

1. Item 1.1: A transparência é a regra e o sigilo é exceção

Problema: O texto original foca na publicidade passiva. É necessário incluir a obrigação de transparência ativa por padrão e em formatos interoperáveis.

Sugestão de Nova Redação:

"A transparência pública deve ser garantida na maior medida possível, priorizando-se a transparência ativa por padrão, em formato aberto, estruturado e legível por máquina, conforme o Art. 29 da Lei nº 14.129/2021. O sigilo deve ser interpretado restritivamente, e a divulgação de informações deve observar o princípio da minimização de dados, assegurando que apenas o estritamente necessário ao interesse público seja publicado, preservando a dignidade do titular."

2. Item 1.2: Exceções da transparência - Dados Pessoais

Problema: O Guia cita o prazo de 100 anos de forma isolada, o que pode incentivar o sigilo excessivo. É preciso integrar a presunção de 15 anos.

Sugestão de Nova Redação:

"As informações pessoais relativas à intimidade têm seu acesso restrito (Art. 31 da LAI), mas o prazo de 100 anos é um limite máximo, não a regra. Na ausência de indicação expressa de prazo motivado pelo risco concreto, presume-se a restrição de apenas 15 (quinze) anos, conforme o Enunciado CGU nº 1/2024. Decorrido este período, o órgão deve reavaliar a informação, priorizando o acesso via técnicas de descaracterização (tarjamento) para não prejudicar o controle social nem a privacidade."

3. Item 1.2: Fundamentos administrativos para negativa (Desproporcionalidade)

Problema: O texto atual permite negativas subjetivas por "esforço excessivo", servindo de barreira à fiscalização.

Sugestão de Nova Redação (Rigorismo Pro-Cidadão):

"A negativa de acesso fundamentada em desproporcionalidade ou desarrazoabilidade não pode ser invocada de maneira geral ou abstrata. O órgão é obrigado a evidenciar, por análise técnica, a falta de recursos para o atendimento. Independentemente da alegação, a Administração deve obrigatoriamente disponibilizar meios para que o cidadão realize a consulta *in loco* ou obtenha a informação de forma parcial ou descaracterizada, garantindo a auditabilidade do processo."

4. Inclusão Necessária: Proteção Prioritária de Crianças e Adolescentes

Problema: O capítulo 1 ignora o tratamento especial exigido pelo Estatuto Digital da Criança e do Adolescente.

Sugestão de Inclusão de Novo Parágrafo:

"Proteção Prioritária de Menores: No tratamento de dados de crianças e adolescentes em sistemas de transparência, o Poder Público deve garantir o nível mais elevado de proteção por padrão (*High Level of Protection by Design*), sendo vedado qualquer perfilamento comportamental ou divulgação nominal que não atenda estritamente ao seu melhor interesse, nos termos do Art. 7º da Lei nº 15.211/2025."

5. Final do Capítulo 1: Gestão Documental e Fiscalização

Problema: Falta clareza sobre a rastreabilidade das decisões de sigilo impostas pelo gestor.

Sugestão de Nova Redação:

"O aprimoramento da gestão documental deve obrigatoriamente incluir mecanismos de auditabilidade e rastreabilidade de acessos e decisões. Toda operação de tarjamento ou anonimização deve gerar uma trilha de auditoria que identifique o agente responsável e o fundamento legal, permitindo que a CGU e a ANPD fiscalizem se a proteção ao titular foi aplicada corretamente ou se houve ocultação indevida de ato ilegal."

CONTRIBUIÇÕES TÉCNICAS AO GUIA ORIENTATIVO: LAI E LGPD NA ADMINISTRAÇÃO PÚBLICA

Apresentam-se sugestões de aprimoramento ao texto do Guia Orientativo promovido pela Controladoria-Geral da União (CGU) e pela Autoridade Nacional de Proteção de Dados (ANPD), com foco no aperfeiçoamento da governança pública, inovação tecnológica e proteção de direitos fundamentais:

1. COMPLEMENTAÇÃO AO CAPÍTULO 3 (Item 3.3, alínea 'd' – Estatísticas e Pesquisas)

- **Seção Correspondente:** Capítulo 3, Item 3.3, alínea 'd' (*Orientações para fornecer informações pessoais para pesquisa compatibilizando as disposições da LAI e da LGPD*).
- **Sugestão de Aprimoramento:** Recomenda-se incluir no Guia a orientação para que os órgãos públicos e instituições de ensino/pesquisa adotem ambientes virtuais controlados de amostragem (*Data Cleanrooms*) e protocolos padronizados de pseudonimização. Essa medida assegura a utilidade estatística dos dados acadêmicos para o avanço da ciência e da inovação pública, garantindo pleno alinhamento aos princípios da minimização, segurança e finalidade previstos no art. 6º da LGPD.

2. COMPLEMENTAÇÃO AO CAPÍTULO 4 (Item 4.3 – Transparência por Desenho)

- **Seção Correspondente:** Capítulo 4, Item 4.3 (*Transparência por desenho e revisão de fluxos de trabalho*).
- **Sugestão de Aprimoramento:** Recomenda-se aprofundar as diretrizes do Item 4.3 para orientar a inclusão de requisitos funcionais de *Privacy and Transparency by Design* desde a fase de modelagem, desenvolvimento e contratação de sistemas de informação públicos (em alinhamento à Lei do Governo Digital – Lei nº 14.129/2021). A arquitetura dos sistemas deve prever nativamente a segregação de bancos de dados, permitindo a extração automatizada de dados abertos com mascaramento automático de identificadores sensíveis, reduzindo o custo operacional e o tempo de resposta a pedidos via LAI.

3. COMPLEMENTAÇÃO AO CAPÍTULO 2 (Item 2.1 – Princípios e Direitos dos Titulares)

- **Seção Correspondente:** Capítulo 2, Item 2.1 (*Princípios e hipóteses legais aplicáveis ao tratamento de dados pessoais pelo Poder Público*).
- **Sugestão de Aprimoramento:** Propõe-se a inclusão de diretrizes para a padronização dos fluxos operacionais de atendimento aos direitos dos titulares de dados (art. 18 da LGPD) no setor público. Recomenda-se a integração dos canais formais de Ouvidoria e da Plataforma Fala.BR com os sistemas de identificação digital do Poder Público, adotando os níveis de autenticação da Plataforma Gov.br (Níveis Prata e Ouro) como parâmetro seguro de verificação de identidade, garantindo celeridade, interoperabilidade e proteção contra acessos não autorizados.

CONSULTA PÚBLICA — GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

CGU / ANPD — Brasil Participativo

Contribuinte: Luiz Felipe Vieira de Siqueira

Doutorando em Inovação Tecnológica — PPGIT/UFMG

Orientadora: Profa. Dra. Rita de Cássia de Oliveira Sebastião | Coorientador: Prof. Dr. Fabrício B. P. Polido

E-mail: lfvsiqueira@gmail.com | Lattes: <http://lattes.cnpq.br/7239020013220546>

CONTRIBUIÇÃO AO CAPÍTULO 4 DO GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

Garantindo a Transparência Pública com Proteção dos Dados Pessoais — Itens 4.1 e 4.2

Prezados membros da Controladoria-Geral da União (CGU) e da Autoridade Nacional de Proteção de Dados (ANPD),

Parabenizo a iniciativa de elaboração deste Guia, que representa um avanço significativo na redução da insegurança jurídica enfrentada pela Administração Pública no tratamento de pedidos de acesso à informação que envolvam dados pessoais. A ausência de critérios operacionais claros de ponderação tem alimentado o fenômeno que a doutrina identifica como "*escudo argumentativo*": a instrumentalização da LGPD como cláusula de barreira genérica para ocultar informações de interesse público — prática evidenciada em episódios como o caso INEP e debatida no Acórdão TCU 96/2024. A consequência é uma patologia administrativa que compromete simultaneamente a *accountability* e a segurança jurídica dos titulares de dados.

Como pesquisador de doutorado com foco na intersecção entre a LAI e a LGPD, desenvolvi o Sistema de Apoio à Decisão LAI×LGPD (SAD v8.0) — um motor lógico-algorítmico, construído mediante *Design Science Research*, que traduz o juízo de proporcionalidade em uma arquitetura computacional baseada em regras de decisão. O artefato foi submetido à Rodada 1 do método Delphi (n=30 especialistas em Direito Digital e Governança Regulatória), que atingiu consenso elevado quanto à utilidade do SAD como framework capaz de converter a "zona cinzenta" da LGPD em processo decisório claro e auditável. O protótipo funcional de código aberto está disponível em [SAD LAI×LGPD v8.0](#) (Manual de Operação: [Tutorial SAD v8.0](#)). Ao analisar os itens 4.1 e 4.2 da minuta, verifico

que o roteiro ali proposto alinha-se estruturalmente aos *gates* lógicos do SAD v8.0, o que permite oferecer três contribuições fundamentadas em evidências de implementação.

1 INVERSÃO METODOLÓGICA DOS PASSOS 4 E 5 DO ROTEIRO (ITEM 4.2)

A minuta propõe que o agente público realize a *"Ponderação entre interesse coletivo e proteção à privacidade"* (Passo 4) antes da *"Análise da necessidade e da minimização dos dados"* (Passo 5). Essa sequência contraria a estrutura lógica do teste trifásico da proporcionalidade, consolidada na doutrina e na jurisprudência constitucionais, segundo a qual a análise de *necessidade* — a busca por meio alternativo menos gravoso ao direito fundamental restringido — deve obrigatoriamente anteceder o sopesamento em sentido estrito.

Na prática, colocar a minimização como etapa posterior ao sopesamento impõe ao gestor público um esforço cognitivo desnecessário: ele é levado a ponderar valores em abstrato quando uma técnica concreta de anonimização ou tarjamento poderia resolver o conflito antes mesmo de chegar ao sopesamento. A experiência de implementação do SAD v8.0 demonstra que, quando o agente é forçado a testar medidas de minimização — como supressão seletiva, pseudonimização ou anonimização por agregação — antes do sopesamento, uma parcela significativa dos pedidos é resolvida pelo deferimento parcial. O encerramento se dá quando o risco residual pós-aplicação da salvaguarda atinge limiar tolerável, parametrizado no *NIST Privacy Framework* (PR.DP-P5 — score $P \times I \leq 25$), dispensando o gate do sopesamento, que é reservado exclusivamente para os casos de genuína tensão irreduzível entre transparência e privacidade.

Sugestão de redação para o Guia:

Recomenda-se que o Passo 4 do roteiro seja dedicado à análise de necessidade e minimização dos dados — avaliação de alternativas menos gravosas, como anonimização, pseudonimização ou tarjamento — e que o Passo 5 seja reservado à ponderação final entre o direito de acesso à informação de interesse coletivo e a proteção à privacidade, em observância à sequência lógica do princípio da proporcionalidade (adequação → necessidade → proporcionalidade em sentido estrito).

2 PARAMETRIZAÇÃO DO PASSO 6 POR MEIO DO RIPD (ITEM 4.2)

O Guia estabelece no Passo 6 que a decisão final deve ser motivada e registrada para possibilitar o controle e evidenciar a ponderação realizada. A medida é acertada, mas a minuta não especifica o instrumento pelo qual esse registro deve ser formalizado em casos de negativa complexa.

A Resolução CD/ANPD nº 2/2022 já prevê o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como instrumento de documentação estruturada do tratamento de dados e dos riscos a ele associados. Orientar expressamente sua utilização no Passo 6 cumpriria dupla função: impor ao Estado um ônus argumentativo auditável — afastando a *"discrecionariade opaca"* — e criaria um repositório padronizado de decisões que favorece a formação de jurisprudência administrativa. A implementação do SAD v8.0 demonstra a viabilidade de automatizar o rascunho do RIPD a partir das variáveis coletadas ao longo dos gates, nos moldes da Resolução CD/ANPD nº 2/2022 e da ISO/IEC 29134:2017, com chancela obrigatória do Encarregado de Dados (DPO) nos termos do art. 41 da LGPD — garantindo que a automação atua como apoio à convicção humana, e não como substituto dela.

Sugestão de redação para o Guia:

Recomenda-se que o Passo 6 oriente expressamente que, nos casos de negativa total ou parcial de acesso a dados pessoais de terceiros, a motivação da decisão seja formalizada por meio de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), estruturado nos termos da Resolução CD/ANPD nº 2/2022, com registro da análise de risco, das alternativas de minimização consideradas e da ponderação realizada, com identificação e chancela do Encarregado de Dados Pessoais (LGPD, art. 41).

3 ACOPLAMENTO DO ROTEIRO A SISTEMAS AUTOMATIZADOS DE TRIAGEM (ITEM 4.1)

O item 4.3 já menciona a *"transparência por desenho"* como diretriz para reduzir a casuística decisória. O SAD v8.0 demonstra a viabilidade técnica de dar um passo além: o fluxograma do item 4.1 pode ser implementado como módulo de triagem acoplado aos portais

e-SIC, permitindo que pedidos de baixo risco sejam resolvidos automaticamente — com deferimento imediato quando o dado for meramente funcional (LAI, art. 31, §3º) ou já tiver sido tornado público pelo próprio titular (LGPD, art. 7º, §4º) — reservando a análise humana para os casos de genuína tensão entre transparência e privacidade.

A prova de conceito mais robusta para essa proposta é a simulação do caso INEP: ao processar os microdados de desempenho escolar, o SAD v8.0 identificou que a negativa total de acesso fundada na LGPD era desproporcional. O motor acionou o laço de PETs e aplicou técnicas de k-anonimato que permitiram a divulgação das estatísticas de interesse público sem possibilitar a reidentificação de estudantes individuais. O Gate G1 (adequação) e o Gate G2 (necessidade/PETs) encerraram o processo antes mesmo de alcançar o sopesamento em sentido estrito — exatamente a sequência lógica cuja correção se propõe na Contribuição 1 supra. Importa destacar que o protótipo funcional opera integralmente em memória local do navegador, sem banco de dados em nuvem ou servidores externos, incorporando o próprio princípio da privacidade por concepção (*Privacy by Design*) que o item 4.3 do Guia recomenda — demonstrando que um sistema de triagem pode ser ao mesmo tempo eficiente e estruturalmente privacidade-compatível.

Sugestão de redação para o Guia:

Recomenda-se que o Guia oriente os órgãos e entidades públicas a implementar o roteiro do item 4.1 em sistemas automatizados de triagem integrados aos portais e-SIC, parametrizando as perguntas fechadas dos Passos 1 a 3 como filtros de acesso imediato, de modo a desonerar as ouvidorias e reservar a análise de proporcionalidade para os pedidos que efetivamente envolvam conflito entre transparência e proteção de dados pessoais.

