a medida em lei, mas o trecho foi vetado pelo presidente da República, e o veto foi mantido em 2019 (Brasil, 2019; Serpro, 2019). Desde então, a lei não exige que a revisão seja humana. Esse direito tem ainda dois limites: depende da iniciativa do interessado, que precisa saber que houve uma decisão, que ela foi automática e onde pedir a revisão, e protege apenas o titular dos dados tratados. Como o jornalista não é titular dos dados que pediu, é duvidoso que possa invocar o art. 20.

No setor público, a LAI oferece por outra via a revisão humana que a LGPD deixou de exigir. A própria LGPD determina que os direitos do titular perante o poder público sigam os procedimentos da legislação específica, incluindo a LAI (Brasil, 2018, art. 23, §3º). A LAI, por sua vez, protege qualquer pessoa que faça um pedido, seja ou

não titular dos dados. Ela exige que a negativa seja motivada e garante recurso à autoridade hierarquicamente superior (Brasil, 2011, arts. 11, §1°, II, e 15), ou seja, a um agente público identificável. O ideal seria inverter a lógica: em vez de esperar que o prejudicado descubra o que aconteceu, o sistema deveria avisar que houve automação e indicar, na própria resposta, o caminho para a revisão humana. Desse modo, a garantia passaria a fazer parte do desenho do sistema, sem depender da iniciativa do cidadão.

6. O MARCO LEGAL DA IA EM DISCUSSÃO

O Projeto de Lei n° 2.338/2023 foi aprovado pelo Senado em dezembro de 2024 e enviado à Câmara dos Deputados em março de 2025, onde é analisado por uma comissão especial (Brasil, 2023b). O relator anunciou, em 25 de março de 2026, que trabalharia para apresentar e votar o parecer entre meados de abril e o início de maio daquele ano (Jota, 2026). Até 25 de setembro de 2026, contudo, o parecer não havia sido votado pela comissão especial: a ficha de tramitação registra, após a previsão do relator, apenas apensações de proposições correlatas (Brasil, 2023b). Paralelamente, o Poder Executivo enviou ao Congresso o PL n° 6.237/2025, que institui o Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial (SIA) e organiza a fiscalização da matéria (Brasil, 2025, art. 1°). Em março de 2026, a Mesa Diretora da Câmara determinou a apensação do PL n° 6.237/2025 ao PL n° 2.338/2023, e a Comissão Especial recebeu a apensação em abril seguinte (Brasil, 2023b), o que reforça a convergência entre os dois textos.

O texto do Senado dialoga diretamente com os cenários deste artigo, garantindo a qualquer pessoa afetada por sistema de IA, qualquer que seja o grau de risco, o direito de saber que está

interagindo com esse tipo de sistema. Para os sistemas de alto risco, assegura o direito à explicação, à contestação e à revisão humana da decisão. Também exige avaliação de impacto algorítmico antes do uso, com conclusões públicas, ressalvados os segredos industrial e comercial. Estabelece ainda que o poder público, ao desenvolver ou contratar sistemas de IA, deve garantir o acesso às bases de dados (Zanatta; Rielli, 2024).

Entre os usos classificados como de alto risco estão os sistemas que avaliam a elegibilidade de pessoas para serviços públicos essenciais, como assistência e seguridade social. O atendimento a pedidos de acesso à informação não aparece nessa lista (Zanatta; Rielli, 2024). Assim, o sistema que negou o pedido do jornalista da seção 4.3 ficaria fora das regras mais rígidas, e o jornalista teria apenas o direito de saber que interagiu com uma máquina. A exceção seria a autoridade competente incluir esse uso entre as hipóteses de alto risco, possibilidade que tanto o texto do Senado quanto o PL nº 6.237/2025 preveem (Brasil, 2025, art. 7º).

