Dados públicos e LGPD: Um teste para decidir o que publicar

Adilson Braga

A dúvida chega ao setor jurídico das entidades públicas quase sempre no mesmo formato: este documento pode ir para o portal? A pergunta costuma vir acompanhada de duas posições extremas. De um lado, o gestor que suprime nomes, números e assinaturas de tudo o que publica, invocando a Lei nº 13.709/2018 (LGPD). De outro, quem publica os autos inteiros, com cópias de documentos de identidade e comprovantes de residência, invocando a Lei nº 12.527/2011 (LAI). As duas condutas falham pela mesma razão, que é a ausência de um método. A LGPD não é sinal verde para negar tudo, assim como a LAI não é autorização para divulgar tudo.

Proponho aqui um teste aplicável pelo servidor que decide, com fundamento normativo em cada etapa, além de uma análise técnica sobre o que distingue anonimização, pseudonimização e mascaramento, temas que a prática administrativa costuma tratar como sinônimos. O texto se dirige a entidades públicas, discute o papel dos planos de classificação da informação e traz, de forma breve, soluções já testadas na França, no Reino Unido, nos Estados Unidos e no sistema interamericano.

1. A LAI já protegia dados pessoais, e a LGPD deu sistematicidade

A proteção de dados pessoais no setor público brasileiro não começou em 2018. A LAI determina, no art. 6º, III, que o poder público assegure a proteção da informação pessoal, e dedica os arts. 31 e 32 ao tema. O art. 31 impõe que o tratamento de informações pessoais se dê de forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem, além das liberdades e garantias individuais. O § 1º restringe o acesso a informações relativas à intimidade, à vida privada, à honra e à imagem, pelo prazo máximo de cem anos, a agentes públicos legalmente autorizados e à própria pessoa. O § 3º dispensa o consentimento em hipóteses específicas e, ao tratar de estatísticas e pesquisas científicas de evidente interesse público, veda expressamente a identificação do titular, o que significa que a exigência de desidentificação já constava do direito brasileiro em 2011. O § 4º completa o desenho ao impedir que a restrição de acesso seja invocada para prejudicar apuração de irregularidades ou a recuperação de fatos históricos relevantes.

O que a LGPD acrescentou foi método. Ela trouxe definições operacionais, princípios aplicáveis a cada operação, bases legais, deveres de segurança e de prestação de contas, além de um capítulo dedicado ao Poder Público. A leitura conjunta das duas leis já foi assentada pela Controladoria-Geral da

União no Enunciado nº 4/2022, segundo o qual as decisões sobre publicidade de informações pessoais em pedidos de acesso devem ser fundamentadas nos arts. 3º e 31 da LAI, e a LAI, a Lei nº 14.129/2021 e a LGPD são sistematicamente compatíveis entre si. Em 2024, a CGU voltou ao tema em dois enunciados sobre o art. 31, § 1º, para afastar a presunção automática do prazo máximo de sigilo e para determinar que as negativas fundadas nesse dispositivo sejam relatadas e monitoradas.

A Advocacia-Geral da União seguiu a mesma direção no Parecer n. 00006/2025/GAB/DECOR/CGU/AGU, de 23 de maio de 2025, ao examinar a divulgação de anexos de convênios no Transferegov. O parecer recomendou a supressão de dados pessoais excessivos ou desnecessários, como CPF, RG, endereço e estado civil, à luz dos princípios da finalidade, da necessidade e da proporcionalidade, e ao mesmo tempo rejeitou leitura da legislação ordinária que inviabilize o controle social da Administração. O ponto decisivo, e que costuma passar despercebido, é que a própria LAI funciona como base legal para o tratamento: publicar dado pessoal em cumprimento de dever legal de transparência é cumprimento de obrigação legal, na forma do art. 7º, II, da LGPD, combinado com os arts. 23 e 26 da mesma lei. Não é preciso consentimento do titular para publicar aquilo que a lei manda publicar, e não é lícito publicar o que a lei não exige apenas porque o documento chegou ao processo. O guia orientativo da Agência Nacional de Proteção de Dados sobre o Poder Público segue a mesma lógica ao recomendar anonimização ou pseudonimização sempre que isso não comprometa o exercício do controle social.