4 SÍNTESE DAS PROPOSTAS

Em síntese, propõe-se: (i) a inversão dos Passos 4 e 5 do roteiro do item 4.2, para observância da sequência lógica do teste trifásico da proporcionalidade; (ii) a indicação expressa do RIPD como instrumento de registro da motivação nos casos de negativa complexa (Passo 6), com chancela do Encarregado de Dados (LGPD, art. 41); e (iii) a recomendação de

implementação do roteiro do item 4.1 em sistemas automatizados de triagem nos portais e-SIC, em consonância com o princípio da transparência por desenho (item 4.3 do Guia).

Coloco o protótipo funcional do SAD v8.0 (código-fonte HTML/JS — [Anexo I](#)) e o Manual Didático de Operação para gestores públicos, advogados e DPOs ([Anexo II](#)) à disposição da CGU e da ANPD, para demonstrar a viabilidade tecnológica de transformar o roteiro do Capítulo 4 em ferramenta executável para toda a Administração Pública Federal.

Belo Horizonte, julho de 2026.

Documento assinado digitalmente
 LUIZ FELIPE VIEIRA DE SIQUEIRA
Data: 18/07/2026 12:36:23-0300
Verifique em <https://validar.iti.gov.br>

Luiz Felipe Vieira de Siqueira

Doutorando em Inovação Tecnológica — PPGIT/UFMG

Orientadora: Profa. Dra. Rita de Cássia de Oliveira Sebastião

Coorientador: Prof. Dr. Fabrício B. P. Polido

lfvsiqueira@gmail.com

CONSULTA PÚBLICA — GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

CGU / ANPD — Brasil Participativo

Contribuinte: Luiz Felipe Vieira de Siqueira

Doutorando em Inovação Tecnológica — PPGIT/UFMG

Orientadora: Profa. Dra. Rita de Cássia de Oliveira Sebastião | Coorientador: Prof. Dr. Fabrício B. P. Polido

E-mail: lfvsiqueira@gmail.com | Lattes: <http://lattes.cnpq.br/7239020013220546>

CONTRIBUIÇÃO AO CAPÍTULO 4 DO GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

Garantindo a Transparência Pública com Proteção dos Dados Pessoais — Itens 4.1 e 4.2

Prezados membros da Controladoria-Geral da União (CGU) e da Autoridade Nacional de Proteção de Dados (ANPD),

Parabenizo a iniciativa de elaboração deste Guia, que representa um avanço significativo na redução da insegurança jurídica enfrentada pela Administração Pública no tratamento de pedidos de acesso à informação que envolvam dados pessoais. A ausência de critérios operacionais claros de ponderação tem alimentado o fenômeno que a doutrina identifica como "*escudo argumentativo*": a instrumentalização da LGPD como cláusula de barreira genérica para ocultar informações de interesse público — prática evidenciada em episódios como o caso INEP e debatida no Acórdão TCU 96/2024. A consequência é uma patologia administrativa que compromete simultaneamente a *accountability* e a segurança jurídica dos titulares de dados.

Como pesquisador de doutorado com foco na intersecção entre a LAI e a LGPD, desenvolvi o Sistema de Apoio à Decisão LAI×LGPD (SAD v8.0) — um motor lógico-algorítmico, construído mediante *Design Science Research*, que traduz o juízo de proporcionalidade em uma arquitetura computacional baseada em regras de decisão. O artefato foi submetido à Rodada 1 do método Delphi (n=30 especialistas em Direito Digital e Governança Regulatória), que atingiu consenso elevado quanto à utilidade do SAD como framework capaz de converter a "zona cinzenta" da LGPD em processo decisório claro e auditável. O protótipo funcional de código aberto está disponível em [SAD LAI×LGPD v8.0](#) (Manual de Operação: [Tutorial SAD v8.0](#)). Ao analisar os itens 4.1 e 4.2 da minuta, verifico

que o roteiro ali proposto alinha-se estruturalmente aos *gates* lógicos do SAD v8.0, o que permite oferecer três contribuições fundamentadas em evidências de implementação.

1 INVERSÃO METODOLÓGICA DOS PASSOS 4 E 5 DO ROTEIRO (ITEM 4.2)

A minuta propõe que o agente público realize a *"Ponderação entre interesse coletivo e proteção à privacidade"* (Passo 4) antes da *"Análise da necessidade e da minimização dos dados"* (Passo 5). Essa sequência contraria a estrutura lógica do teste trifásico da proporcionalidade, consolidada na doutrina e na jurisprudência constitucionais, segundo a qual a análise de *necessidade* — a busca por meio alternativo menos gravoso ao direito fundamental restringido — deve obrigatoriamente anteceder o sopesamento em sentido estrito.

Na prática, colocar a minimização como etapa posterior ao sopesamento impõe ao gestor público um esforço cognitivo desnecessário: ele é levado a ponderar valores em abstrato quando uma técnica concreta de anonimização ou tarjamento poderia resolver o conflito antes mesmo de chegar ao sopesamento. A experiência de implementação do SAD v8.0 demonstra que, quando o agente é forçado a testar medidas de minimização — como supressão seletiva, pseudonimização ou anonimização por agregação — antes do sopesamento, uma parcela significativa dos pedidos é resolvida pelo deferimento parcial. O encerramento se dá quando o risco residual pós-aplicação da salvaguarda atinge limiar tolerável, parametrizado no *NIST Privacy Framework* (PR.DP-P5 — score $P \times I \leq 25$), dispensando o gate do sopesamento, que é reservado exclusivamente para os casos de genuína tensão irreduzível entre transparência e privacidade.

Sugestão de redação para o Guia:

Recomenda-se que o Passo 4 do roteiro seja dedicado à análise de necessidade e minimização dos dados — avaliação de alternativas menos gravosas, como anonimização, pseudonimização ou tarjamento — e que o Passo 5 seja reservado à ponderação final entre o direito de acesso à informação de interesse coletivo e a proteção à privacidade, em observância à sequência lógica do princípio da proporcionalidade (adequação → necessidade → proporcionalidade em sentido estrito).

2 PARAMETRIZAÇÃO DO PASSO 6 POR MEIO DO RIPD (ITEM 4.2)

O Guia estabelece no Passo 6 que a decisão final deve ser motivada e registrada para possibilitar o controle e evidenciar a ponderação realizada. A medida é acertada, mas a minuta não especifica o instrumento pelo qual esse registro deve ser formalizado em casos de negativa complexa.

A Resolução CD/ANPD nº 2/2022 já prevê o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como instrumento de documentação estruturada do tratamento de dados e dos riscos a ele associados. Orientar expressamente sua utilização no Passo 6 cumpriria dupla função: impor ao Estado um ônus argumentativo auditável — afastando a *"discrecionalidade opaca"* — e criaria um repositório padronizado de decisões que favorece a formação de jurisprudência administrativa. A implementação do SAD v8.0 demonstra a viabilidade de automatizar o rascunho do RIPD a partir das variáveis coletadas ao longo dos gates, nos moldes da Resolução CD/ANPD nº 2/2022 e da ISO/IEC 29134:2017, com chancela obrigatória do Encarregado de Dados (DPO) nos termos do art. 41 da LGPD — garantindo que a automação atua como apoio à convicção humana, e não como substituto dela.

Sugestão de redação para o Guia:

Recomenda-se que o Passo 6 oriente expressamente que, nos casos de negativa total ou parcial de acesso a dados pessoais de terceiros, a motivação da decisão seja formalizada por meio de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), estruturado nos termos da Resolução CD/ANPD nº 2/2022, com registro da análise de risco, das alternativas de minimização consideradas e da ponderação realizada, com identificação e chancela do Encarregado de Dados Pessoais (LGPD, art. 41).

3 ACOPLAMENTO DO ROTEIRO A SISTEMAS AUTOMATIZADOS DE TRIAGEM (ITEM 4.1)

O item 4.3 já menciona a *"transparência por desenho"* como diretriz para reduzir a casuística decisória. O SAD v8.0 demonstra a viabilidade técnica de dar um passo além: o fluxograma do item 4.1 pode ser implementado como módulo de triagem acoplado aos portais

e-SIC, permitindo que pedidos de baixo risco sejam resolvidos automaticamente — com deferimento imediato quando o dado for meramente funcional (LAI, art. 31, §3º) ou já tiver sido tornado público pelo próprio titular (LGPD, art. 7º, §4º) — reservando a análise humana para os casos de genuína tensão entre transparência e privacidade.

A prova de conceito mais robusta para essa proposta é a simulação do caso INEP: ao processar os microdados de desempenho escolar, o SAD v8.0 identificou que a negativa total de acesso fundada na LGPD era desproporcional. O motor acionou o laço de PETs e aplicou técnicas de k-anonimato que permitiram a divulgação das estatísticas de interesse público sem possibilitar a reidentificação de estudantes individuais. O Gate G1 (adequação) e o Gate G2 (necessidade/PETs) encerraram o processo antes mesmo de alcançar o sopesamento em sentido estrito — exatamente a sequência lógica cuja correção se propõe na Contribuição 1 supra. Importa destacar que o protótipo funcional opera integralmente em memória local do navegador, sem banco de dados em nuvem ou servidores externos, incorporando o próprio princípio da privacidade por concepção (*Privacy by Design*) que o item 4.3 do Guia recomenda — demonstrando que um sistema de triagem pode ser ao mesmo tempo eficiente e estruturalmente privacidade-compatível.

Sugestão de redação para o Guia:

Recomenda-se que o Guia oriente os órgãos e entidades públicas a implementar o roteiro do item 4.1 em sistemas automatizados de triagem integrados aos portais e-SIC, parametrizando as perguntas fechadas dos Passos 1 a 3 como filtros de acesso imediato, de modo a desonerar as ouvidorias e reservar a análise de proporcionalidade para os pedidos que efetivamente envolvam conflito entre transparência e proteção de dados pessoais.

4 SÍNTESE DAS PROPOSTAS

Em síntese, propõe-se: (i) a inversão dos Passos 4 e 5 do roteiro do item 4.2, para observância da sequência lógica do teste trifásico da proporcionalidade; (ii) a indicação expressa do RIPD como instrumento de registro da motivação nos casos de negativa complexa (Passo 6), com chancela do Encarregado de Dados (LGPD, art. 41); e (iii) a recomendação de

implementação do roteiro do item 4.1 em sistemas automatizados de triagem nos portais e-SIC, em consonância com o princípio da transparência por desenho (item 4.3 do Guia).

Coloco o protótipo funcional do SAD v8.0 (código-fonte HTML/JS — [Anexo I](#)) e o Manual Didático de Operação para gestores públicos, advogados e DPOs ([Anexo II](#)) à disposição da CGU e da ANPD, para demonstrar a viabilidade tecnológica de transformar o roteiro do Capítulo 4 em ferramenta executável para toda a Administração Pública Federal.

Belo Horizonte, julho de 2026.

Documento assinado digitalmente
 LUIZ FELIPE VIEIRA DE SIQUEIRA
Data: 18/07/2026 12:36:23-0300
Verifique em <https://validar.iti.gov.br>

Luiz Felipe Vieira de Siqueira

Doutorando em Inovação Tecnológica — PPGIT/UFMG

Orientadora: Profa. Dra. Rita de Cássia de Oliveira Sebastião

Coorientador: Prof. Dr. Fabrício B. P. Polido

lfvsiqueira@gmail.com

Pág.	Trecho referido no documento	Comentário
4	“Para que o princípio da máxima divulgação funcione, é essencial que qualquer restrição ao acesso à informação tenha uma base legal clara e legítima.”	Sugere-se utilizar a expressão /base legal/ somente quando se referir a LGPD, evitando-se a utilização da expressão, típico da LGPD para falar sobre a LAI. No caso em tela, sugere-se substituir pela palavra /justificativa/.
5	Quadro IMPORTANTE: “Apenas leis ou normas com status equivalentes ou superiores podem estabelecer sigilos...”	Sugere-se reavaliar a presente afirmação, pois ela nega validade ao Decreto 7.724/2012, que regulamenta a própria LAI.
5	Seção sobre sigilos e informações empresariais	O conceito de ‘informação empresarial’ não possui definição legal e, por isso, não deveria ser mencionado expressamente.
6	Título “Fundamentos administrativos para negativa de informação”	Considerando que as negativas possuem fundamento legal, sugere-se substituir o título para /Outros Fundamentos JURÍDICOS para negativa de acesso à informação. Contribuição sobre as Particularidades das Empresas Estatais em Ambiente Concorrencial Nas empresas públicas e sociedades de economia mista que explorem atividade econômica em regime de concorrência, a análise da publicidade de dados pessoais e funcionais deve considerar não apenas os direitos à privacidade e proteção de dados pessoais, mas também a proteção de informações estratégicas, negociais, comerciais e empresariais. Nesses casos, determinados dados funcionais aparentemente relacionados ao exercício profissional podem revelar estruturas organizacionais, cadeias de comando, projetos estratégicos, áreas de negócio, capacidades técnicas, posicionamentos competitivos ou informações protegidas por normas específicas aplicáveis à atividade econômica desenvolvida pela estatal. A avaliação da publicidade deve considerar o contexto institucional da entidade e os riscos concretos decorrentes da divulgação para a competitividade empresarial, a governança corporativa, a segurança institucional e a preservação do interesse público associado à atividade econômica desempenhada. Como prática, nesses casos: • ocultar siglas completas; • ocultar descrições detalhadas de função; • não divulgar livremente contatos individuais. Sigilo Empresarial em Empresas Estatais Nas empresas estatais que explorem atividade econômica, devem ser observadas também as hipóteses de proteção decorrentes do sigilo empresarial, comercial, estratégico, concorrencial e negocial previsto na

Pág.	Trecho referido no documento	Comentário
		legislação específica e nos regimes regulatórios aplicáveis, inclusive quando tais informações não se enquadrem estritamente como segredo industrial. Avaliação de Riscos à Segurança Institucional e Competitividade Deve-se avaliar se a divulgação da informação poderá gerar riscos relevantes à segurança institucional, à atividade regulada, à competitividade empresarial da organização ou à proteção de estratégias negociais e comerciais legitimamente resguardadas pelo ordenamento jurídico. Dados de Contato Corporativo A divulgação de dados de contato corporativo deve observar a existência de canais institucionais de atendimento ao público. Quando a divulgação de e-mails individuais, telefones funcionais ou ramais puder comprometer a continuidade das atividades, gerar sobrecarga operacional ou substituir indevidamente os canais oficiais de relacionamento com a sociedade, poderá ser adotada a divulgação apenas dos canais institucionais da organização. Dados pessoas do assento funcional de empregado e funcionários públicos Arts. 18 e 19, da LGPD, abordam acesso à informação, sendo o ponto de contato mais direto entre as leis em análise. Considerando esses artigos da LGPD, segundo os quais o objeto do direito é o acesso aos dados pessoais tratados, e não aos documentos administrativos em si considerados, a LGPD não deve ser interpretada como canal para solicitação de documentos pessoais, especialmente para empresas e órgãos estatais. Usar o canal de LGPD como caminho para buscar documentos e não informações sobre tratamento de dados pessoais, mesmo quando há relatos de atendimentos de primeira instância, pode desviar os esforços deste canal especializado para temas cotidianos de gestão de pessoas. Interpretando sistematicamente os arts. 18 e 19 da LGPD, conclui-se pela falta de previsão legal a impor reconstrução de arquivos históricos, produção de documentos inéditos, consolidação manual de informações dispersas, pesquisa ilimitada em acervos físicos e restauração de registros regularmente eliminados. Portanto, quando não for possível satisfazer integralmente o requerimento, a resposta poderá indicar, de forma motivada e transparente, as razões que obstam o atendimento integral do pedido, nos termos do art. 18, § 4º, da LGPD.