Quanto à fiscalização, os dois textos convergem: ambos criam um sistema nacional de regulação da IA com papel central para a ANPD. O projeto do Executivo atribui à Agência a tarefa de monitorar o cumprimento de padrões mínimos de transparência dos sistemas de alto risco usados pela administração pública federal (Brasil, 2025, art. 5º, XIII). Também permite que ela peça a esses órgãos esclarecimentos sobre os dados usados no treinamento e emita recomendações (Brasil, 2025, art. 5º, VII). As duas competências, porém, alcançam apenas os sistemas de alto risco e, no caso do monitoramento, apenas a administração federal. Um assistente municipal como o dos cenários 4.1 e 4.4 ficaria fora delas.

No plano comparado, o Regulamento (UE) nº 2024/1689 (AI Act) adota lógica convergente: seu art. 50, nº 1, exige que os sistemas destinados a interagir diretamente com pessoas naturais sejam concebidos de modo a informá-las de que estão interagindo com um sistema de inteligência artificial, salvo quando isso for óbvio para uma pessoa razoavelmente bem informada e observadora; seu art. 50, nº 2, determina que os conteúdos gerados ou manipulados artificialmente sejam marcados em formato legível por máquina; e os sistemas usados por autoridades públicas para avaliar elegibilidade a benefícios e serviços públicos essenciais são classificados como de alto risco (União Europeia, 2024, considerando 58 e Anexo III, ponto 5). Também nesse regime, o atendimento a pedidos de acesso à informação não figura entre as hipóteses de alto risco.

7. PARÂMETROS DE GOVERNANÇA

Considere-se um município que decidiu contratar um assistente virtual para atendimento ao público, mas não tem uma lista do que precisa estar pronto antes do primeiro atendimento nem do que deve ser acompanhado depois. Esta seção propõe essa lista em oito parâmetros, todos apoiados em normas em vigor e cada um ligado a um risco apontado nas seções 4 e 5. O Quadro 1 mostra essa correspondência e indica como os órgãos de controle podem verificar cada parâmetro.

Quadro 1. Riscos, normas aplicáveis, parâmetros e formas de verificação

Risco	Norma aplicável	Parâmetro	Como verificar

Sistema implantado sem análise prévia de riscos (4.1 a 4.4)	LGPD, arts. 5º, XVII, 32 e 38	Avaliação prévia de impacto	Resumo público do relatório, com data, escopo e versão do sistema avaliada
Funcionamento do sistema desconhecido pelo público (5.2)	LAI, art. 8º; LGPD, art. 20, §1º	Ficha pública do sistema	Ficha publicada e atualizada a cada versão; comparação com o sistema em uso durante auditoria
Reuso dos dados fora da finalidade (4.2)	LGPD, art. 7º, §§3º e 7º; Lei nº 14.133/2021, art. 25, §3º	Regras de uso e de contratação	Termos de uso com a finalidade da publicação; cláusulas sobre dados na minuta de contrato divulgada com o edital
Identificação pela soma de respostas (4.1)	LGPD, art. 12, §1º; LAI, art. 31	Limites à soma de respostas	Relatório público dos testes de reidentificação, com método e resultados
Falta de registro do que o sistema fez (4.1 a 4.4)	LGPD, arts. 6º, III, 37 e 46	Registro das operações	Registros entregues aos órgãos de controle quando requisitados; prazo de guarda e regras de acesso definidos; teste de isolamento entre sessões
Resposta falsa (4.4)	LAI, arts. 6º, II, e 7º, IV; LGPD, arts. 5º, II, e 6º, V; Lei nº 14.289/2022, art. 2º; CF, art. 5º, X	Garantia de fidelidade	Resultados dos testes com perguntas de resposta conhecida; número de pedidos de correção e prazo médio para corrigir

Negativa sem análise humana (4.3)	LAI, arts. 11, §1º, II, e 15; Lei nº 9.784/1999, art. 50, I e §2º (âmbito federal)	Nenhuma negativa totalmente automática	Amostra de negativas com identificação do servidor responsável; taxa de reversão em recurso
Revisão que depende da iniciativa do cidadão (5.3)	LAI, art. 15; LGPD, arts. 20 e 23, §3º	Aviso de automação com caminho para revisão humana	Aviso presente nas respostas automatizadas; número de revisões feitas por servidores e tempo médio de resposta

Fonte: elaborado pelos autores (2026).