Há ainda um terceiro pilar, frequentemente esquecido, que é o acesso parcial. O art. 7º, § 2º, da LAI determina que, quando não for autorizado o acesso integral por ser a informação parcialmente sigilosa, assegura-se o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte protegida. O direito brasileiro já possui, portanto, a figura que o direito comparado chama de versão pública. Negar o documento inteiro porque um campo contém dado pessoal contraria esse dispositivo, e é exatamente esse o erro mais comum nas respostas a pedidos de acesso. No plano do compartilhamento entre órgãos, o Supremo Tribunal Federal, ao julgar a ADI 6.649 e a ADPF 695, submeteu o fluxo de dados pessoais na Administração aos parâmetros da LGPD, com exigência de finalidade, necessidade, proporcionalidade e publicidade, o que reforça que transparência e proteção de dados operam no mesmo eixo, e não em eixos opostos.

A adaptação normativa interna também já tem precedentes. O Conselho Nacional do Ministério Público editou a Resolução nº 311/2025 para atualizar, à luz da LGPD, a norma que aplicava a LAI no âmbito da instituição (Braga; Ferreira, 2026, p. 48). É o tipo de movimento que estados e municípios precisam replicar, já que os decretos locais de regulamentação da LAI

costumam ser anteriores à LGPD e não tratam da articulação entre as duas leis.

2. Antes de publicar ou anonimizar, minimizar

A discussão sobre anonimização costuma chegar tarde. Quando o servidor pergunta se deve tarjar o CPF de um anexo, o dado já foi coletado, digitalizado, replicado em três sistemas e enviado por correio eletrônico. O princípio da necessidade do art. 6º, III, da LGPD opera antes disso, na definição de quais dados o procedimento exige. Editais que pedem cópia de documento de identidade quando bastaria o número do registro profissional, formulários de ouvidoria que exigem endereço residencial para responder a uma reclamação sobre iluminação pública e processos de inscrição que anexam certidões inteiras produzem o problema que depois se tenta resolver com tarja.

A regra prática é simples: dado não coletado não precisa ser protegido, tampouco anonimizado, e nunca vaza. No caso de processos de contratação, a distinção foi bem posta na obra que escrevi com Ricardo Padovini Pleti Ferreira: informações que permitem saber quem contratou com o poder público, por qual valor e em que condições devem ser públicas, enquanto endereços residenciais, telefones pessoais, dados de terceiros sem pertinência e cópias de documentos pessoais anexadas por hábito não agregam controle social e apenas ampliam a superfície de risco (Braga; Ferreira, 2026, p. 87-89).

3. O teste de publicação

A Tabela 1 organiza, em sete etapas, a decisão sobre um dado pessoal que se pretende publicar. Ela não substitui a análise do caso concreto, mas obriga o decisor a percorrer os pontos que a jurisprudência e os órgãos de controle consideram relevantes, e a registrar as razões.

Tabela 1. Teste de publicação de dado pessoal pelo ente público

Etapa	Pergunta	Fundamento	Consequência
1	**O dado é necessário ao procedimento que o gerou?**	**LGPD, art. 6º, III**	**Se não, corrigir a origem e deixar de coletar**
2	**Há dever legal específico de divulgar essa informação?**	**LAI, arts. 7º e 8º; LC 131/2009; Lei 14.129/2021**	**Havendo dever, a base legal é o art. 7º, II, da LGPD**

Etapa	Pergunta	Fundamento	Consequência
3	O dado é pessoal, sensível ou de criança e adolescente?	LGPD, arts. 5º, I e II, 11 e 14	Sensível e de menor exigem justificativa reforçada
4	A divulgação desse dado específico contribui para o controle social?	LAI, art. 3º; LGPD, art. 6º, I e II	Sem contribuição, não se publica
5	O fim de transparência pode ser atingido com informação menos identificável?	LGPD, arts. 6º, III, 12 e 13	Preferir agregação ou desidentificação, quando não frustrar o controle
6	A restrição é proporcional e está motivada?	LAI, art. 31; LINDB, arts. 20 a 22	Tarjar sem motivação equivale a negar sem fundamento
7	A decisão foi registrada e é revisável?	LGPD, arts. 6º, X, 37 e 38	Documentar no registro de operações e revisar por temporalidade