1.

Pág.	Trecho referido no documento	Comentário Petrobras
32	Seção Dados pessoais de agentes públicos	Sugere-se fazer distinção para os empregados públicos, não conferindo o mesmo tratamento atribuído aos servidores públicos de regime estatutário regidos pela Lei 8112/90.
34	Seção Dados pessoais em processos administrativos disciplinares	Sugere-se fazer distinção para os empregados públicos, não conferindo o mesmo tratamento atribuído aos servidores públicos de regime estatutário regidos pela Lei 8112/90.
34	Mesmo trecho sobre PADs	Com o objetivo de diferenciar dos procedimentos disciplinares de empregados públicos que são disponibilizados apenas ao próprio empregado que foi investigado, sugerimos a seguinte redação: ‘Em tese, são públicos os procedimentos administrativos disciplinares regidos pela Lei nº 8.112/1990
35	Tabela de divulgação de informações em PAD	Especificar que os dados contidos nessa tabela se referem a PAD regido pela Lei nº 8.112/90.

Consulta Pública - Guia de Transparência e Proteção de Dados Pessoais

São Paulo, 24 de julho de 2026

À Controladoria-Geral da União (CGU) e a Agência Nacional de Proteção de Dados (ANPD)

Assunto: CONTRIBUIÇÃO DA DATA PRIVACY BRASIL À CONSULTA PÚBLICA DO GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

Capítulo 3

1. Incorporação da proteção de dados para além da proteção à privacidade

O Capítulo 3 do Guia trata das hipóteses de acesso por terceiros a informações pessoais protegidas, buscando orientar órgãos e entidades públicas na compatibilização entre a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD).

No entanto, **recomenda-se que o Capítulo 3 seja aprimorado para evitar uma leitura restritiva da proteção de dados pessoais**, muitas vezes apresentada como equivalente à proteção da privacidade ou ao sigilo da informação. Essa aproximação aparece em diferentes trechos do Guia e pode produzir uma compreensão limitada da LGPD, como se sua principal função fosse impedir a circulação de dados pessoais.

A título de exemplo, o Guia afirma:

“Como já mencionado, a LAI e a LGPD compatibilizam os direitos fundamentais **de acesso à informação e de proteção da privacidade**. É a LAI que estabelece as hipóteses de restrição de acesso a informações pessoais para o poder público, e não a LGPD, conforme previsto no Enunciado CGU nº 4, de 10 de março de 2022.” p.16 do guia.

[...]



“A hipótese de divulgação de dados pessoais para atendimento ao interesse público e geral preponderante exige análise cuidadosa por parte do órgão público. É fundamental realizar a **ponderação caso a caso entre o direito de acesso à informação e a proteção da privacidade do indivíduo.**” P. 16

Embora o trecho esteja correto ao reconhecer a especialidade da LAI na definição das hipóteses de restrição de acesso a informações pessoais pelo Poder Público, recomenda-se que a redação seja ajustada para não reduzir a LGPD à proteção da privacidade. A proteção de dados pessoais é um direito fundamental autônomo e possui escopo mais amplo. Ela não se limita à preservação de uma esfera privada contra a exposição pública, mas regula o modo como dados pessoais são coletados, utilizados, compartilhados, divulgados, armazenados e tratados, inclusive quando esses dados circulam em contextos de interesse público.

Ainda que a LAI seja uma norma especial que rege os pedidos de acesso à informação, consolidado inclusive no Enunciado CGU nº 4/2022, não significa que sua interpretação deve ser mantida a mesma desde 2011. A LGPD, além de lei posterior, instituiu o regime geral do tratamento de dados pessoais no Brasil expressamente aplicável ao Poder Público (arts. 23 e seguintes), e fixou fundamentos e princípios – autodeterminação informativa, finalidade, necessidade, prevenção, responsabilização – que conformam toda operação de tratamento, inclusive aquelas realizadas em cumprimento à LAI.

O fato de ser uma lei especial não garante imunidade hermenêutica diante da nova ordem normativa. Nesse sentido, **o guia não deve apenas replicar o art. 31 da LAI – e sim trazer uma integração efetiva compatível com os princípios, finalidades e dogmática da proteção de dados pessoais.** Esse é o esforço proposto pelo próprio enunciado supracitado ao afirmar a compatibilidade sistemática entre LAI, Lei de Governo Digital e LGPD: trata-se de uma interpretação integrada, não a aplicação isolada da lei de 2011.

Mais do que a sucessão de leis no tempo, destaca-se o caráter constitucional tanto da transparência pública, quanto da proteção de dados. **A elevação da proteção de dados ao artigo 5º da Constituição impõe um novo filtro hermenêutico.** Agora, toda e qualquer aplicação da LAI que envolva dados pessoais de um indivíduo deve, obrigatoriamente, ser ponderada com os fundamentos e princípios da proteção de dados.



A LAI, como toda legislação infraconstitucional, deve ser interpretada conforme a Constituição vigente, e não conforme o quadro normativo de sua edição. Assim, **o conceito de dado pessoal previsto no artigo 31 não pode ser interpretado sob a égide da intimidade e vida privada, categorias do texto de 2011, devendo incorporar as dimensões próprias do direito fundamental à proteção de dados**: parâmetros de justiça e salvaguardas nos fluxos de informações pessoais, o mapeamento e mitigação de riscos decorrentes do tratamento e a garantia da promoção de direitos fundamentais dos titulares de dados.

O caminho reverso de interpretação implica em uma sobrevalorização dos conceitos de intimidade e vida íntima que foram requalificados no julgamento da ADI 6387-STF e o sentido do direito fundamental à proteção de dados pessoais. Na interpretação constitucional do Supremo Tribunal Federal sobre a natureza jurídica da proteção de dados pessoais, ela é vista como vinculada às cláusulas assecuratórias das liberdades e da dignidade da pessoa humana.

A interpretação harmônica entre os dois regimes exige compreender que a LGPD oferece critérios para qualificar o tratamento de dados pessoais realizado no âmbito da transparência pública. **Quando a divulgação de informações pessoais observa os princípios da lei como a necessidade, proporcionalidade, transparência, segurança, prevenção e responsabilização e se ampara adequadamente em uma das bases legais, a abertura de dados contribui para a concretização da LGPD.**

Muito embora a proteção da privacidade seja um dos princípios da LGPD e esteja incluída na proteção de dados, ela não é o seu elemento central ou definidor. Proteção de dados está para além da proteção da informação de um determinada pessoa em relação à esfera pública, mas sobre como o uso desses dados ocorre sendo eles públicos ou privados.

A formulação poderia ser aperfeiçoada para **substituir a referência à “proteção da privacidade” pela referência expressa à “proteção de dados pessoais”**. Isso porque a ponderação exigida nesses casos envolve a análise mais ampla dos riscos decorrentes do fluxo de dados pessoais: quem acessará a informação, para qual finalidade, em que contexto, com quais possibilidades de reutilização, com quais impactos sobre o titular e com quais salvaguardas.



A proteção de dados pessoais está relacionada à proteção da pessoa diante dos efeitos do tratamento de seus dados. Por isso, abrange dimensões como autodeterminação informativa, liberdade, igualdade, prevenção de riscos, não discriminação, segurança, transparência e responsabilização.

Nesse sentido, recomenda-se que o Guia evite construir a relação entre LAI e LGPD como uma oposição entre acesso à informação e privacidade. **Quando a LGPD é entendida apenas como uma lei de proteção à privacidade, ela parece ocupar o lugar de obstáculo à transparência.** No entanto, quando compreendida como um regime amplo de regulação dos fluxos de dados pessoais, ela permite aprimorar a própria abertura de dados públicos, oferecendo critérios para que a transparência seja realizada de forma legítima, segura e orientada ao interesse público.

2. Consentimento e bases legais

Outro ponto que merece aprimoramento diz respeito ao uso do consentimento como fundamento para o acesso por terceiros a informações pessoais protegidas. O Capítulo 3 do Guia apresenta a hipótese de fornecimento da informação mediante consentimento expresso do titular, indicando que esse consentimento deve ser expresso e documentado. Também menciona que, nos casos de falecimento ou ausência do titular, o consentimento poderia ser obtido junto ao cônjuge, companheiro, descendentes ou ascendentes.

Diante da centralidade que o guia traz à base legal do consentimento, é preciso situar o lugar que ele ocupa na arquitetura da LGPD.

A LGPD acompanhou um movimento mais amplo de **descentralização do consentimento na regulação da proteção de dados pessoais**. Como demonstra Bruno Bioni¹, o modelo regulatório estruturado exclusivamente sobre o binômio notificação-consentimento revelou-se insuficiente para assegurar a autodeterminação informativa: ele sobrecarrega o titular com decisões que este não tem condições reais de compreender e avaliar, ao mesmo tempo em que desonera as organizações de responsabilidade sobre os fluxos de dados que promovem.

¹ BIONI, Bruno. Proteção de Dados Pessoais: a função e os limites do consentimento. 2 ed. 2020. Editora Forense.



Por conta desse cenário, a LGPD não conferiu ao consentimento posição hierarquicamente superior: ele é apenas uma entre as dez bases legais do art. 7º, sem qualquer preponderância ou preferência sobre as demais.

Esse rol de hipóteses legitimam o tratamento de dados independentemente de autorização expressa do titular. Isso confere segurança jurídica a atividades essenciais para a sociedade e para a execução de serviços, inclusive perante o poder público em atividades de transparência.

Essa mudança tem consequência direta para o Guia: ao tratar o consentimento como via preferencial de acesso por terceiros a informações pessoais protegidas, o documento adota uma premissa que a própria LGPD superou. Além disso, os requisitos de validade do consentimento na LGPD precisam ser considerados na sua articulação com a LAI, e eles podem não ser viáveis em muitas das situações que o Guia pretende disciplinar.

No molde jurídico atual da LGPD, o consentimento precisa ser “livre”, “informado”, “inequívoco” e “específico”. **Livre** pois a sua escolha não pode advir de consequências negativas ou positivas da cessão de dados pessoais além de poder revogar seu consentimento a qualquer momento; **informado** pois é preciso que o titular tenha informações suficientes claras para se decidir sobre a concessão de seu consentimento; **inequívoco** pois é preciso que a cessão dos dados ocorra a partir de uma manifestação de vontade do titular para uma finalidade determinada. Sendo vedada a obtenção do consentimento por uma inação ou omissão do titular; **específico ou expresso**, pois em alguns casos é preciso que certas formas de tratamento de dados tenham uma camada maior de proteção e ofereçam maior oportunidade de ponderação do titular.

Todo esse processo de adjetivação serve para privilegiar o **consentimento enquanto um processo de tomada de decisão**², para além de um momento estático de aceite ou recusa da concessão de dados pessoais. Contudo, o que precisamos observar é que a adjetivação cria obrigações para os agentes de tratamento, deslocando parte da responsabilidade pelo fluxo de dados que antes estava exclusivamente com o titular. Para além de todos esses

² BIONI, Bruno; LUCIANO, Maria. **O CONSENTIMENTO COMO PROCESSO: EM BUSCA DO CONSENTIMENTO VÁLIDO**. In Tratado de Proteção de Dados Pessoais. Rio de Janeiro Forense Editora, 2021.

requisitos, **o consentimento precisa ser revogável e reversível em relação ao tratamento de dados pessoais.**

Nesse sentido, a orientação do guia de que o consentimento expresso do titular de um dado permite a sua divulgação para terceiros parece irrazoável e até inválida. Primeiro, pois o guia dá a entender que basta um consentimento expresso para garantir o acesso, deixando de lado todos os demais requisitos do consentimento. O segundo elemento está na liberdade desse consentimento. Afinal, o consentimento nestes casos parece não ser reversível. Isto pois na medida em que um titular consinta para a divulgação desses dados, ainda que ele solicite que a divulgação de seus dados seja interrompida, os efeitos produzidos pela sua abertura como o acesso e cópia desses dados para diferentes fontes e usos, não é reversível, razão pela qual esse consentimento pode não ser verdadeiramente livre. Além disso, pode ser que tal situação possa ser entendida como uma limitação relevante da sua autodeterminação informativa ao não ser possível ter um controle mais adequado do seu fluxo de dados pessoais a partir do momento em que tal sujeito consentir com essa divulgação.

O uso do consentimento nestes casos também cria um ruído operacional que pode pôr em risco ou ao menos tensionar as obrigações de abertura de dados públicos com interesse público. Isto pois a necessidade de um consentimento para publicização de dados pessoais pode impedir o acesso a dados que têm interesse público ao mesmo tempo que irá exigir dos responsáveis pelas respostas de pedido de LAI uma análise de interesse público, dificultando ainda mais a consecução de objetivos da Lei de Acesso à Informação.

A situação se agrava no caso de falecimento do titular pois cria uma fricção operacional na medida em que caso familiares não estejam disponíveis ou negarem esse consentimento, o acesso à informação de dados com interesse público pode ficar dificultado. Lembrando que no caso de falecimento, as disposições da LGPD não se aplicam pois o caráter pessoal do dado deixa de existir com o falecimento do titular.³

A centralidade que o consentimento assume no Capítulo 3 e no roteiro de tomada de decisão do Capítulo 4 pode induzir órgãos e entidades a criarem mecanismos de concordância ou recusa de abertura de dados pessoais - tanto para cidadãos quanto

³AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (Brasil). **Nota Técnica nº 3/2023/CGF/ANPD**. Assunto: Memorial no Portal Web da Polícia Rodoviária Federal. Processo nº 00261.002079/2022-56. Brasília, DF: ANPD, 2023.

servidores públicos. Ainda que a princípio possa ser considerada uma medida para dar maior transparência ao tratamento de dados, a institucionalização da consulta ao titular produz dois efeitos negativos.

O primeiro é a incorporação de uma lógica privatista em uma esfera que deveria ser regida pelo interesse público: a divulgação de informações custodiadas ou coletadas pelo Estado passa a ser uma transação entre indivíduo e administração pública, dependente de autorização prévia. O regime da LAI, no entanto, é estruturado sobre a publicidade enquanto preceito geral e princípios como prestação de contas e controle social

Informações relacionadas ao exercício de função pública ou à aplicação de recursos públicos não são objeto de disposição individual do titular. Uma pessoa que venha a realizar contratos com a administração pública não pode optar por limitar certas informações: é papel do órgão identificar potenciais excessos e, mediante justificção, indicar o que pode ser retirado do controle social. Condicionar a divulgação de dados ao consentimento inverte a premissa constitucional do regime de acesso.