7.1. Antes de o Sistema Entrar no Ar

O primeiro parâmetro é a avaliação prévia de impacto. A LGPD prevê o relatório de impacto à proteção de dados pessoais, documento que descreve quais dados serão tratados, com que finalidade, com quais riscos e com quais medidas para reduzi-los (Brasil, 2018, arts. 5º, XVII, e 38). Um sistema que atende o público e consulta dados pessoais em grande volume deveria ter esse relatório pronto antes do primeiro atendimento, e o relatório deveria ser refeito a cada mudança relevante de versão ou de base de dados. Um resumo deve ser publicado, prática que a própria LGPD prevê ao permitir que a ANPD solicite ao poder público a publicação desses relatórios (Brasil, 2018, art. 32). Com essa medida, a administração antecipa a lógica de avaliação de impacto que o PL nº 2.338/2023 reserva aos sistemas de alto risco (Zanatta; Rielli, 2024).

O segundo parâmetro é a ficha pública do sistema. Essa ficha deve informar, de forma compreensível, de onde vêm os dados, quais

informações o sistema pode consultar, que tipos de pergunta ele se recusa a responder, qual versão está em uso e qual autoridade a aprovou. São exatamente as informações que o pesquisador da seção 5.2 procurava. O fundamento é a leitura ampla do art. 8º da LAI (Brasil, 2011), somada ao dever do controlador de fornecer informações claras sobre os critérios e procedimentos das decisões automatizadas (Brasil, 2018, art. 20, §1º). A LGPD exige essas informações quando solicitadas, e a ficha as torna públicas antes de qualquer pedido.

O terceiro parâmetro são as regras de uso e de contratação. Os termos de uso dos portais devem informar para que os dados foram publicados. Isso dá concretude ao dever de respeitar a finalidade que justificou a disponibilização (Brasil, 2018, art. 7º, §3º) e dificulta que um reuso como o da seção 4.2 alegue desconhecer essa finalidade. Quando a própria administração contrata o sistema, o contrato deve definir quem responde pelos dados, proibir o fornecedor de reaproveitá-los em outros produtos e garantir ao órgão acesso aos registros. Como a minuta do contrato integra o edital e deve ser divulgada em sítio eletrônico oficial (Brasil, 2021, art. 25, §3º), qualquer cidadão pode conferir essas cláusulas.

7.2. Enquanto o Sistema Funciona

O quarto parâmetro são os limites à soma de respostas. O sistema deve limitar consultas combinadas feitas pelo mesmo usuário, emitir alertas quando uma sequência de perguntas se aproximar da identificação de alguém e passar por testes periódicos de reidentificação, com método e resultados publicados. O fundamento é a LGPD, segundo a qual a possibilidade de reverter a anonimização deve ser avaliada por fatores objetivos, como custo,

tempo e tecnologias disponíveis (Brasil, 2018, art. 12, §1º). Em um assistente virtual, um desses fatores é o que pode ser somado ao dado ao longo da conversa, como ocorreu com a fiscal da seção 4.1 (De Montjoye *et al.*, 2013; Rocher; Hendrickx; De Montjoye, 2019).

O quinto parâmetro é o registro das operações. O órgão deve guardar cada pergunta, cada resposta, a versão do sistema e a regra aplicada (Brasil, 2018, art. 37). Esse registro sustenta os demais parâmetros, porque sem ele não há como provar o que o sistema respondeu e os órgãos de controle não têm o que auditar. Como as perguntas também podem conter dados pessoais de quem pergunta, o registro deve ter prazo de guarda definido e acesso restrito, em respeito ao princípio da necessidade (Brasil, 2018, art. 6º, III). O sistema deve ainda segregar as sessões de usuários distintos, de modo que dados informados em uma conversa não fiquem disponíveis em outra, em cumprimento ao dever de segurança do art. 46 da LGPD (Brasil, 2018, art. 46).