Elaboração do autor, a partir da Lei nº 12.527/2011, da Lei nº 13.709/2018, do Enunciado CGU nº 4/2022 e do Parecer n. 00006/2025/GAB/DECOR/CGU/AGU.

Três observações sobre o uso do teste. A primeira é que a etapa 2 resolve a maioria dos casos. Quando a lei determina a publicação, o debate sobre consentimento é impertinente, e foi nesse sentido que o Supremo Tribunal Federal fixou, no Tema 483 da repercussão geral, que é legítima a publicação, inclusive em sítio eletrônico mantido pela Administração, dos nomes dos servidores e dos valores dos respectivos vencimentos e vantagens pecuniárias. A segunda é que a etapa 4 exige um exercício honesto: perguntar o que o cidadão consegue fiscalizar com aquele dado. O nome do responsável que assinou o contrato permite controle; o número do documento de identidade dele, na maioria das vezes, não permite. A terceira é que a etapa 6 vale nas duas direções. Ocultar sem motivar é tão irregular quanto expor sem necessidade, e a ausência de motivação é justamente o vício que a AGU apontou no parecer citado.

Quatro exemplos mostram como o teste opera. Na folha de pagamento, o dever legal existe e o Tema 483 é expresso, de modo que nome, cargo, lotação e remuneração são publicados; o CPF, o endereço e o número de dependentes não ajudam no controle e ficam de fora. Em uma lista de beneficiários de programa social, o interesse público recai sobre o número de atendidos, os critérios e a distribuição territorial, o que se alcança com agregação, enquanto a identificação individual, quando exigida por norma específica, deve ser limitada ao mínimo indispensável e jamais incluir dado de saúde ou de condição social que revele vulnerabilidade. Em processo de contratação, a regra se inverte: identificar o contratado e quem assinou é o núcleo do controle, e a supressão desses elementos esvazia a fiscalização. Em manifestação de ouvidoria, o conteúdo da demanda pode ser público em forma estatística, mas a identidade do manifestante é protegida, sob pena de inibir o próprio canal.

4. Anonimizar, pseudonimizar e mascarar não são sinônimos

A LGPD define dado anonimizado como aquele relativo a titular que não possa ser identificado, considerando o uso de meios técnicos razoáveis e disponíveis na ocasião do tratamento (art. 5º, III e XI). O art. 12 retira o dado anonimizado do âmbito da lei, salvo quando o processo for revertido ou quando a reidentificação exigir esforços razoáveis, cujos critérios incluem custo, tempo e tecnologias disponíveis. A pseudonimização, tratada no art. 13, § 4º, é o tratamento pelo qual o dado perde a possibilidade de associação direta ou indireta ao indivíduo, exceto pelo uso de informação adicional mantida separadamente e em ambiente controlado. Dado pseudonimizado continua sendo dado pessoal.

O mascaramento não é categoria jurídica, e sim família de técnicas. A ISO/IEC 20889:2018 classifica as técnicas de desidentificação e trata o mascaramento, a supressão, a generalização e a randomização como transformações distintas, cada uma com efeito próprio sobre a utilidade e sobre o risco residual. A ISO/IEC 27559:2022 acrescenta o enquadramento de governança, ao exigir avaliação de contexto, de ameaças e de controles antes da escolha da técnica. O erro comum na Administração é supor que ocultar dígitos de um identificador produz anonimização. Não produz. O Grupo de Trabalho do Artigo 29 fixou, na Opinião 05/2014, três critérios para avaliar a eficácia de uma anonimização, que são a possibilidade de individualizar um titular no conjunto, a de vincular registros do mesmo titular e a de inferir informação sobre ele (Article 29 Data Protection Working Party, 2014). Um CPF parcialmente oculto permite individualizar e vincular, especialmente quando acompanhado de nome, cargo ou lotação no mesmo documento.