Isso se relaciona a um segundo efeito: a criação de uma falsa expectativa de sigilo. Ao ser consultado sobre a divulgação de seus dados, o titular razoavelmente supõe que sua recusa impedirá a abertura. No entanto, como o próprio Guia reconhece, há diversas hipóteses que prescindem do consentimento — previsão legal específica, pesquisas e estatísticas, ordem judicial, defesa de direitos humanos, recuperação de fatos históricos e, sobretudo, o interesse público e geral preponderante.

Isso significa que os dados de um titular que negou consentimento poderão, ainda assim, serem divulgados de forma lícita.

Um consentimento cuja recusa não vincula a decisão é fictício: não é livre, porque não há qualquer consequência real, e não cumpre função protetiva. Seu resultado é minar a confiança do titular na Administração, alimentar contenciosos administrativos e judiciais de quem se sentir enganado pela divulgação posterior e transferir ao servidor responsável o ônus de explicar por que a manifestação colhida foi desconsiderada.

Assim, a consulta ao titular gera mais problemas do que resolve. Recomenda-se, portanto, que o roteiro do Capítulo 4 seja ajustado para que o consentimento não figure como etapa



central do fluxo decisório, mas como hipótese residual, aplicável aos casos em que a divulgação efetivamente dependa da vontade do titular.

3. Proteção de dados pessoais prevista na LAI

A hipótese de interesse público geral e preponderante é justamente o ponto em que a leitura integrada entre LAI e LGPD se mostra mais necessária. Não é preciso escolher entre transparência pública e proteção de dados pessoais, mas estabelecer as condições pelas quais a transparência poderá ocorrer em consonância com a proteção de dados.

A LAI fornece o regime de acesso à informação e estabelece a publicidade como regra e o sigilo como exceção. A LGPD, por sua vez, oferece critérios para que os fluxos de dados pessoais decorrentes da transparência sejam adequados, seguros, proporcionais e orientados a finalidades legítimas. Em alguns momentos o Guia assume a postura de que para dar acesso à informação é preciso flexibilizar a proteção de dados

O Enunciado CGU no 12/2023 estabelece que a proteção de dados pessoais deve ser compatibilizada com o direito de acesso à informação, podendo ser flexibilizada quando, na situação concreta, prevalecer o interesse público geral e preponderante.

Dessa forma, recomendamos que a abertura de informações pessoais de interesse público seja lida como uma operação de tratamento que deve observar os princípios e deveres da LGPD.

Essa interpretação também evita a falsa oposição entre os dois regimes legais. Se a proteção de dados for compreendida apenas como privacidade ou sigilo dos dados, e a transparência como abertura de acordo com o interesse público preponderante, a relação entre LAI e LGPD parecerá inevitavelmente conflitiva. No entanto, se a proteção de dados for compreendida como governança dos fluxos de dados pessoais, a abertura e a restrição de informações passam a ser analisadas a partir de uma mesma pergunta: qual tratamento é adequado, necessário, proporcional e justificável diante do interesse público e dos direitos dos titulares?



A discussão do Capítulo 3 deve ser conectada ao Capítulo 4 do Guia, especialmente à proposta de transparência por desenho e à necessidade de instrumentos prévios de ponderação. Se o Capítulo 3 indica as hipóteses de acesso por terceiros a dados pessoais protegidos, o Capítulo 4 deve oferecer o método para que essas hipóteses sejam aplicadas de forma consistente.

A análise do interesse público geral e preponderante não deve depender exclusivamente da percepção individual do servidor responsável pela resposta ao pedido de LAI. Sem uma metodologia institucional, a ponderação tende a variar conforme a sensibilidade de cada servidor ou conforme a cultura interna de cada órgão. Isso pode produzir decisões inconsistentes, ora excessivamente restritivas, ora excessivamente permissivas.

Nesse sentido, recomenda-se que o Guia estimule o uso do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como instrumento especialmente adequado para estruturar, de forma prévia e documentada, a ponderação entre transparência pública e proteção de dados pessoais. O RIPD pode permitir que o órgão público identifique categorias recorrentes de pedidos de acesso, mapeie dados pessoais envolvidos, avalie o valor público da divulgação, identifique riscos aos titulares, define medidas de mitigação e estabeleça parâmetros para decisões futuras. Esta sugestão será melhor elaborada na seção seguinte, destinada ao capítulo 4 do guia.

Essa abordagem permite que a análise do Capítulo 3 seja operacionalizada por meio de uma metodologia institucional, sem a necessidade de que se de refaça integralmente a ponderação a cada pedido, o órgão passa a contar com critérios previamente documentados, sem afastar a necessidade de análise individualizada em casos novos, sensíveis ou atípicos. O resultado pode levar a uma tomada de decisão mais segura, eficiente, motivada e sujeita a controle social.

Capítulo 4. Garantindo a transparência pública com proteção dos dados pessoais

RIPD como mecanismo prévio para o balanceamento da transparência pública e respeito à proteção de dados



Recomenda-se que o Guia inclua o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como instrumento especialmente adequado para apoiar, de forma prévia e estruturada, a ponderação entre transparência pública e proteção de dados pessoais.

Nos termos da LGPD, o RIPD consiste na documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas, salvaguardas e mecanismos de mitigação de risco. Além disso, a própria LGPD prevê que a ANPD poderá solicitar ao controlador a elaboração de RIPD, inclusive quando o tratamento tiver como fundamento o legítimo interesse.

O RIPD também é uma importante ferramenta de prestação de contas (*accountability*) em observação ao princípio previsto no artigo 6º, X da LGPD. Nesse sentido, a documentação pode demonstrar que o controlador avaliou sua cadeia de tratamento de dados, adotando medidas para proteger os direitos dos titulares. Esse entendimento também foi publicado no Enunciado 679 da IX Jornada de Direito Civil:

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser entendido como uma medida de prevenção e de *accountability* para qualquer operação de tratamento de dados considerada de “alto risco”, tendo sempre como parâmetro o risco aos direitos dos titulares.

No contexto do Poder Público, esse instrumento pode cumprir papel relevante para tornar mais transparente, documentada e justificável a tomada de decisão sobre a disponibilização de dados pessoais em iniciativas de transparência ativa, transparência passiva e abertura de dados. A decisão de divulgar ou restringir um dado pessoal em resposta a um pedido de acesso à informação é um juízo de ponderação: de um lado, o direito de acesso e o interesse público na transparência; de outro, a intimidade, a vida privada e a proteção de dados do titular. O Guia CGU-ANPD coloca essa ponderação como o último filtro do seu roteiro



decisório — a aferição do interesse público e geral preponderante — e exige que ela resulte numa decisão concreta, motivada e registrada. A presente contribuição vai no sentido de que, sem um método que a estruture, essa ponderação tende a variar conforme a sensibilidade de cada servidor.

O RIPD é o instrumento privilegiado para essa tarefa por dois motivos. O primeiro é normativo: a LGPD o define como o documento destinado a descrever os processos de tratamento que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas para mitigá-los. O segundo é institucional: a própria ANPD, no caso da retirada de microdados do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep)⁴, determinou que o instituto elaborasse um RIPD para avaliar a amplitude adequada da divulgação de dados pessoais, consolidando o relatório como o vetor por meio do qual o órgão público analisa riscos, adota salvaguardas e presta contas. O RIPD, porém, é um procedimento de documentação e governança que depende de uma metodologia para tornar os riscos efetivamente visíveis e as medidas de mitigação executáveis.

Nesse sentido, propõe-se a incorporação da metodologia de custo-benefício (explicada adiante) na tomada de decisão para respostas a pedidos de LAI. Tratando-se de disponibilização de dados de interesse público, ela permite avaliar antecipadamente, de um lado, o valor da abertura — o benefício esperado para a coletividade — e, de outro, o risco aos titulares, já considerando o efeito das medidas de mitigação. A partir dessa avaliação conjunta, o órgão decide entre ampliar os benefícios, reduzir os riscos ou rever a divulgação, caso verifique-se que os riscos são maiores que o valor público de sua

⁴ Veja mais em:

<https://www.dataprivacybr.org/documentos/relatorio-workshop-lgpd-e-microdados-avancando-em-metodologias-para-avaliar-riscos-e-garantir-a-transparencia/>

divulgação. Incorporada ao RIPD, essa metodologia faz o relatório deixar de ser um inventário de riscos e passar a ser um instrumento de decisão.

A proposta reverbera com a premissa de transparência por desenho do Guia, a qual recomenda antecipar, desde a concepção de processos e sistemas, o que pode ser divulgado, com qual detalhamento e suas salvaguardas. Sob a dogmática da proteção de dados pessoais, o RIPD é o veículo concreto dessa antecipação. Ao mapear as categorias de dados que o órgão trata com regularidade, o valor público de cada uma e o risco de sua abertura, o relatório pode incluir a análise das situações comuns de transparência passiva, resolvendo de antemão a equação entre interesse público da divulgação e respeito aos direitos dos titulares.

A partir desse esforço prévio, há um efeito prático que reverbera com o princípio da eficiência na administração pública: ao de refazer integralmente a ponderação a cada pedido, servidores e servidoras podem aplicar os critérios já estabelecidos no RIPD do órgão. Depois da triagem jurídica — os primeiros passos do roteiro do Guia, que verificam se o dado é de terceiro, se é protegido pelo art. 31 da LAI, se há consentimento ou hipótese legal de acesso —, recorre-se ao catálogo de benefícios à coletividade como medida do valor (uso adequado do dinheiro público, fiscalização de agentes, integridade de processos, controle social) e à régua da expectativa de privacidade segundo a proximidade do titular com o Estado como medida do risco. Sobre esses dois eixos aplica-se a fórmula da probabilidade de ocorrência pelo impacto da abertura, já incorporando as medidas que o RIPD definiu. Assim, parâmetros quantificáveis e justificáveis já estabelecidos, baseados em premissas da LGPD, passam a nortear as decisões de transparência passiva.

Assim, o RIPD reduz o universo de situações em que o servidor precisa conduzir a ponderação completa, reservando o esforço analítico aprofundado para os casos novos ou

atípicos, não para os que já foram enfrentados e padronizados. Por ser um documento vivo, atualizado a cada novo processo ou adoção de tecnologias, sua atualização permite incorporar novas demandas que sejam levadas ao órgão. Além disso, sua disponibilização pública — recomendação da própria ANPD no caso Inep — reforça o compromisso com a transparência e controle social dos critérios estabelecidos.

Ao incorporar o RIPD enquanto critério anterior e necessário à ponderação do interesse público preponderante, o ganho final é uma fundamentação averiguável. A resposta do pedido de LAI passa a ser uma metodologia documentada no RIPD do órgão, permitindo que cada passo seja refeito e avaliado. É exatamente o que o Guia exige ao pedir decisões motivadas e registradas, e o que a LGPD persegue com o princípio da responsabilização e prestação de contas. A metodologia não substitui o juízo do servidor nem a responsabilidade institucional do órgão, mas oferece uma estrutura replicável, escalável e auditável para sustentar, com critérios, o equilíbrio entre proteção de dados pessoais e transparência pública.

Nesse sentido, a Data Privacy Brasil recomenda que o Guia estimule a utilização da metodologia de análise de custo-benefício da disponibilização de dados públicos para situações que envolvam a publicização de dados pessoais de interesse público. Essa abordagem permite avaliar previamente a presença de interesse público, por meio da identificação dos benefícios esperados com a divulgação de determinados dados, e os riscos de dano aos titulares, considerando também as medidas de mitigação disponíveis, como análise da necessidade e minimização de dados e identificação de meios alternativos menos invasivos, e seus efeitos sobre a utilidade pública da informação.

A metodologia de custo-benefício é uma proposta voltada a enfrentar o dilema da construção de soluções de aumento de transparência pelo Estado em harmonia com a Lei



Geral de Proteção de Dados. Ela busca orientar a tomada de decisão em programas de dados abertos e em outras iniciativas de abertura ou disponibilização de dados pelo Estado brasileiro, permitindo que a decisão sobre divulgar tais dados seja tomada de forma documentada, proporcional e orientada ao interesse público.

Neste sentido, a proposta já está alinhada com o Guia, tanto em objetivos, quanto nas etapas propostas. Entretanto, ela vai além, reforçando a *accountability* do processo decisório para garantir sua segurança e legitimidade.

De forma geral, a metodologia pode ser estruturada em seis etapas.

A primeira etapa consiste na definição do tratamento de dados voltado à disponibilização de dados pessoais. Nesse momento, o órgão deve descrever quais dados pretende disponibilizar. Também devem ser indicados a finalidade da divulgação, o contexto institucional da iniciativa e os fundamentos jurídicos que autorizam ou justificam a disponibilização.

Correspondência com o Guia: A qualificação dos dados prevista nesta etapa pode englobar a análise indicada no Guia no *Roteiro de tomada de decisão* (passos 1 a 4) e se assemelha ao passo 1 do *Teste de Interesse Público*.

Adição da Data: Nesta etapa, há também a identificação da finalidade da divulgação (princípio da LGPD) e a justificativa e fundamentos jurídicos foram inseridos para que exista o registro e comprovação do atingimento da finalidade pública do tratamento de dados pessoais (art. 23, da LGPD).

A segunda etapa envolve a análise do valor e do risco iniciais. O valor corresponde aos benefícios esperados da disponibilização dos dados. Essa análise deve indicar não apenas qual benefício é esperado, mas também o quanto públicos poderão se beneficiar da abertura, como cidadãos, jornalistas, pesquisadores, organizações da sociedade civil ou

órgãos de controle. O risco, por sua vez, corresponde às possíveis consequências negativas para os titulares, envolvendo as possibilidades de poder se realizar e a gravidade de seus impactos para os titulares de dados.

Correspondência com o Guia: esta etapa é completamente alinhada com os passos 2 e 3 do *Teste de Interesse Público*.

A terceira etapa consiste na definição do grau de custo-benefício inicial. Para isso, compara-se o valor público esperado com os riscos identificados. Quando o valor supera o risco, a disponibilização tende a ser justificável. Quando valor e risco estão em equilíbrio, a abertura exige cautela e deve ser acompanhada de salvaguardas para diminuição dos riscos. Quando o risco supera o valor, a disponibilização deve ser revista antes de qualquer decisão de abertura.

Correspondência com o Guia: esta etapa é alinhada com o passo 4 do *Teste de Interesse Público*.

A quarta etapa corresponde à adoção de medidas de mitigação. Essas medidas devem ser escolhidas de acordo com os riscos identificados. O objetivo é reduzir os riscos sem eliminar o valor público da disponibilização. Caso a medida de mitigação reduza excessivamente a utilidade da base, devem ser avaliadas formas de preservar ou promover o valor da divulgação sem reintroduzir riscos desnecessários.

Correspondência com o Guia: esta etapa está alinhada com o passo 5 do *Teste de Interesse Público*.