O sexto parâmetro é a garantia de fidelidade. Cada resposta deve indicar a fonte consultada e avisar que pode conter erros. O sistema deve oferecer um canal de correção com prazo definido e passar por testes periódicos com perguntas de resposta já conhecida. O fundamento é o dever de fornecer informação autêntica e íntegra (Brasil, 2011, arts. 6º, II, e 7º, IV) e o dever de exatidão dos dados (Brasil, 2018, art. 6º, V), somados à proteção da honra e da imagem (Brasil, 1988, art. 5º, X). Quando a resposta envolve saúde, aplicam-se ainda a proteção reforçada dos dados sensíveis e a vedação legal de divulgar informação que permita identificar a condição de saúde, inclusive no âmbito da administração pública (Brasil, 2018, art. 5º, II; Brasil, 2022c, art. 2º, IV).

7.3. Quando o Sistema Decide

O sétimo parâmetro é que nenhuma negativa seja totalmente automática. O sistema pode sugerir uma resposta, mas a negativa de acesso deve ser decidida e assinada por um servidor, com motivação própria para aquele pedido, como exige a LAI (Brasil, 2011, arts. 11, §1º, II, e 15). No âmbito federal, a Lei de Processo Administrativo exige motivação para os atos que neguem direitos e admite o uso de "meio mecânico que reproduza os fundamentos das decisões", "desde que não prejudique direito ou garantia dos interessados" (Brasil, 1999, art. 50, I e §2º). A lei aceita, portanto, o apoio mecânico à motivação, sem dispensar que alguém decida.

O oitavo parâmetro é o aviso de automação com caminho para a revisão humana. Sempre que o sistema negar, filtrar ou redirecionar um pedido, deve informar ao cidadão que a resposta foi automatizada e indicar como pedir que um servidor a reveja, nos prazos da LAI. É a mudança de lógica defendida na seção 5.3. A revisão humana, que a LGPD deixou de exigir (Brasil, 2018, art. 20), fica assegurada pela via da LAI (Brasil, 2011, art. 15; Brasil, 2018, art. 23, §3º) e passa a ser oferecida pelo próprio serviço, sem depender de o cidadão descobrir que precisa pedi-la.

8. CONSIDERAÇÕES FINAIS

O problema de pesquisa era saber se o entendimento atual sobre a compatibilização entre a LAI e a LGPD permanece suficiente quando o atendimento a pedidos de acesso à informação é feito por sistemas de inteligência artificial. A resposta é que ele permanece válido quanto ao conteúdo, mas se mostra insuficiente quanto ao modo de operação: sua eficácia depende de três condições que a

automação enfraquece: a análise do pedido por uma pessoa, a existência de uma decisão identificável e contestável e o conhecimento exato da informação divulgada.

Atingiu-se o objetivo geral com a proposta de oito parâmetros de governança, todos apoiados em normas em vigor. O objetivo específico (a) foi atingido na seção 3, que identifica essas três condições. O objetivo (b) foi atingido na seção 4, em que quatro cenários mostram como a reidentificação por agregação, o reuso de dados abertos, a negativa automatizada e a informação falsa enfraquecem essas condições. O objetivo (c) foi atingido na seção 5, que aponta as lacunas quanto ao término do tratamento, à divulgação obrigatória sobre os sistemas e à revisão de decisões automatizadas. O objetivo (d) foi atingido na seção 7, que transforma essas conclusões em parâmetros verificáveis, cada um associado a um meio de auditoria.

A contribuição teórica está em deslocar o debate da compatibilidade abstrata entre as leis para as condições fáticas que a tornam operante. A contribuição prática está em oferecer a gestores e órgãos de controle uma lista auditável, organizada em três momentos do ciclo de vida do sistema: antes da implantação, durante o funcionamento e na decisão. O marco legal da inteligência artificial segue em tramitação: até 25 de setembro de 2026, o parecer sobre o PL nº 2.338/2023 não havia sido votado pela comissão especial da Câmara, e o PL nº 6.237/2025, apensado a ele, atribui à ANPD as competências examinadas na seção 6 (art. 5º, VII e XIII), que alcançam apenas os sistemas de alto risco da administração federal. A adoção das salvaguardas propostas, portanto, não depende de nova lei.