O regulador britânico chegou a conclusão equivalente na orientação sobre anonimização e pseudonimização publicada em 28 de março de 2025, que

trabalha com o espectro de identificabilidade e com o teste do intruso motivado, e exige a redução do risco de identificação a um nível suficientemente remoto (Information Commissioner's Office, 2025). No plano europeu, o Comitê Europeu de Proteção de Dados submeteu a consulta pública as Diretrizes 01/2025 sobre pseudonimização, e o Tribunal de Justiça da União Europeia, no acórdão de 4 de setembro de 2025, decidiu que dado pseudonimizado não é dado pessoal em todos os casos e para toda pessoa, o que impõe avaliar a identificabilidade em relação a quem recebe a informação. Essa abordagem relativa é diretamente útil ao setor público, porque a mesma base pode ser pessoal quando publicada em portal aberto e não pessoal quando compartilhada em ambiente controlado, com contrato, registro de acesso e proibição de reidentificação.

Do lado técnico, os modelos formais de risco são conhecidos há duas décadas. O k-anonimato exige que cada combinação de quase identificadores se repita ao menos k vezes na base (Sweeney, 2002), enquanto a privacidade diferencial trabalha com garantia matemática de que a presença ou ausência de um indivíduo não altera de modo perceptível o resultado de uma consulta (Dwork, 2006). O NIST tratou o assunto especificamente para dados governamentais na SP 800-188, de setembro de 2023, que recomenda a criação de um comitê de revisão de divulgação, a escolha explícita do modelo de compartilhamento, a fixação de padrões mensuráveis e a realização de estudos de reidentificação, e adverte que ferramentas simples de mascaramento não entregam desidentificação.

A conclusão prática é que a técnica segue a finalidade e a base legal, e não a estética do documento. Prova disso é a Resolução TCU nº 354/2023, que considera o CPF dado imprescindível ao exercício das competências do Tribunal, determina sua presença em acórdãos e demais documentos e veda qualquer técnica de mascaramento ou ocultação nesses casos. Há doutrina que critica com razão a descaracterização automática de identificadores em documentos públicos, por falta de amparo na LGPD e por excesso de burocracia (Pironti, 2025). O ponto não é escolher um lado, e sim reconhecer que a resposta depende da finalidade: identificar responsável em processo de controle externo é finalidade que exige o identificador; divulgar a lista de beneficiários de um programa social não exige.

A escolha da técnica também depende do tipo de informação. Identificadores diretos, como nome e número de documento, admitem supressão quando não são o objeto do controle. Quase identificadores, como data de nascimento, município e cargo, pedem generalização, porque a combinação de poucos deles individualiza uma pessoa em bases pequenas, risco tanto maior quanto menor o município. Valores contínuos, como remuneração e idade, admitem faixas. Bases inteiras destinadas a pesquisa admitem ambientes controlados em vez de publicação aberta. O ponto a reter é que a mesma informação pode

ser publicável em forma agregada e indevida em forma nominal, e que a escolha deve ser registrada, com a indicação do risco residual aceito.

5. O plano de classificação da informação como solução institucional

Nenhum teste funciona se cada servidor decidir sozinho, documento a documento. O instrumento que industrializa a decisão é o plano de classificação da informação, associado à tabela de temporalidade. Classificar significa dizer, antes do caso concreto, quais categorias de informação são de divulgação obrigatória, quais têm acesso restrito, quais contêm dados pessoais, quais contêm dados sensíveis e por quanto tempo cada uma permanece nessa condição. Com isso, a decisão deixa de ser interpretativa e passa a ser de aplicação, o que reduz erro, acelera resposta a pedidos e permite auditoria.