A quinta etapa consiste na definição do custo-benefício residual. Após a adoção das medidas de mitigação, o órgão deve reavaliar o cenário para verificar quais riscos permanecem e qual valor público ainda subsiste. Essa etapa é essencial porque uma medida pode reduzir riscos, mas também diminuir a utilidade dos dados para transparência. O objetivo é identificar se, após as salvaguardas, ainda existe uma relação proporcional entre o valor da abertura e os riscos remanescentes.

Correspondência com o Guia: esta etapa está em linha com os passos 2 a 4 do *Teste de Interesse Público* e o item 4.3 (*Transparência por desenho*).

Adição da Data: esta etapa amplia o Guia por propor uma revisão da análise feita a fim de verificar se as medidas de mitigação de riscos impactaram os benefícios previstos e, conseqüentemente, a utilidade da publicação. Também indica a possibilidade de se pensar em medidas que favoreçam a transparência, isto é, ampliando sua acessibilidade para o público destinatário. Estas são formas de garantir a ponderação adequada, com o menor prejuízo ao interesse público e aos titulares.

Por fim, a sexta etapa corresponde à decisão sobre a disponibilização dos dados. A partir do custo-benefício residual, o órgão poderá decidir pela divulgação ou não disponibilização dos dados. Em qualquer hipótese, a decisão deve ser justificada de forma clara. A metodologia não substitui a responsabilidade decisória do órgão, mas qualifica e documenta a ponderação entre transparência pública e proteção de dados pessoais.

Correspondência com o Guia: esta etapa está completamente alinhada com o passo 6 do *Teste de Interesse Público* e o item 4.3 (*Transparência por desenho*).

Adição da Data: Esta é a etapa em que alcança-se o resultado sobre o custo-benefício da



disponibilização e consequentemente quando o órgão tomará sua decisão. Em todas as etapas da metodologia proposta é solicitado registro e justificativa dos passos e conclusões alcançadas em cada um deles, pretendendo que seja inserida no RIPD, como forma de garantir a *accountability* de todo o processo decisório.

Essa metodologia é especialmente relevante pois decisões mais qualificadas, capazes de preservar o valor público da informação e, simultaneamente, reduzir riscos desnecessários ou desproporcionais aos direitos dos titulares. No caso dos servidores responsáveis por responder pedidos de acesso à informação, o RIPD pode ser utilizado de forma preventiva pelo órgão ou entidade pública para mapear situações recorrentes de transparência passiva que envolvam dados pessoais. Assim, o órgão pode analisar previamente quais tipos de informações costumam ser solicitadas, quais dados pessoais estão envolvidos, qual interesse público justifica a divulgação, quais riscos podem decorrer do acesso e quais medidas de mitigação devem ser adotadas em cada hipótese.

Dessa forma, o RIPD, combinado a uma metodologia de custo-benefício, pode reduzir o escopo de situações em que o servidor responsável por pedidos de LAI precisará realizar a ponderação entre direito de acesso à informação e proteção de dados pessoais. Em vez de transferir integralmente essa responsabilidade ao servidor no momento da resposta ao pedido, o órgão passa a contar com orientações institucionais previamente documentadas e específicas, baseadas em análise de riscos, benefícios e medidas de mitigação.

Além disso, **recomenda-se que o Guia destaque que o RIPD deve ser compreendido como documento vivo, sujeito a revisão e atualização periódica.** Novas demandas de acesso à informação, novos entendimentos regulatórios, mudanças tecnológicas, alterações nas bases de dados, incidentes de segurança ou identificação de riscos antes não previstos podem justificar a atualização do relatório. Essa característica permite que o RIPD acompanhe a evolução das práticas de transparência do órgão e incorpore, ao longo do

tempo, novas situações comuns de ponderação entre interesse público e direitos dos titulares de dados pessoais.

No documento anexo a esta contribuição, a Data Privacy Brasil detalha o processo da metodologia de custo-benefício, bem como sua construção a partir da análise de diferentes iniciativas nacionais e internacionais de metodologias de avaliação de riscos. Recomenda-se, portanto, que o Guia reconheça a importância de instrumentos metodológicos desse tipo para apoiar órgãos e entidades públicas na construção de práticas de transparência compatíveis com a proteção de dados pessoais.

Por fim, para que os princípios da transparência e da responsabilização e prestação de contas se materialize de forma concreta, é fundamental que, independentemente do formato, o instrumento utilizado para a realizar a ponderação entre direito de acesso à informação de interesse coletivo e proteção à privacidade seja tornado público, para que não só eventuais solicitantes, mas toda comunidade jurídica e cidadãos possam compreender a ponderação realizada e, a partir disso, fomentar um modelo de co-regulação em rede na construção de melhores práticas da ponderação entre esses direitos. Esse entendimento também é compartilhado pela ANPD em seus processos de fiscalização: no caso dos Microdados do Inep (Nota Técnica nº 46/2022/CGF/ANPD), cadastro e tratamento de dados de crianças e adolescentes no TikTok (Nota Técnica nº 6/2023/CGF/ANPD), o uso de dados pessoais para treinamento de inteligência artificial da Meta AI, (Voto nº 11/2024/DIR-MW/CD), a agência exigiu a apresentação de RIPD e uma versão pública da documentação para tornar possível o controle social das escolhas feitas por esses agentes de tratamento sobre o sopesamento de riscos do tratamento de dados.



METODOLOGIAS DE CUSTO-BENEFÍCIO PARA ABERTURA DE DADOS: COMPATIBILIZANDO TRANSPARÊNCIA E PROTEÇÃO DE DADOS

Gabriela Vergili, Pedro Bastos Lobo Martins,
Pedro Henrique Martins dos Santos e Pedro Saliba

Junho de 2026



FICHA TÉCNICA

Autoria

Gabriela Vergili
Pedro Bastos Lobo Martins
Pedro Henrique Martins dos Santos
Pedro Saliba

Diagramação e Design

Bárbara Yamasaki

Como citar

VERGILI, Gabriela; MARTINS, Pedro; SANTOS, Pedro Henrique; SALIBA, Pedro. Metodologias de custo-benefício para abertura de dados: compatibilizando transparência e proteção de dados. São Paulo: Data Privacy Brasil, 2026.

A **Data Privacy Brasil** é uma organização de ensino, pesquisa e incidência que produz conhecimento e forma pessoas para um ecossistema informacional justo. Por meio da educação, construção de saberes e mobilização da sociedade, buscamos uma sociedade democrática na qual as tecnologias estejam a serviço da autonomia, dignidade das pessoas e redução de assimetrias de poder.

Direção

Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordenação

Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Equipe

Ana Luiza Serafini, Bárbara Yamasaki, Bianca Marques, Eduardo Mendonça, Gabriela Vergili, Gabriel Franco, Giovanna Amaral, Giovana Andrade, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Luize Ribeiro, Matheus Arcanjo, Natasha Nóvoa, Paula Uematsu, Pedro Henrique Santos, Rafael Guimarães, Rodolfo Rodrigues e Vanessa Nobre.

Licença

Creative Commons
É livre a utilização, circulação, ampliação e produção de documentos derivados desde que citada a fonte original e para finalidades não comerciais.

Imprensa

Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacy.br.org

SUMÁRIO EXECUTIVO

Este relatório se dedica a analisar metodologias de avaliação de risco que melhor compatibilizem a relação entre transparência e proteção de dados pessoais no atendimento de obrigações decorrentes da Lei de Acesso à Informação (Lei nº 12.527/2011) e de execução de políticas de abertura de dados.

A análise de literatura científica, decisões administrativas da Autoridade Nacional de Proteção de Dados (ANPD) e Controladoria-Geral da União (CGU) levam à conclusão inicial de não haver incompatibilidade entre os direitos à transparência e à proteção de dados. Dessa forma, o principal desafio no atual cenário não é a construção de uma interpretação jurídica-dogmática entre transparência e proteção de dados que permita sua compatibilização, mas no desenvolvimento e aplicação de um ferramental que possibilite a conjugação de ambos em situações concretas.



Portanto, adotou-se como hipótese da pesquisa que o Relatório de Impacto à Proteção De Dados (RIPD), instrumento previsto pela Lei Geral de Proteção de Dados Pessoais (LGPD) como uma ferramenta para avaliar e mitigar riscos a direitos fundamentais decorrentes de atividades de tratamento de dados, pode ser o vetor mais adequado para que controladores avaliem os riscos relacionados a processos de abertura de dados, adotem medidas para mitigá-los e atendam ao princípio da responsabilização e prestação de contas. Essa hipótese é corroborada pelo entendimento da ANPD no caso Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), em que se determinou que o Instituto elaborasse um Relatório de Impacto à Proteção de Dados (RIPD) para avaliar a amplitude mais adequada da divulgação de dados pessoais.

A partir de revisão da literatura dedicada a analisar o Relatório de Impacto à Proteção de Dados e metodologias de avaliação de risco, chegou-se à conclusão de que o modelo metodológico mais adequado seria um que permitisse a compatibilização de dois pólos distintos de análise (transparência e proteção de dados) e uma síntese da relação entre essas duas variáveis. Desta forma, a metodologia de risco e benefício adotada em estudos conduzidos pelo Berkman Klein Center de Harvard e pela Future of Privacy Forum para apoiar decisões de políticas públicas sobre dados abertos em prefeituras de cidades estadunidenses serviu como ponto de partida para a construção de uma metodologia própria.

Como etapa final da pesquisa, a partir da supracitada metodologia de risco e benefício, foram feitas adaptações e incrementos com objetivo de melhor adequar as bases metodológicas aos preceitos da proteção de dados pessoais no Brasil, permitindo uma análise que seja centrada nos riscos a direitos fundamentais, não apenas no risco à reidentificação dos titulares no processo de abertura de dados.



Ademais, contextualiza e concretiza os benefícios esperados do processo de transparência em curso pelo poder público. Traz-se ainda, como resultado da pesquisa, a proposição de um passo-a-passo e um modelo de framework que permita, após a análise inicial de risco e valor,

medidas de mitigação de risco sejam adotadas e uma nova avaliação de risco e valor seja feita, a das medidas previstas, para se chegar a um resultado final de custo-benefício que conjugue integralmente estas duas variáveis. Denominou-se a presente metodologia como metodologia de custo-benefício.

A metodologia de custo-benefício proposta se dá por meio de seis etapas:

- **Passo 1** - Descrição da atividade de abertura de dados. Identificação do controlador, da base de dados envolvida, das categorias de dados pessoais, dos titulares afetados e do contexto jurídico aplicável.
- **Passo 2** - Análise do valor e do risco iniciais. Avaliação independente do grau de valor esperado com a abertura dos dados e do grau de risco aos titulares. Ambos são calculados pela combinação entre probabilidade de ocorrência e impacto esperado, e o valor global de risco e valor são extraídos a partir da média entre todos os riscos e benefícios mapeados em uma matriz 3×3 compatível com o modelo de RIPD já utilizado pelo Ministério da Gestão e Inovação no Setor Público (MGI).
- **Passo 3** - Cálculo do custo-benefício inicial. Comparação entre o grau de valor global e o grau de risco global para determinar se a abertura, tal como planejada, apresenta uma relação favorável, equilibrada ou desfavorável entre benefício público e risco aos titulares.
- **Passo 4** - Adoção de medidas de mitigação. Identificação de medidas capazes de reduzir os riscos sem eliminar ou comprometer significativamente o valor da divulgação. Quando as medidas de mitigação reduzirem o valor da abertura, devem ser avaliadas medidas complementares de promoção do valor.
- **Passo 5** - Definição do custo-benefício final. Recálculo do valor global remanescente e do risco residual global após a aplicação das medidas de mitigação, resultando na avaliação definitiva do custo-benefício da abertura.
- **Passo 6** - Decisão sobre a disponibilização dos dados. Com base no custo-benefício final, a decisão de abertura, abertura parcial ou não disponibilização pode ser feita amparada por uma análise empírica e contextual.

Por fim, o relatório traz, em síntese, três recomendações de melhores práticas para a tomada de decisão e desenvolvimento de políticas públicas de dados abertos em órgãos públicos:

1. **Conduzir análise de riscos a direitos fundamentais específica para decisões sobre abertura (ou sua negativa) de dados pessoais**, sem condicionar a abertura de dados pessoais a processos de anonimização ou pseudonimização ou limitar a análise de riscos a unicamente riscos relativos à reidentificação dos titulares.
2. **Disponibilizar versões públicas dos RIPDs elaborados em contextos de abertura de dados**. Em consonância com o entendimento consolidado da ANPD e com os

princípios constitucionais da publicidade e da transparência administrativa, os relatórios de impacto produzidos por órgãos públicos devem estar disponíveis para acesso e controle social, com as adaptações necessárias para proteger informações sensíveis de segurança.

- 3. Incorporar a metodologia de custo-benefício como metodologia de análise de risco na elaboração de RIPDs.** A decisão sobre a disponibilização de dados que contenham informações pessoais deve incluir, de forma sistemática, a avaliação do valor público esperado e dos riscos aos titulares, e a partir da maximização do valor público e minimização do risco, tomar decisões fundamentadas acerca da abertura, abertura parcial ou não disponibilização.