O estudo se limita à análise normativa de cenários hipotéticos construídos a partir de casos documentados e não mede a frequência dos riscos. O levantamento foi realizado até setembro de 2026, e a comparação internacional restringe-se ao Regulamento europeu de inteligência artificial. Trabalhos futuros podem verificar, em portais federais, estaduais e municipais, o grau de uso de sistemas automatizados no atendimento, a proporção de negativas geradas por esses sistemas e a taxa de reversão dessas negativas em recurso, o que permitiria testar a aplicabilidade dos parâmetros propostos.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, V. S. de; ZULLO, B. A.; TORRES, M. Big data, algoritmos e inteligência artificial na administração pública: reflexões para a sua utilização em um ambiente democrático. **A&C – Revista de Direito Administrativo & Constitucional,** Belo Horizonte, v. 20, n. 80, p. 241-261, abr./jun. 2020. DOI: https://doi.org/10.21056/aec.v20i80.1219. Disponível em: https://revistaaec.com/index.php/revistaaec/article/view/1219. Acesso em: 25 set. 2026.

ÁVILA, H. **Teoria dos princípios:** da definição à aplicação dos princípios jurídicos. 18. ed. São Paulo: Malheiros, 2018.

BAROCAS, S.; SELBST, A. D. Big data's disparate impact. **California Law Review,** Berkeley, v. 104, n. 3, p. 671-732, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899. Acesso em: 25 set. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988.

Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 set. 2026.

BRASIL. Agência Nacional de Proteção de Dados. **Nota Técnica nº 1/2026/FIS/CGF/ANPD: sistema de inteligência artificial Grok.** Brasília, DF: ANPD, 2026a. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-1-2026-fis-cgf-anpd.pdf/@@display-file/file. Acesso em: 25 set. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo: tratamento de dados pessoais pelo poder público.** Versão 2.0. Brasília, DF: ANPD, 2023a. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_tratamento_de_dados_pessoais_pelo_poder_publico. Acesso em: 4 nov. 2026.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília, DF: Câmara dos Deputados, 2023b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: 25 set. 2026.

BRASIL. Congresso Nacional. **Veto nº 24/2019 (parcial): proteção de dados pessoais.** Brasília, DF: Congresso Nacional, 2019. Disponível em:

https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12445. Acesso em: 25 set. 2026.

BRASIL. Controladoria-Geral da União. Enunciado nº 4, de 10 de março de 2022. Diário Oficial da União: seção 1, Brasília, DF, ed. 49, p. 152, 14 mar. 2022b. Disponível em: https://www.in.gov.br/en/web/dou/-/enunciado-n-4-de-10-de-marco-de-2022-385474869. Acesso em: 25 set. 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022a. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 25 set. 2026.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 25 set. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018.

Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 set. 2026.

BRASIL. **Lei nº 14.133, de 1º de abril de 2021.** Lei de Licitações e Contratos Administrativos. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 25 set. 2026.

BRASIL. Lei nº 14.289, de 3 de janeiro de 2022. Torna obrigatória a preservação do sigilo sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose. Brasília, DF: Presidência da República, 2022c. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14289.htm. Acesso em: 25 set. 2026.

BRASIL. **Lei nº 15.352, de 25 de fevereiro de 2026.** Transforma cargos no âmbito do Poder Executivo federal; altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), para dispor sobre a Agência Nacional de Proteção de Dados (ANPD), a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, a Lei nº 15.211, de 17 de setembro de 2025 (Estatuto Digital da Criança e do Adolescente), para dispor sobre o início da vigência da referida Lei; altera as Leis nºs 9.008, de 21 de março de 1995, 11.890, de 24 de dezembro de 2008, 13.326, de 29 de julho de 2016, 13.848, de 25 de junho de 2019, e 14.600, de 19 de junho de 2023; revoga a Medida Provisória nº 1.319, de 17 de setembro de 2025; e dá outras providências. Brasília, DF: Presidência da República, 2026b. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2026/lei-15352-25-fevereiro-2026-798731-norma-pl.html. Acesso em: 25 set. 2026.

BRASIL. **Lei nº 9.784, de 29 de janeiro de 1999.** Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília, DF: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 25 set. 2026.