O diagnóstico brasileiro mostra por que esse é o elo faltante. No levantamento do Núcleo de Proteção de Dados do Tribunal de Contas do Estado de Minas Gerais, que reuniu respostas de 1.355 instituições públicas mineiras, 84% não possuíam política de classificação da informação, 83% não tinham diretrizes para identificar dados pessoais, sensíveis e de crianças e adolescentes, e, entre as que declararam ter política de classificação, menos da metade havia implementado tabela de temporalidade. No mesmo levantamento, 90,18% não mantinham registro das operações de tratamento. Sem inventário e sem classificação, a Administração decide sobre publicação no varejo, caso a caso, com resultados inconsistentes entre setores do mesmo órgão.

O contraste com a transparência formal é evidente. No Programa Nacional de Transparência Pública de 2025, conduzido pela Atricon com 33 Tribunais de Contas, foram avaliados mais de dez mil portais públicos, o índice nacional de transparência alcançou 66,6% e 2.912 portais receberam selo, sendo 998 diamante, 1.082 ouro e 832 prata (Atricon, 2025). Publica-se cada vez mais, e com melhor estrutura, sem que a triagem de dados pessoais tenha acompanhado o mesmo ritmo. O risco dessa assimetria aparece em casos concretos, como o da prefeitura amazonense que publicou lista de vacinados com dados pessoais de crianças, apurado pela Agência Nacional de Proteção de Dados e concluído em abril de 2025.

O plano de classificação da informação não precisa ser produzido do zero, e essa é a informação que costuma faltar ao gestor. Existe normalização técnica consolidada sobre o tema, distribuída em três camadas que hoje convivem sem conversar entre si.

A camada arquivística é a mais antiga. No plano internacional, a ISO 15489-1:2016 fixa os conceitos e princípios da gestão de documentos e trata o esquema de classificação, os metadados, as regras de acesso e a destinação como controles do próprio documento, aplicáveis a qualquer formato ou

ambiente tecnológico. As ISO 30300 e 30301 transformam isso em sistema de gestão com requisitos auditáveis, na mesma lógica das normas de sistema de gestão. No plano nacional, a política de arquivos da Lei nº 8.159/1991, regulamentada pelo Decreto nº 4.073/2002, e o Decreto nº 10.148/2019 estruturam o sistema e as comissões permanentes de avaliação de documentos, que são o colegiado competente para aprovar classificação e temporalidade em cada ente. Os instrumentos concretos existem: a Resolução CONARQ nº 14/2001 aprovou o código de classificação das atividades-meio, hoje substituído, no Poder Executivo federal, pelos instrumentos da Portaria AN/MGI nº 174, de 23 de setembro de 2024, que revogou a Portaria AN nº 47/2020. Para o ambiente digital, a Resolução CONARQ nº 50/2022 instituiu o e-ARQ Brasil, versão 2, com os requisitos funcionais e os metadados que um sistema de gestão arquivística deve implementar.

A segunda camada é a da segurança da informação. A ISO/IEC 27001:2022, em seu Anexo A, e a ISO/IEC 27002:2022, nos controles 5.12 e 5.13, tratam da classificação e da rotulagem da informação, exigindo esquema baseado em confidencialidade, integridade e disponibilidade, somado aos requisitos legais aplicáveis, com revisão periódica e marcação consistente ao longo do ciclo de vida. A terceira camada é a da privacidade, na qual a ISO/IEC 27701 estende o sistema de gestão para o tratamento de dados pessoais, e as ISO/IEC 20889 e 27559, já citadas, entram no momento em que se decide a técnica de desidentificação.