LISTA DE ILUSTRAÇÕES

Figura 1 – Matriz probabilidade x impacto _____	42
Figura 2 – Matriz probabilidade x impacto inspiradas em autoridades do Uruguai e Argentina _____	44
Figura 3 – Escala do elemento exposição da metodologia _____	45
Figura 4 – Relação entre riscos de privacidade e cibersegurança definidos pelo NIST _	47
Figura 5 – Matriz Probabilidade x Impacto _____	66

LISTA DE QUADROS

Quadro 1 – Menções a risco na Lei Geral de Proteção de Dados _____	32
Quadro 2 – Matriz de risco de probabilidade inspirada em autoridades do Uruguai e Argentina _____	43
Quadro 3 – Matriz de risco e benefícios _____	50
Quadro 4 – Quadro de conceitos para análise de riscos e benefícios desenvolvida pelos pesquisadores do Berkman Klein Center for Internet & Society _____	51
Quadro 5 – Escala de grau de probabilidade dos riscos desenvolvida pela Future of Privacy Forum traduzida e adaptada pela Data Privacy Brasil _____	54
Quadro 6 – Escala de grau de impacto de benefício desenvolvida pela Future of Privacy Forum traduzida e adaptada pela Data Privacy Brasil _____	55
Quadro 7 – Índices de probabilidade do valor _____	63
Quadro 8 – Índices do impacto do valor _____	64
Quadro 9 – Exemplos para o grau do impacto do valor _____	64
Quadro 10 – Probabilidade do risco _____	68
Quadro 11 – Impacto do risco _____	68
Quadro 12 – Exemplos para o grau do impacto do risco _____	69
Quadro 13 – Relação entre valor e risco _____	71
Quadro 14 – Matriz de custo-benefício _____	71
Quadro 15 – Tipos de medidas de mitigação _____	72
Quadro 16 – Indicadores de custo-benefício _____	74

LISTA DE ABREVIATURAS E SIGLAS

AAIP Agencia de Acceso a la Información Pública da Argentina

ADI Ação Direta de Inconstitucionalidade

ANPD Agência Nacional de Proteção de Dados

CGAT Coordenação de Autos de Infração

CGF Coordenação-Geral de Fiscalização

CGPDP Coordenação-Geral de Proteção de Dados Pessoais

CGU Coordenadoria Geral da União

CIAM Coordenação de Apuração de Infrações Ambientais (CIAM)

CNPJ Cadastro Nacional da Pessoa Jurídica

CPF Cadastro de Pessoas Físicas

DAPS Divisão de Assuntos Prioritários e Estratégicos

DGE Departamento de Planejamento e Gestão Estratégica

DPIA Avaliação de Impacto à Proteção de Dados

DPO Encarregado de Proteção de Dados

DTC Diretoria de Transparência e Controle Social

ENEM Exame Nacional do Ensino Médio

FPF Future of Privacy Forum

GABIN Gabinete do Ministro

GDPR General Data Protection Regulation

HRIA Human Rights Impact Assessment

IA Inteligência Artificial

IBAMA Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis

IBGE Instituto Brasileiro de Geografia e Estatística

ICMBio Instituto Chico Mendes de Conservação da Biodiversidade

Inep Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira

LAI Lei de Acesso à Informação

LGPD Lei Geral de Proteção de Dados Pessoais

LIA Teste Do Legítimo Interesse

D

MGI Ministério da Gestão e Inovação no Setor Público

MP Medida Provisória

NIST National Institute of Standards and Technology

PFE Procuradoria Federal Especializada

PGF Procuradoria-Geral Federal

RIPD Relatório de Impacto à Proteção de Dados

SEI Sistema Eletrônico de Informações

SSC Secretaria de Serviços Compartilhados

STF Supremo Tribunal Federal

STJ Superior Tribunal de Justiça

STPC Secretaria de Transparência e Prevenção da Corrupção

TI Tecnologia da Informação

O

UFMG Universidade Federal de Minas Gerais

URCDP Unidad Reguladora y de Control de Datos Personales do Uruguai

ÍNDICE

Sumário executivo	03
Introdução	12
Metodologia	14
Objetivos de pesquisa	14
Desenho da pesquisa	14
Revisão de literatura, análise documental e interpretação institucional da LGPD em contextos de transparência pública	15
Entrevistas com gestores e servidores públicos	15
Revisão de literatura sobre o conceito de risco em Relatórios de Impacto à Proteção de Dados	16
Parâmetros conceituais e institucionais dos Relatórios de Impacto à Proteção de Dados	16
Metodologias de análise de riscos e benefícios	17
Desenvolvimento da metodologia de custo-benefício proposta	17
Estudos de caso e aplicação da metodologia	18
01. Transparência e proteção de dados	19
1.1. Harmonia entre transparência e proteção de dados: casos práticos	21
1.2. Anonimização	24
02. Relatório de impacto à proteção de dados e risco	27
2.1. Risco	28
2.2. Introdução ao RIPD	34
2.3. Requisitos e melhores práticas na elaboração de um RIPD	35

03. Riscos e benefícios	41
3.1. Metodologias de análise de risco	42
3.2. Metodologias de riscos e benefícios	50
04. Uma metodologia de custo-benefício	60
Passo 1 – Definição do tratamento de dados voltado para a disponibilização de dados pessoais	62
Passo 2 – Análise do Valor e do Risco iniciais	62
Passo 3 – Descobrindo o grau do custo-benefício	71
Passo 4 – Adoção de medidas de mitigação	73
Passo 5 – Definição do custo-benefício final	74
Passo 6 – Decisão sobre a disponibilização dos dados	75
Limitações	76
Conclusão	77
Referências	79
Apêndice A – aplicação da metodologia	83

INTRODUÇÃO

INTRODUÇÃO

O presente estudo é resultado de uma contratação do Ministério de Gestão e Inovação de Serviços Públicos (MGI) que teve como objetivo o desenvolvimento de uma pesquisa sobre quais seriam os principais elementos que um relatório de impacto à proteção de dados pessoais precisaria conter para abordar mais adequadamente situações de abertura de dados pessoais tratados pelo poder público.

A transparência pública é essencial para oferecer dados confiáveis para todas as camadas da sociedade, sendo uma ferramenta para garantir o direito de acesso à informação, o controle social e o exercício da cidadania. Diante do elevado valor que informações públicas podem ter para fins do interesse público, faz-se necessária a pesquisa sobre o tema.

Assim, a análise desenvolvida a seguir pretende abarcar como pensar os riscos e os benefícios da abertura de dados pessoais em ações de transparência pública, seja ativa e passiva. Para isso, elaborou-se uma metodologia de custo-benefício que complementa o modelo padrão de Relatório de Impacto à Proteção de Dados (RIPD) já desenvolvido pela Coordenação-Geral de Proteção de Dados Pessoais - CGPD/DPD/SSC/MGI. A ideia subjacente a essa metodologia consiste em reforçar o processo de avaliação de risco e, simultaneamente, demonstrar a importância de se analisar a relevância da publicação de dados pessoais.

Os processos de análise sugeridos neste relatório foram elaborados de modo a evidenciar 1) a importância de buscar o equilíbrio considerando também na avaliação o valor (benefícios), e não apenas os riscos (custos) da publicação; 2) que, em vista do interesse público e a partir de uma avaliação completa, há riscos que são toleráveis e é possível tomar uma decisão mais informada sobre como seguir com o tratamento de forma segura; 3) compreender quais os benefícios esperados com a publicação é um meio de garantir manutenção da utilidade da base de dados durante o processo de mitigação de risco; e 4) para além da transparência dos dados em si, o relatório de impacto à proteção de dados é um documento que também precisa estar disponibilizado para a população.

O texto está organizado em quatro capítulos. Inicialmente, apresenta-se a metodologia aplicada ao desenvolvimento deste relatório. Em seguida, o primeiro capítulo discute a relação entre transparência e proteção de dados. O segundo capítulo dedica-se ao relatório de impacto à proteção de dados e a avaliação de risco. O terceiro capítulo detalha a metodologia de custo-benefício desenvolvida. Por fim, o quarto capítulo apresenta os casos práticos em que é aplicada a metodologia de custo-benefício a fim de demonstrá-la concretamente.

METODOLOGIA

OBJETIVOS DA PESQUISA

A pesquisa teve como objetivo geral desenvolver recomendações de melhores práticas para a construção de Relatórios de Impacto à Proteção de Dados (RIPD) aplicados a atividades de tratamento de dados relacionadas à transparência pública e à abertura de dados pessoais no setor público.

Para alcançar esse objetivo geral, a pesquisa foi orientada pelos seguintes objetivos específicos:

1. identificar os parâmetros conceituais, regulatórios e os requisitos mínimos que orientaram a elaboração de RIPDs no contexto da LGPD e das recomendações da Agência Nacional de Proteção de Dados;
2. mapear os principais desafios institucionais e operacionais enfrentados pela administração pública na compatibilização entre transparência pública e proteção de dados pessoais;
3. examinar como a metodologia de análise de riscos e benefícios pode ser aplicada à avaliação de atividades de tratamento de dados relacionadas à transparência pública;
4. produzir uma metodologia de custo-benefício com base em influências metodológicas de diferentes modelos de análise de riscos, considerando também as especificidades do campo brasileiro;
5. testar a aplicação dessa metodologia em estudos de caso reais ou representativos, demonstrando sua utilidade para orientar decisões sobre transparência de dados;
6. produzir recomendações metodológicas para a administração pública na elaboração de RIPDs voltados a iniciativas de transparência que envolvessem dados pessoais.

DESENHO DA PESQUISA

Para atender a esses objetivos, foram combinadas quatro estratégias metodológicas principais: *revisão de literatura, análise documental, entrevistas semiestruturadas com gestores e servidores públicos e desenvolvimento de estudos de caso*. Essas estratégias foram articuladas de acordo com as perguntas orientadoras da pesquisa, de modo que cada etapa metodológica contribuiu para responder a uma dimensão específica do problema investigado.

A metodologia adotada buscou, portanto, articular uma dimensão teórico-conceitual, voltada à compreensão dos fundamentos do RIPD, da noção de risco e da metodologia de riscos e benefícios, com uma dimensão empírica e aplicada, direcionada à análise de documentos ins-

titucionais, à escuta de gestores públicos e à aplicação da metodologia proposta em estudos de caso.

Revisão de literatura, análise documental e interpretação institucional da LGPD em contextos de transparência pública

A primeira etapa da pesquisa buscou responder à seguinte pergunta: *como a produção científica, as instituições públicas e os órgãos reguladores interpretaram e aplicaram os princípios da LGPD em situações de transparência pública e abertura de dados?*

Para responder a essa pergunta, foi realizada revisão bibliográfica sobre a relação entre proteção de dados pessoais e transparência pública, com atenção especial aos debates sobre acesso à informação, abertura de dados, publicidade administrativa e limites jurídicos para a divulgação de dados pessoais pelo poder público.

Além disso, foi conduzida análise documental de materiais institucionais e decisões administrativas relevantes, incluindo notas técnicas, orientações de órgãos reguladores e fiscalizadores, manifestações administrativas e documentos relacionados à divulgação de dados públicos. Essa análise permitiu observar como os conflitos entre transparência e proteção de dados foram tratados na prática institucional, especialmente quanto à interpretação de princípios como finalidade, necessidade, adequação, transparência, segurança e responsabilização.

Essa etapa metodológica permitiu construir uma ponte entre o debate acadêmico e a realidade administrativa, evidenciando como os princípios da LGPD foram mobilizados em situações concretas de abertura e restrição de acesso a dados pessoais no setor público.



Entrevistas com gestores e servidores públicos

Nessa primeira etapa da pesquisa, também buscou-se responder à pergunta: *quais foram os principais desafios enfrentados por gestores e servidores públicos na compatibilização entre transparência pública e proteção de dados pessoais?*

Para isso, foram realizadas entrevistas semiestruturadas com gestores e servidores públicos envolvidos em atividades relacionadas à transparência, abertura de dados, acesso à informação, governança de dados e proteção de dados pessoais de órgãos como a Coordenadoria Geral da União (CGU) e do Ministério da Gestão e da Inovação em Serviços Públicos (MGI). A escolha por entrevistas semiestruturadas permitiu combinar um roteiro previamente definido com a possibilidade de aprofundamento de temas emergentes durante as conversas.

Essa estratégia foi adotada porque parte relevante dos desafios enfrentados pela administração pública não aparece necessariamente documentada em normas, notas técnicas ou decisões administrativas. As entrevistas permitiram acessar percepções práticas sobre dificuldades institucionais, limitações operacionais, inseguranças jurídicas, ausência de metodologias consolidadas, conflitos entre áreas internas e desafios de implementação da LGPD em rotinas de transparência pública.

Com isso, a pesquisa pôde aproximar suas recomendações das necessidades reais do setor público, evitando a formulação de propostas apenas abstratas ou excessivamente distantes da prática administrativa.

Tanto a análise documental e de literatura, quanto as entrevistas compõem o capítulo 1 deste trabalho.

Revisão de literatura sobre o conceito de risco em Relatórios de Impacto à Proteção de Dados

A terceira pergunta da pesquisa foi: *o que significa risco em um Relatório de Impacto à Proteção de Dados?*

Para respondê-la, foi realizada revisão bibliográfica sobre o conceito de risco em proteção de dados. A pesquisa examinou como a literatura especializada, com predominância das obras de Bruno Bioni (2022), Maria Cecília O. Gomes (2020), Rafael Zanatta (2017) e Raphaël Gellert (2017), compreendeu o risco como a universalidade de eventos que pode afetar direitos e liberdades fundamentais dos titulares de dados pessoais.

Essa etapa foi fundamental porque a análise de risco constitui o pressuposto central dos relatórios de impacto. Antes de propor uma metodologia aplicável a casos de transparência pública, foi necessário delimitar o que estava sendo entendido por risco, quais dimensões deveriam ser consideradas e como esse conceito poderia ser operacionalizado em uma metodologia voltada ao setor público.

A revisão permitiu compreender a dimensão conceitual de risco, denotando a importância das metodologias que o tornam visível e das medidas de mitigação possíveis.

Parâmetros conceituais e institucionais dos Relatórios de Impacto à Proteção de Dados

A quarta pergunta orientadora da pesquisa foi: quais foram os parâmetros conceituais e institucionais para a elaboração de Relatórios de Impacto à Proteção de Dados?

Essa etapa foi desenvolvida por meio de revisão bibliográfica nacional sobre Relatórios de Impacto à Proteção de Dados, bem como pela análise das previsões legais da LGPD e das recomendações produzidas pela Agência Nacional de Proteção de Dados. O objetivo foi identificar os requisitos mínimos, os fundamentos jurídicos e os elementos operacionais que orientaram a construção de RIPDs no Brasil.

A análise buscou compreender o RIPD como um processo de governança e prestação de contas específico e com sua dimensão dada pela LGPD. Assim, foram examinadas suas funções de forma a estabelecer uma base conceitual clara para a pesquisa, delimitando o papel do RIPD em atividades de tratamento de dados pessoais realizadas pelo setor público.

As respostas das perguntas 3 e 4 estão consolidadas no capítulo 2 deste trabalho.

Metodologias de análise de riscos e benefícios

A quinta pergunta orientadora foi: *o que é e como funciona a metodologia de análise de riscos e benefícios, e como ela pôde auxiliar na tomada de decisão em situações de tensão entre proteção de dados e transparência pública?*

Essa etapa foi conduzida por meio de revisão bibliográfica em duas etapas. A primeira versou sobre diferentes metodologias do risco relacionadas à governança de dados pessoais. Já o segundo momento versou sobre a metodologia de análise de riscos e benefícios aplicadas a relatórios de impacto e a processos decisórios envolvendo dados pessoais. Com relação à primeira etapa, examinamos as diferentes metodologias, suas limitações e virtudes quando o assunto é proteção de dados pessoais e governança.

Já com relação à segunda etapa dessa pergunta, a pesquisa examinou experiências relevantes que descreveram e aplicaram a metodologia de riscos e benefícios no contexto de abertura de dados no setor público, com atenção à lógica de seu funcionamento e suas limitações.

A análise buscou demonstrar a utilidade dessas metodologias em contextos nos quais a proteção de dados e a transparência pública se tornam valores em disputa. Isso porque a metodologia de riscos e benefícios permite avaliar conjuntamente os ganhos esperados com a abertura de dados e os riscos que essa abertura poderia gerar aos titulares.

Essa etapa foi importante para demonstrar que a tomada de decisão em matéria de transparência pública pode ser mais qualificada quando os benefícios da abertura são explicitados, os riscos são documentados e as medidas de mitigação são avaliadas de forma proporcional e contextual.