BRASIL. Presidência da República. Projeto de Lei nº 6.237, de 2025. Institui o Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial (SIA). Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/projetos/ato_2023_2026/2025/pl/pl-6237.htm. Acesso em: 25 set. 2026.

BRASIL. Supremo Tribunal Federal (Plenário). Recurso Extraordinário com Agravo nº 652.777/SP (Tema 483 da repercussão geral). Relator: Min. Teori Zavascki, 23 abr. 2015. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=4121428&numeroProcesso=652777&classeProcesso=ARE&numeroTema=483. Acesso em: 25 set. 2026.

CANADÁ. Civil Resolution Tribunal of British Columbia. **Moffatt v. Air Canada, 2024 BCCRT 149.** Vancouver, 2024. Disponível em: https://www.canlii.org/en/bc/bccrt/doc/2024/2024bccrt149/2024bccrt149.html. Acesso em: 25 set. 2026.

CRIVELATTI, Q. D.; SILVA, C. B. F. da. A relação entre o princípio da publicidade, a LAI e a LGPD no exercício do controle da Administração Pública pelo Ministério Público. **Boletim Científico ESMPU,** Brasília, n. 64, 2025. DOI: https://doi.org/10.63601/bcesmpu.2025.n64.e-64tc01. Disponível em:

https://escola.mpu.mp.br/publicacoescientificas/index.php/boletim/article/view/869. Acesso em: 25 set. 2026.

DE MONTJOYE, Y.-A. *et al.* Unique in the crowd: the privacy bounds of human mobility. **Scientific Reports,** London, v. 3, art. 1376, 2013. DOI: https://doi.org/10.1038/srep01376. Disponível em: https://www.nature.com/articles/srep01376. Acesso em: 25 set. 2026.

FIQUEM SABENDO. Veja como o governo vem usando a LGPD para negar pedidos de acesso à informação. Fiquem Sabendo, São Paulo, 30 ago. 2021. Disponível em: https://fiquemsabendo.com.br/transparencia/lgpd-negativa-cgu/. Acesso em: 25 set. 2026.

FUJITA, M. S. L.; OLIVEIRA, M. F. de. A lei da transparência e de acesso à informação no Brasil: o caso do Estado de São Paulo. **Perspectivas em Ciência da Informação,** Belo Horizonte, v. 28, e-41917, 2023. DOI: https://doi.org/10.1590/1981-5344/41917. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/41917. Acesso em: 25 set. 2026.

JI, Z. *et al.* Survey of hallucination in natural language generation. **ACM Computing Surveys,** New York, v. 55, n. 12, art. 248, 2023. DOI: https://doi.org/10.1145/3571730. Disponível em: https://dl.acm.org/doi/10.1145/3571730. Acesso em: 25 set. 2026.

JOTA. Relator prevê votação do PL de IA na comissão especial até o início de maio. Jota, São Paulo, 25 mar. 2026. Disponível em: https://www.jota.info/legislativo/relator-preve-votacao-do-pl-de-ia-na-comissao-especial-ate-o-inicio-de-maio. Acesso em: 25 set. 2026.

LEWIS, P. *et al.* Retrieval-augmented generation for knowledge-intensive NLP tasks. In: CONFERENCE ON NEURAL INFORMATION PROCESSING SYSTEMS (NEURIPS), 34., 2020, [S. l.]. **Advances in Neural Information Processing Systems,** [S. l.], v. 33, p. 9459-9474, 2020. Disponível em: https://proceedings.neurips.cc/paper/2020/file/6b493230205f780e1bc26945df7481e5-Paper.pdf. Acesso em: 25 set. 2026.

LIMBERGER, T. Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI): um diálogo (im)possível? As influências do direito europeu. **Revista de Direito Administrativo,** Rio de Janeiro, v. 281, n. 1, p. 113-142, 2022. DOI: https://doi.org/10.12660/rda.v281.2022.85654. Disponível em: https://periodicos.fgv.br/rda/article/view/85654. Acesso em: 25 set. 2026.

MONTEIRO, R. L. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?** Rio de Janeiro: Instituto Igarapé, 2018. (Artigo Estratégico, 39). Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 25 set. 2026.