O ponto é que essas camadas costumam ser tratadas por áreas diferentes do mesmo órgão, que não se falam. O arquivo classifica séries documentais, a tecnologia da informação classifica ativos por criticidade e o encarregado mantém, quando mantém, um inventário de operações de tratamento. Um plano de classificação da informação útil é aquele que amarra as três em uma única tabela, de modo que cada série documental tenha simultaneamente a sua destinação arquivística, o seu grau de sigilo na forma dos arts. 23 a 30 da LAI e do Decreto nº 7.724/2012, o seu nível de segurança e a indicação de se contém dado pessoal ou sensível. O que falta, em regra, é justamente esse cruzamento com o inventário de operações de tratamento exigido pelo art. 37 da LGPD. Um plano útil responde, para cada série documental, a seis perguntas: qual a categoria de informação, qual a base legal do tratamento, se contém dado pessoal ou sensível, se é de divulgação obrigatória, facultativa ou restrita, qual a técnica aplicável antes da publicação e por quanto tempo permanece nessa condição. Quando esse quadro existe, a decisão sobre publicar deixa de depender do servidor que abriu o processo naquele dia, e a fiscalização por parte dos órgãos de controle passa a ter parâmetro objetivo.

6. O que já funciona fora do Brasil

A França resolveu parte do problema por regra geral. O art. L. 312-1-2 do Code des relations entre le public et l'administration determina que documentos administrativos que contenham dados pessoais só podem ser tornados públicos após tratamento que impossibilite a identificação, ressalvadas as hipóteses de previsão legal em sentido contrário, consentimento e categorias definidas em regulamento. A anonimização deixa de ser decisão episódica e passa a ser etapa do fluxo de publicação.

O Reino Unido investiu no desenho do ambiente, e não apenas no dado. O modelo dos Cinco Seguros, desenvolvido pelo Office for National Statistics, avalia simultaneamente pessoas, projetos, ambientes, dados e resultados, de modo que a base pode ser mais detalhada quando o acesso ocorre em ambiente seguro, com pesquisadores credenciados e verificação de saídas (UK Data Service, [s. d.]). Nos Estados Unidos, a SP 800-188 do NIST dá ao órgão público uma estrutura de governança, com comitê de revisão de divulgação, antes de qualquer decisão técnica. No plano interamericano, a Lei Modelo 2.0 sobre Acesso à Informação Pública, aprovada pela Assembleia Geral da Organização dos Estados Americanos em outubro de 2020, estrutura a solução em quatro peças que faltam a boa parte dos entes brasileiros: máxima publicidade como princípio (art. 2), difusão proativa de informação-chave (arts. 5 e 6), prova de dano com prevalência do interesse público (arts. 26 e 35) e versão pública do documento, na qual se tarjam apenas as partes alcançadas pela exceção (art. 38) (Organização dos Estados Americanos, 2020).

A versão pública merece destaque, porque é a tradução prática do teste proposto. Em vez de negar o documento inteiro ou publicá-lo por completo, o órgão produz uma versão em que a supressão é pontual, motivada e visível, preservando a compreensão do todo. É o oposto da prática, comum entre nós, de indisponibilizar anexos inteiros por precaução.

A União Europeia seguiu caminho semelhante ao tratar de dados abertos. A Diretiva (UE) 2019/1024, relativa aos dados abertos e à reutilização de informações do setor público, condiciona expressamente sua aplicação ao respeito ao Regulamento Geral sobre a Proteção de Dados, de modo que a abertura de bases não funciona como autorização para divulgar dados pessoais. A lição comum a esses arranjos é que nenhum deles escolheu entre transparência e proteção. Todos criaram etapas intermediárias, seja a desidentificação prévia obrigatória, seja o ambiente seguro de acesso, seja a versão pública do documento, seja a governança formal da decisão de divulgar.

Considerações finais

A convergência entre LAI e LGPD não é um problema de hermenêutica, e sim de processo de trabalho. As duas leis protegem direitos fundamentais de mesma hierarquia constitucional, e a compatibilização já foi afirmada pela

CGU, pela AGU e pela ANPD. O que falta às entidades públicas é o caminho entre a norma e a mesa do servidor.

Esse caminho tem cinco peças: minimizar na origem, classificar previamente a informação, aplicar um teste padronizado de publicação, escolher a técnica de desidentificação conforme a finalidade e registrar a decisão. Um ato normativo interno que fixe categorias de dados publicáveis e restritos, um plano de classificação com tabela de temporalidade, um fluxo de revisão antes da publicação e um responsável pela decisão resolvem, com baixo custo, a maior parte dos casos que hoje chegam ao jurídico como dúvida individual. Transparência e proteção de dados falham juntas quando a Administração não decide com método, e é o método, não a escolha entre uma lei e outra, que separa o portal que informa daquele que expõe.