Desenvolvimento da metodologia de custo-benefício proposta

A sexta pergunta da pesquisa foi: *como metodologias de risco-benefício podem ser adaptadas para o contexto analisado?*

Com base nas etapas anteriores, foi desenvolvida uma metodologia de custo-benefício voltada à avaliação de iniciativas de transparência pública e abertura de dados pessoais no setor público. Essa metodologia foi construída a partir da revisão bibliográfica de metodologias nacionais e internacionais de análise de risco em proteção de dados, bem como da análise documental de modelos institucionais de Relatório de Impacto à Proteção de Dados, incluindo a metodologia de riscos presente no modelo desenvolvido pelo Ministério da Gestão e Inovação em Serviços Públicos.

A metodologia proposta buscou adaptar influências internacionais e nacionais às especificidades do campo brasileiro. Dessa forma, desenvolvemos uma metodologia que permite considerar tanto os riscos aos direitos e liberdades dos titulares quanto os valores decorrentes da

disponibilização de dados. Ao comparar essas duas dimensões, é possível tomar decisões com base no custo e no benefício promovido por iniciativas dessa natureza.

Essa etapa permitiu tornar explícitas as principais influências metodológicas utilizadas na construção da proposta, além de contribuir para o debate sobre formas de avaliar risco em serviços públicos que envolvem dados pessoais.

A metodologia pode ser vista no capítulo 4 deste trabalho.

Estudos de caso e aplicação da metodologia

A sétima pergunta da pesquisa foi: *em que medida a utilização da metodologia de custo-benefício pôde aprimorar a elaboração de RIPDs voltados a iniciativas de transparência pública e abertura de dados?*

Para responder a essa pergunta, foram desenvolvidos estudos de caso nos quais a metodologia proposta foi aplicada a situações representativas de divulgação de dados no setor público simulando como poderia ser feita a avaliação. Os casos escolhidos foram a plataforma Divulga-CandContas, que divulga dados de candidaturas eleitorais, e a abertura de dados de embargos e autos de infração do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio), que significou a listagem de infratores ambientais. Os estudos de caso permitiram observar como a metodologia se comportou diante de situações concretas de tensão entre proteção de dados pessoais e transparência pública.

A aplicação prática buscou demonstrar como a metodologia de riscos e benefícios funcionou em casos conhecidos de embate entre abertura de dados e proteção de dados. Além disso, permitiu verificar quais vantagens a metodologia teve em tornar riscos e benefícios mais visíveis, suas limitações e cuidados deveriam ser considerados em sua implementação no contexto brasileiro.

O Estudo de caso pode ser visto no Apêndice A deste trabalho.

01 TRANSPARÊNCIA E PROTEÇÃO DE DADOS

01 TRANSPARÊNCIA E PROTEÇÃO DE DADOS

A transparência pública e a proteção de dados pessoais frequentemente são equivocadamente identificadas como deveres estatais opostos, às vezes até antagônicos¹. Enquanto a transparência decorre do direito do cidadão à informação, seja ela particular ou de interesse público, e do princípio da publicidade para controle das atividades da administração pública (art. 5º, XXXII, e art. 37, da CF), a proteção de dados é vista como um desdobramento do direito à privacidade, tratando da não interferência sobre o cidadão e da não veiculação de suas informações pessoais (Brasil, 1988). Contudo, esta interpretação leva a uma lógica binária, de tudo ou nada (abertura de dados ou não abertura), que não condiz com o real propósito e modelo regulatório da proteção de dados pessoais.

Este direito trata principalmente da garantia de um fluxo apropriado de dados pessoais. Isso significa que, ao contrário da privacidade, que exige o afastamento de terceiros da esfera individual do sujeito, caracterizando-se como uma liberdade negativa, a proteção de dados constitui uma liberdade positiva, ao estabelecer diretrizes para que o titular possa interagir em um ambiente intersubjetivo, mobilizando informações pessoais, mas com a garantia de que essas informações não serão usadas de forma abusiva ou que possa violar algum de seus direitos fundamentais.

Nesse sentido, a proteção de dados pessoais se constitui como uma liberdade positiva, na medida em que cria novas condições de ação para o sujeito, e não apenas restringe a atuação de terceiros perante a ele (Mendes, 2020; Menke, 2020). A confirmação da amplitude e autonomia que a proteção de dados possui em relação ao direito à privacidade é evidenciada quando o inciso LXXIX é inserido no art. 5º, da Constituição Federal (Brasil, 1988), condizente com interpretação já dada pelo Supremo Tribunal Federal (STF) na Ação Direta de Inconstitucionalidade (ADI) 6387, que suspendeu a Medida Provisória 954/2020 que autorizava o compartilhamento de dados telefônicos entre companhias de telecomunicação e o Instituto Brasileiro de Geografia e Estatística (IBGE) e que reconheceu o caráter fundamental e autônomo do direito em questão.

A Lei Geral de Proteção de Dados Pessoais (LGPD), como lei regulamentadora deste direito, estabelece os parâmetros a serem seguidos, orientando os agentes de tratamento de dados. Além dos fundamentos e princípios (art. 2º e 6º, da LGPD, respectivamente) que já instruem significativamente os agentes, a lei traz ferramentas que garantem a legitimidade do tratamento de dados por meio do estabelecimento de procedimentos básicos, como a identificação de

1 Relatório Impactos da LGPD nos pedidos de LAI ao governo federal, produzido pela agência Fiquem Sabendo e pelo Insuper, com apoio da FGV e financiamento da Fundação Heinrich Böll. Disponível em: <https://fiquemsabendo.com.br/transparencia/relatorio-lgpd/>. Acesso em: 25 mai. 2026.

bases legais, obrigações de registro de atividades e elaboração de relatórios de impacto à proteção de dados como forma de prestação de contas, canais claros e acessíveis para exercícios de direitos dos titulares, entre outros. Isso evidencia que a proteção de dados nunca tratou sobre a não utilização destas informações, e sim sobre estabelecer o procedimento adequado para a melhor governança do fluxo informacional (Brasil, 2018).

Nesse sentido, a transparência e proteção de dados pessoais são complementares e essenciais em um contexto em que a datificação dos serviços e atividades públicas têm se intensificado. Dados pessoais são essenciais para o aprimoramento de políticas e serviços públicos, mas também cumprem um papel relevante para que o cidadão possa exercer sua cidadania, o controle social e obter informações oficiais (Facio, 2023).

Sendo assim, o papel da proteção de dados pessoais não é impedir a transparência, mas sim guiá-la para que, com maior segurança jurídica, seja possível identificar em que casos os dados pessoais podem ou, até mesmo, devem ser divulgados, o formato desta divulgação e quais as medidas de mitigação de riscos.

Consequentemente, a Lei de Acesso à Informação (LAI) e a LGPD trabalham para alcançar um maior grau de transparência, ao contrário da lógica de tudo ou nada, elas convergem para reduzir a assimetria informacional entre Estado e cidadão (Bioni; Silva; Martin, 2022).

1.1 HARMONIA ENTRE TRANSPARÊNCIA E PROTEÇÃO DE DADOS: CASOS PRÁTICOS

Alguns casos são emblemáticos para demonstrar as dificuldades práticas advindas de uma interpretação restritiva da relação entre transparência e proteção de dados, mas que também possibilitaram um debate relevante sobre como pensar a harmonia entre as normas.

O primeiro deles é o caso Inep, que ilustra o conflito prático que pode surgir na divulgação de informações quando não se compreende o impacto do tratamento e o quão tolerável é o seu risco. O caso se desenvolveu da seguinte forma: em 2022, o Inep, instituto responsável pela disponibilização de dados do censo educacional, decidiu alterar a disponibilização dos dados do referido censo, a fim de adequar-se às normas da LGPD.

Isso significava retirar a publicidade de microdados dos censos escolares e do Exame Nacional do Ensino Médio (ENEM) uma vez que, considerando as conclusões do estudo elaborado pela Universidade Federal de Minas Gerais contratado por meio do Termo de Execução Descentralizada 870, a ampla transparência destas informações representava um potencial risco de reidentificação dos titulares, sendo a anonimização no processo estatístico insuficiente. Além da reidentificação, a princípio haveria risco de violação à privacidade, inferência a dados sensíveis, além de a maioria dos titulares serem crianças e adolescentes.

As medidas de mitigação de risco, como o Serviço de Acesso a Dados Protegidos que colocava protocolos de segurança mais intensos para o acesso aos dados, foram vistas pelas entidades que dependiam destes dados como demasiadamente restritivas. A sociedade civil se mobilizou apontando que a LGPD não impedia de forma alguma o tratamento destes dados, citando o

art. 7^a, II e III², e que a proteção de dados poderia existir sem prejudicar a transparência de dados de interesse público.



Órgãos públicos também se posicionaram. A CGU, por meio da Nota Técnica 136/2022/CGAT/DTC/STPC em que reforça o compromisso do poder público com a transparência, demonstrando a compatibilidade e harmonia entre LAI e a LGPD. Outra manifestação relevante foi a da ANPD por meio da Nota Técnica nº 46/2022, produzida pela Coordenação Geral de Fiscalização, em que determina a elaboração de uma RIPD a fim de que fossem elencados os riscos aos titulares dos microdados, fornecendo melhores insumos para avaliar as medidas de mitigação de riscos.

Nessa nota, a ANPD também conclui que pode haver hipótese legal legítima para realizar o tratamento referente à divulgação dos microdados. O órgão reforça que a anonimização não é uma solução a ser utilizada em qualquer cenário, não sendo uma condição técnica para a publicação ou compartilhamento de dados.

O aspecto central, considerando as normas da LGPD, é a identificação de riscos e elaborar métodos para mitigá-los. Desse modo, admite-se a existência de riscos quando o tratamento for necessário para atender determinações legais e o interesse público, bem como não obstaculizar o direito à informação. A nota também aponta que a limitação de acesso condicionado à assinatura de termo de responsabilidade também poderia ser uma medida de mitigação de riscos.



Em dezembro do mesmo ano, o Inep apresentou à ANPD os relatórios de impacto exigidos. Em resposta, na Nota Técnica nº 12/2023, a ANPD avalia os relatórios de impacto e conclui que há hipótese legal legítima para realizar o tratamento referente à divulgação dos microdados. Aponta, ainda, que a possibilidade de reidentificação dos titulares, indicada como o risco mais relevante no RIPD apresentado, não representa um descumprimento da lei quando implementadas salvaguardas adequadas.

O segundo caso elencado trata da decisão tomada pelo Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio), descrita no parecer n. 00156/2023/CAI/PFE-ICMBIO/PGF/AGU, que evidência a viabilidade de uma divulgação ampla de dados pessoais quando estes são essenciais para a transparência de informações de interesse público.



Em consulta encaminhada pela Coordenação de Apuração de Infrações Ambientais (CIAM) à Coordenação de Autos de Infração da Procuradoria Federal Especializada (CAI/PFE) junto ao ICMBio, uma das questões levantadas foi se a autoridade competente do ICMBio poderia autorizar a disponibilização de dados de Cadastro de Pessoas Físicas (CPF) para fins de compartilhamento com instituições financeiras visando impedir a concessão de financiamento agrícola para áreas embargadas.

2 Texto legal: “II – para o cumprimento de obrigação legal ou regulatória pelo controlador; III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei” [Brasil, 2018].

O questionamento tinha como objetivo verificar se o ICMBio poderia agir de forma similar ao IBAMA que possuía página para consulta pública com dados de pessoas físicas e jurídicas disponibilizados de forma aberta. O IBAMA já havia publicado o Despacho Decisório No 2/2023/GABIN que por sua vez utilizava os fundamentos do Parecer n. 00010/2023/DAPS/PFE-IBAMA-SEDE/PGF/AGU (AGU, 2023). Nesse parecer é defendida a transparência de CPF e do Cadastro Nacional de Pessoa Jurídica (CNPJ) visto que é de interesse público as informações completas sobre áreas embargadas pelo poder público.

A consulta da CIAM apontava que os embargos não deveriam se restringir apenas ao controle processual, já que a garantia dos efeitos do embargo também depende do controle ambiental, social e econômico. São justamente esses dois últimos aspectos que justificam o interesse público na livre disponibilização de CPF e CNPJ, pois são dados necessários para evitar que transações financeiras e comerciais resultem em infrações ambientais. Fornecendo, portanto, um mecanismo de checagem para instituições financeiras, empresas, a sociedade e organizações da sociedade civil.

D

Em resposta, a CAI/PFE entendeu que era sim possível a publicidade de CPF vinculado a áreas embargadas. Na análise jurídica, reconhece-se que a divulgação de tais informações compõem a estratégia de combate a infrações ambientais, sendo um desdobramento direito coletivo ao meio ambiente ecologicamente equilibrado (art. 225, da Constituição Federal) (Brasil, 1988) materializado na Política Nacional do Meio Ambiente (Lei 6.938/1981) (Brasil, 1981) que estabelece instrumentos de divulgação de informações necessárias para a proteção do meio ambiente e nos deveres do Poder Público previstos no art. 18, 96 e 149, do Decreto 6.514/2008 (Brasil, 2008) e art. 70, da Lei 9.605/1998 (Brasil, 1998) que dispõe sobre a infração ambiental e seu caráter de público, incluindo a publicidade das sanções administrativas.

Sobre a transparência pública, complementam citando, dentre outras, a decisão do Superior Tribunal de Justiça no Recurso Especial n. 1857.098 - MS, em que afirma que a obrigação do Estado com a transparência ambiental é presumida, sujeita a controle judicial e que seu descumprimento deve ser justificado.

No desenvolvimento da análise, conclui-se que há o devido respaldo legal para divulgação de informações de infratores, tanto pelo dever estatal de transparência, quanto para a garantia da política pública em prol do meio ambiente. Quanto aos dados pessoais em específico, a análise se debruça sobre a LGPD, observando a hipótese de tratamento, referente ao art. 7º, II³, da lei, para a consecução de políticas públicas visando o atendimento da finalidade pública na persecução do interesse público, conforme o art. 23⁴, da mesma lei.

Portanto, a análise dos casos acima revela uma convergência entre a interpretação dos órgãos de controle e da Autoridade Nacional de Proteção de Dados. A proteção de dados pesso-

O

3 Ver nota 2.

4 “O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 [Lei de Acesso à Informação], deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público [...]” (Brasil, 2018).

ais não é um direito fundamental que se materializa pela interdição do fluxo de dados pessoais, mas sim por uma adequada governança sobre este fluxo.

É perfeitamente compatível com os fundamentos da LGPD a divulgação pública de informações pessoais independentemente da autorização do titular. A Lei inclusive cria ferramentas para que isso se dê com maior segurança jurídica ao estabelecer um rol de bases legais que não se limitam, e até prescindem do consentimento do titular.

Novamente, por não se tratar de um direito que opera na lógica tudo-ou-nada, a proteção de dados dispõe do ferramental adequado para que os agentes de tratamento consigam avaliar os riscos das atividades de tratamento de dados, estabeleçam mecanismos de mitigação destes riscos, e contrastem estes riscos com outros valores constitucionais dotados de interesse público, como a transparência.