OHM, P. Broken promises of privacy: responding to the surprising failure of anonymization. **UCLA Law Review,** Los Angeles, v. 57, p. 1701-1777, 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em: 25 set. 2026.

ROCHER, L.; HENDRICKX, J. M.; DE MONTJOYE, Y.-A. Estimating the success of re-identifications in incomplete datasets using generative models. **Nature Communications,** London, v. 10, art. 3069, 2019. DOI:

https://doi.org/10.1038/s41467-019-10933-3. Disponível em: https://www.nature.com/articles/s41467-019-10933-3. Acesso em: 25 set. 2026.

SERPRO. Congresso aprecia veto ao artigo 20 da LGPD. **Serpro,** Brasília, 2 out. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/congresso-aprecia-veto-ao-artigo-20-da-lgpd. Acesso em: 25 set. 2026.

SWEENEY, L. **Simple demographics often identify people uniquely.** Pittsburgh: Carnegie Mellon University, 2000. (Data Privacy Working Paper, 3). Disponível em: https://dataprivacylab.org/projects/identifiability/paper1.pdf. Acesso em: 25 set. 2026.

THE MARKUP. Malfunctioning NYC AI chatbot still active despite widespread evidence it's encouraging illegal behavior. The Markup, New York, 2 abr. 2024b. Disponível em: https://themarkup.org/artificial-intelligence/2024/04/02/malfunctioning-nyc-ai-chatbot-still-active-despite-widespread-evidence-its-encouraging-illegal-behavior. Acesso em: 25 set. 2026.

THE MARKUP. NYC's AI chatbot tells businesses to break the law. The Markup, New York, 29 mar. 2024a. Disponível em: https://themarkup.org/artificial-intelligence/2024/03/29/nycs-ai-chatbot-tells-businesses-to-break-the-law. Acesso em: 25 set. 2026.

TRANSPARÊNCIA BRASIL. "Sigilos de 100 anos": o uso do art. 31 da LAI em negativas. São Paulo: Transparência Brasil, 2022. Disponível em:

https://www.transparencia.org.br/downloads/publicacoes/sigilo_100anos_uso_art_31_lai_negativas.pdf. Acesso em: 25 set. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024,** que estabelece medidas harmonizadas no domínio da inteligência artificial (Regulamento relativo à inteligência artificial). Jornal Oficial da União Europeia, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689. Acesso em: 25 set. 2026.

ZANATTA, R. A. F.; RIELLI, M. **A construção da legislação de inteligência artificial no Brasil: análise técnica do texto que será votado no plenário do Senado Federal.** Data Privacy Brasil, São Paulo, 5 dez. 2024. Disponível em: https://www.dataprivacybr.org/a-construcao-da-legislacao-de-inteligencia-artificial-no-brasil-analise-tecnica-do-texto-que-sera-votado-no-plenario-do-senado-federal/. Acesso em: 25 set. 2026.

---

[1] Mestrando. Discente do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação. Universidade Federal de Roraima, Campus Paricarana, Av. Cap. Ene Garcez, 2413, Aeroporto, CEP 69.310-000, Boa Vista/RR, Brasil. E-mail: acesse o artigo original para visualizar o e-mail. ORCID: https://orcid.org/0009-0001-5518-5204.

[2] Doutor em Química. Docente do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação (orientador). Universidade Federal de Roraima, Campus Paricarana, Av. Cap. Ene Garcez, 2413, Aeroporto, CEP 69.310-000, Boa Vista/RR, Brasil. E-mail: acesse o artigo original para visualizar o e-mail. ORCID: https://orcid.org/0000-0003-2674-8634.

[3] Doutora em Biodiversidade e Biotecnologia. Docente do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação (coorientadora). Universidade Federal de Roraima, Campus Paricarana, Av. Cap. Ene Garcez, 2413, Aeroporto, CEP 69.310-000, Boa Vista/RR, Brasil. E-mail: acesse o artigo original para visualizar o e-mail. ORCID: https://orcid.org/0000-0001-9102-8751.