Para quem precisa começar amanhã, a sequência mínima é conhecida. Levantar as séries documentais que hoje vão ao portal e mapear que dados pessoais elas contêm. Editar ato normativo interno com as categorias publicáveis e restritas, aprovado pela autoridade máxima e publicado. Incluir no fluxo de publicação uma etapa obrigatória de revisão, com responsável identificado. Padronizar a versão pública, com supressão pontual e nota explicativa sobre o que foi ocultado e por quê. Treinar as áreas que mais publicam, que costumam ser contratações, recursos humanos, assistência social e saúde. Registrar as decisões no inventário de operações e revisá-las nos prazos da tabela de temporalidade.

REFERÊNCIAS

ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 05/2014 on anonymisation techniques. WP 216. Brussels, 10 Apr. 2014.

ATRICON. Associação dos Membros dos Tribunais de Contas do Brasil. Resultados do Programa Nacional de Transparência Pública 2025. Brasília: Atricon, 5 dez. 2025. Disponível em: https://atricon.org.br/iv-citc-resultados-do-programa-nacional-de-transparencia-publica-2025-sao-divulgados/. Acesso em: 12 set. 2026.

BRAGA, Adilson Fernandes; FERREIRA, Ricardo Padovini Pleti. Transformação digital e proteção de dados na Administração Pública. Uberlândia: Marco Teórico, 2026.

BRASIL. Advocacia-Geral da União. Parecer n. 00006/2025/GAB/DECOR/CGU/AGU. Brasília, DF: AGU, 23 maio 2025.

BRASIL. Agência Nacional de Proteção de Dados. 3º Relatório de ciclo de monitoramento: 1º semestre de 2025. Brasília, DF: ANPD, 2025.

BRASIL. Agência Nacional de Proteção de Dados. Guia orientativo: tratamento de dados pessoais pelo Poder Público. Versão 2.0. Brasília, DF: ANPD, jun. 2023.

BRASIL. Arquivo Nacional. Portaria AN/MGI nº 174, de 23 de setembro de 2024. Aprova o código de classificação e a tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo federal. Brasília, DF: Arquivo Nacional, 2024.

BRASIL. Conselho Nacional de Arquivos. Resolução nº 14, de 24 de outubro de 2001. Aprova a versão revisada e ampliada do código de classificação de documentos de arquivo para a administração pública: atividades-meio. Rio de Janeiro: CONARQ, 2001.

BRASIL. Conselho Nacional de Arquivos. Resolução nº 50, de 6 de maio de 2022. Dispõe sobre o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos, e-ARQ Brasil, versão 2. Rio de Janeiro: CONARQ, 2022.

BRASIL. Controladoria-Geral da União. Enunciado nº 4, de 10 de março de 2022. Compatibilidade entre a Lei nº 12.527/2011, a Lei nº 14.129/2021 e a Lei nº 13.709/2018. Diário Oficial da União: seção 1, Brasília, DF, ed. 49, p. 152, 14 mar. 2022.

BRASIL. Controladoria-Geral da União. Portaria Normativa CGU nº 176, de 30 de setembro de 2024. Aprova enunciados sobre a aplicação do art. 31 da Lei nº 12.527/2011. Brasília, DF: CGU, 2024.

BRASIL. Supremo Tribunal Federal (Plenário). Ação Direta de Inconstitucionalidade 6.649/DF e Arguição de Descumprimento de Preceito Fundamental 695/DF. Relator: Min. Gilmar Mendes, 15 set. 2022.

BRASIL. Supremo Tribunal Federal (Plenário). Recurso Extraordinário com Agravo 652.777/SP. Tema 483 da repercussão geral. Relator: Min. Teori Zavascki, 23 abr. 2015.

BRASIL. Tribunal de Contas da União. Resolução TCU nº 354, de 12 de abril de 2023. Regulamenta o tratamento da informação relativa ao número de inscrição no CPF nos processos, peças e publicações do TCU. Brasília, DF: TCU, 2023.

BRASIL. Decreto nº 4.073, de 3 de janeiro de 2002. Regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados. Brasília, DF: Presidência da República, 2002.

BRASIL. Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011. Brasília, DF: Presidência da República, 2012.

BRASIL. Decreto nº 10.148, de 2 de dezembro de 2019. Dispõe sobre o Sistema de Gestão de Documentos e Arquivos da administração pública federal e sobre as comissões permanentes de avaliação de documentos. Brasília, DF: Presidência da República, 2019.

BRASIL. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados. Brasília, DF: Presidência da República, 1991.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto na Constituição Federal. Brasília, DF: Presidência da República, 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital. Brasília, DF: Presidência da República, 2021.

DWORK, Cynthia. Differential privacy. In: INTERNATIONAL COLLOQUIUM ON AUTOMATA, LANGUAGES AND PROGRAMMING (ICALP), 33., 2006, Venice. Proceedings [...]. Berlin: Springer, 2006. p. 1-12.

ESTADOS UNIDOS. National Institute of Standards and Technology. De-identifying government datasets: techniques and governance. NIST SP 800-188. Gaithersburg: NIST, Sept. 2023. Disponível em: https://csrc.nist.gov/pubs/sp/800/188/final. Acesso em: 12 set. 2026.

EUROPEAN DATA PROTECTION BOARD. Guidelines 01/2025 on pseudonymisation. Brussels: EDPB, 16 Jan. 2025. Disponível em: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf. Acesso em: 12 set. 2026.

FRANÇA. Code des relations entre le public et l'administration, art. L. 312-1-2. Paris, 2016. Disponível em: https://www.cada.fr/administration/lanonymisation-des-donnees. Acesso em: 12 set. 2026.

INFORMATION COMMISSIONER'S OFFICE. Anonymisation, pseudonymisation and privacy enhancing technologies guidance. Wilmslow: ICO, 28 Mar. 2025. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-

guidance-and-resources/data-sharing/anonymisation/about-this-guidance/. Acesso em: 12 set. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 15489-1:2016: information and documentation, records management, part 1: concepts and principles. Geneva: ISO, 2016.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 20889:2018: privacy enhancing data de-identification terminology and classification of techniques. Geneva: ISO, 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27001:2022: information security, cybersecurity and privacy protection, information security management systems, requirements. Geneva: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27002:2022: information security, cybersecurity and privacy protection, information security controls. Geneva: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27559:2022: privacy enhancing data de-identification framework. Geneva: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27701:2025: information security, cybersecurity and privacy protection, privacy information management systems, requirements and guidance. 2. ed. Geneva: ISO, 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 30301:2019: information and documentation, management systems for records, requirements. Geneva: ISO, 2019.

MINAS GERAIS. Tribunal de Contas do Estado. Núcleo de Proteção de Dados. [Diagnóstico da adequação das instituições públicas mineiras à LGPD]. Auditoria operacional. Processo SEI nº 24.0.000000310-3. Belo Horizonte: TCEMG, 10 fev. 2025.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública. Washington, DC: OEA, out. 2020.

PIRONTI, Rodrigo. Seria o CPF um dado pessoal "especial"? A "novela" da descaracterização de dados pessoais em documentos públicos. Curitiba: Zênite Fácil, 7 abr. 2025.

SWEENEY, Latanya. k-anonymity: a model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, v. 10, n. 5, p. 557-570, 2002.

UK DATA SERVICE. What is the Five Safes framework? Colchester: UK Data Service, [s. d.]. Disponível em: https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/. Acesso em: 12 set. 2026.

UNIÃO EUROPEIA. Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público. Jornal Oficial da União Europeia, Luxemburgo, L 172, p. 56-83, 26 jun. 2019.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Acórdão de 4 de setembro de 2025, EDPS contra CUR, processo C-413/23 P. Luxemburgo, 2025.