1.2 ANONIMIZAÇÃO

Uma medida frequentemente aventada para fortalecer o tratamento seguro e adequado de dados pessoais é a anonimização. Esse processo, conforme definido no art. 5º, XI, da LGPD, consiste na “[...] utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo” (Brasil, 2018). Na medida em que dados anonimizados perdem a qualificação de dados pessoais, a incidência das regras de proteção de dados estaria afastada, sendo uma medida de aumentar não só a segurança técnica perante o tratamento de dados, mas também jurídica.

Contudo, existem três pontos de atenção sobre a anonimização relevantes para esta análise. Em primeiro lugar, nem todo tratamento consegue se beneficiar da anonimização uma vez que a manutenção de informações pessoais pode ser necessária, inclusive em casos de transparência pública⁵, e a divulgação de informações pessoais não representa necessariamente uma violação à LGPD, conforme abordado na seção anterior.

O segundo ponto é que a anonimização não é uma técnica que reduz o risco de reidentificação a zero (ANPD, 2022). A anonimização deve ser compreendida como um conjunto de técnicas possíveis de serem aplicadas, em uma abordagem baseada em processo, que reduz significativamente o risco de um conjunto de dados identificar um titular. Os fatores a serem considerados nesta probabilidade de reidentificação, conforme estabelecido pelo art. 12 §1º são o custo, tempo e tecnologia disponíveis à época, sendo assim, somar a anonimização com outras salvaguardas é sempre recomendável em casos em que o que se objetiva é não tratar dados pessoais (Brasil, 2018).

E por fim, em terceiro lugar, possibilidade de reidentificação não é impeditivo absoluto para a divulgação de informações anonimizadas ou pseudonimizadas. Assim como visto no caso Inep, há informações que precisam ser divulgadas de forma anonimizada, mas a possibilidade de reversão e seus riscos devem ser avaliados frente ao benefício para o interesse público a fim

5 A utilidade do dado é um ponto relevante quando se analisa a possibilidade ou não de se anonimizar dados pessoais. Ver em: <https://www.gov.br/participamaisbrasil/blob/baixar/37060>. Acesso em: 26 mai. 2026.

de garantir a transparência pública e direitos que possam estar envolvidos no caso concreto⁶.

É justamente sobre este último ponto que trata o caso Inep. A supressão de microdados do Censo da Educação e Exame Nacional do Ensino Médio, o Inep afirmou que a medida foi tomada porque, em estudo promovido pelo Laboratório Inscript, da UFMG, verificou-se a possibilidade de reversão dos processos de anonimização impostos à época. Por haver dados de crianças e adolescentes, além de outros sensíveis, como raça ou condições de saúde, o órgão optou pela supressão completa dessas informações.

Diante do impasse, ANPD firmou entendimentos importantes sobre o tema na Nota técnica nº 46/2022/CGF/ANPD. O documento afirma que a LGPD não estabeleceu a anonimização como condição técnica para a divulgação pública ou compartilhamento de dados pessoais por entidades e órgãos públicos. A principal determinação é quanto à necessidade de avaliação de riscos e adoção de medidas para mitigar a ocorrência de danos.

Diante do interesse público na divulgação dos dados pelo Inep, a Agência afirmou ser necessário ponderar o direito à privacidade e proteção de dados com análise de riscos da divulgação de informações pessoais, bem como medidas de mitigação para possíveis danos decorrentes do tratamento. Para isso, devem ser considerados cenários e evidências com aspectos objetivos da realidade, evitando especulações para a avaliação de riscos e mitigação dos danos.

Na prática, o precedente demonstra que, mesmo havendo risco de reidentificação de titulares de dados, havendo interesse público relevante na transparência ativa, há possibilidade de publicação de bases – nesse caso, voltadas para a educação. Segundo a Agência,

A LGPD não estabeleceu a anonimização como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais por entidades e órgãos públicos. Ao contrário, como já mencionado, a principal determinação da LGPD é quanto à necessidade de avaliação de riscos e de adoção de medidas para mitigar a ocorrência de danos. Por isso, a eventual identificação dos titulares ou a admissão de algum grau de risco de sua identificação, quando necessário para atender, por exemplo, a determinações legais, o interesse público e o direito de acesso à informação, são compatíveis com a LGPD, desde que adotadas as salvaguardas apropriadas (ANPD, 2022, p. 7-8).

Vê-se, portanto, que a anonimização não é considerada uma solução definitiva para harmonizar preceitos da proteção de dados e transparência pública. Na verdade, **admite-se a possibilidade de reidentificação de titulares de dados quando houver interesse público, determinação legal ou direito de acesso à informação** condicionado à adoção de medidas técnicas e administrativas capazes de mitigar potenciais danos.

⁶ O estudo preliminar sobre anonimização desenvolvido pela ANPD elabora mais a fundo como pode funcionar a gestão de riscos de reidentificação. Ver a publicação, nas páginas 18 e 19, disponível em: <https://www.gov.br/participamaisbrasil/blob/baixar/37060>. Acesso em: 25 mai. 2026.

Para isso, a ANPD afirma que o RIPD tem centralidade no tema. Definido como

[...] documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Brasil, 2018).

O RIPD é um registro formal do compromisso da organização com a proteção de dados, servindo como evidência para efetivação dos princípios da transparência, responsabilização e prestação de contas.

Ademais, como parte deste processo prévio de avaliação, na transparência ativa e passiva, cabe execução de um teste de interesse público, uma avaliação discricionária que visa compreender se a probabilidade e o grau de um dano é maior ou menor do que o interesse público envolvido na divulgação de certa informação. O dano, no caso, feriria um direito ou bem jurídico específico e interesse público deve considerar a relevância da informação para a participação social e exercício da cidadania, prestação de contas e responsabilização da administração pública, fomento da transparência pública, entre outros (Ribeiro; Machado, 2020).

Assim, demonstra-se que o caminho essencial para harmonização do direito à proteção de dados pessoais e transparência pública perpassa o conceito de risco no tratamento de dados, pelo equilíbrio entre o interesse público e probabilidade de dano, bem como a documentação de processos pelo RIPD.

02 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS E RISCO

2.1 RISCO

Compreender o que significa risco no RIPD envolve entender que esse conceito parte de um processo amplo de risquificação do direito à proteção de dados. Com isso é possível ver a necessidade de um RIPD bem como da circunscrição de riscos que ele foi pensado no Brasil.

Em *Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?*, Rafael Zanatta (2017) busca apresentar o conceito de risquificação do direito e sua conexão com a regulação em proteção de dados. A partir da análise do direito europeu, Hood, Hothstein e Baldwin (2001 apud Zanatta, 2017, p. 181) mostra que tal processo coloca o risco como elemento central e se concentra em processos de “[...] (i) reunião de informação e cognição de riscos, (ii) criação de regras e padrões de conduta e (iii) enforcement e monitoramento da modificação do comportamento social”. Em termos gerais, esse modelo de “direito do risco” busca o “isolamento de questões complexas e incertezas científicas para agentes decisórios de orientação marcadamente tecnicista que podem ou não seguir um modelo decisório baseado em precaução” (Zanatta, 2017, p. 181).

A partir da visão deste modelo de direito do risco são criadas diversas obrigações jurídicas com o objetivo modificar o comportamento potencialmente danoso a “níveis ótimos, evitar catástrofes e processos irreversíveis” e “aumentar o nível de informação disponível para qualificação dos processos de percepção dos riscos” marcados por “vieses culturais e visões de mundo contrastantes” (Zanatta, 2017, p. 181).

No contexto da proteção de dados, Zanatta (2017, p. 184) destaca que a risquificação do direito é um processo

[...] de reformatação jurídica a partir da ampliação da tutela coletiva e sua imbricação com a autoridade independente de proteção de dados pessoais, a disseminação de instrumentos regulatórios ex ante e o uso intensivo de metodologias de gestão de risco e calibragem entre riscos, inovações e imunidades.

Em outras palavras, a risquificação acontece principalmente em três esferas: *institucional, normativa e cultural*.

Institucional na medida em que a tutela da proteção de dados passa a ser exercida de forma combinada entre organizações da sociedade civil e autoridades de proteção de dados. Movimento que amplia a tutela coletiva sobre esse direito, principalmente sobre seus potenciais

riscos a uma dimensão coletiva.

Normativa pois registra a presença, em leis de proteção de dados, de obrigações e instrumentos de identificação e mitigação de riscos. Tais leis nomeiam e descrevem os modos pelos quais os riscos dos tratamentos de dados precisam ser vistos e enfrentados. É nessa modificação que instrumentos como a Avaliação de Impacto à Proteção de Dados (DPIA) e Relatório de Impacto à Proteção de Dados se insere.

Cultural por decorrência da disseminação de metodologias de análise de risco produzidas por diferentes agentes e políticas de governança de dados que lidam com os potenciais do tratamento de dados pessoais. Esse aspecto é decorrente das obrigações normativas e institucionais da risquificação da proteção de dados e permite enxergar as principais discussões sobre o que é risco no contexto de um RIPD.

Para além disso, esse processo de risquificação da proteção de dados na Europa abriu maior espaço para co-regulação com a previsão pela General Data Protection Regulation (GDPR) de que agentes regulados podem criar melhores práticas, códigos de condutas, certificações e orientações profissionais como forma de lidar com os riscos do tratamento de dados pessoais (Zanatta, 2017).

Embora o trabalho de Zanatta (2017) tenha considerado o desenvolvimento da risquificação europeia da proteção de dados, é possível dizer que a LGPD também se apropriou desse modelo. Principalmente na previsão da possibilidade de estabelecimento de boas práticas pelos agentes regulados (art. 50 LGPD), códigos de boas condutas e certificações para comprovação de respeito às normas de proteção de dados e enfrentamento do risco nos casos de transferência internacional de dados (art. 33, II LGPD) o teste do legítimo interesse (art. 10) e a própria previsão do Relatório de Impacto a Proteção de Dados (art. 5, XVII LGPD).

Dentro desta abordagem regulatória, o principal comando da LGPD para os agentes de tratamento é que estes mobilizem a caixa de ferramentas trazidas pela lei para materializar contextualmente os princípios e conceitos jurídicos indeterminados. Conforme argumenta Bioni (2022, p. 52):

A evolução do texto da LGPD tem um fio condutor que é a progressiva delegação de uma série de competências decisórias aos agentes de tratamento de dados. Com isso, os atores regulados passam a ter um maior nível de discricionariedade, seja para significar conceitos jurídicos indeterminados, seja para eleger os meios pelos quais cumprem eficazmente – para usar um termo da definição do princípio da accountability – a lei.

Conectar a abordagem de regulação de risco com os mecanismos previstos na LGPD implica reconhecer que a lei estrutura espaços de decisão nos quais os agentes de tratamento devem avaliar, justificar e responder pelos riscos de suas atividades. Como vimos, a regulação de risco

envolve uma arquitetura normativa que combina discricionariedade, instrumentos jurídicos e exigências de prestação de contas.

A LGPD estabelece em diversos momentos a possibilidade de que o agente de tratamento atuará de boa-fé e será capaz de justificar suas escolhas e permitirá formas de controle social e institucional. Essa lógica está diretamente alinhada à avaliação contextual e contínua dos riscos envolvidos no tratamento de dados pessoais.

No escopo de aplicação da LGPD, por exemplo, a própria definição de dado anonimizado revela esse movimento. A lei adota uma conceituação aberta, segundo a qual o dado é considerado anônimo quando ele não pode identificar um titular, considerando a utilização de “meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (art 5º, III, LGPD). Isso transfere ao agente a responsabilidade de avaliar, no caso concreto e na contemporaneidade, se um dado pode ser considerado efetivamente anonimizado. Trata-se de uma decisão que produz o efeito de fazer incidir ou não a LGPD sem necessariamente exigir uma validação prévia da Agência Nacional de Proteção de Dados (ANPD).

A base legal do legítimo interesse segue lógica semelhante (art.10 LGPD). Ao permitir o tratamento com fundamento em interesse legítimo do controlador ou de terceiros, a LGPD exige uma análise que envolve a ponderação entre finalidades do tratamento e impactos sobre direitos e liberdades fundamentais dos titulares. Essa operação, essencialmente contextual do tratamento de dados, não é previamente definida pela lei, mas construída pelo agente de tratamento, que deve documentar e justificar sua decisão, especialmente à luz de legítimas expectativas dos titulares. Ou seja, a legislação estabelece os parâmetros pelos quais os agentes de tratamento devem se guiar e realizar a ponderação de interesses, mas não condiciona essa avaliação a uma aprovação de um órgão regulador ou pré-determina hipóteses exaustivas da utilização desta base legal.

No caso em questão, o princípio da boa-fé tem papel essencial em estabelecer deveres de informação e lealdade com o titular dos dados, o que permite verificar quais são as legítimas expectativas dele. Por exemplo, se o tratamento é intrusivo ou não, se há transparência quanto ao tipo de tratamento realizado, se é possível a esse titular exercer os seus direitos, bem como da presença de documentação adequada para concretizar essa expectativa do titular em relação ao tratamento (ANPD, 2024).

No campo das transferências internacionais de dados também temos algo parecido. Embora a lei estabeleça como regra a transferência para países com nível adequado de proteção, ela admite que agentes de tratamento possam comprovar o atendimento a um grau adequado de proteção de dados por meio da adoção de cláusulas contratuais, normas corporativas globais, certificações e outros instrumentos (art. 33, II LGPD). Mesmo na ausência de um nível de proteção de dados considerado adequado, admite-se que práticas de agentes de tratamento bem estruturadas possam assegurar a conformidade com os princípios e disposições da proteção de dados.

Esses exemplos mostram que a LGPD organiza um sistema no qual os agentes de tratamento promovem decisões sobre o uso de dados pessoais orientadas por risco. Instrumentos como

códigos de conduta, certificações, testes de balanceamento e, especialmente, o Relatório de Impacto à Proteção de Dados, funcionam como mecanismos que estruturam, documentam e tornam controlável esse exercício de avaliação constante. Dessa forma, a abordagem de regulação de risco se concretiza não apenas na identificação de perigos abstratos, mas na exigência de que o agente avalie, justifique e mitigue, de forma contínua, os riscos decorrentes de suas atividades de tratamento.

Mas a questão sobre o que significa risco nesse contexto permanece aberta. Essa é a mesma questão que Gellert (2017) aborda em *Understanding the notion of risk in the General Data Protection Regulation*. Ao enfrentar esse problema, Gellert (2017) elabora inicialmente dois conceitos de risco. Em seu sentido vernacular, essa relação costuma estar associada à previsão de consequências negativas, isto é, à antecipação de danos ou prejuízos decorrentes de determinada ação. Já em um sentido técnico, o risco envolve a previsão de consequências, sejam elas positivas ou negativas, e a adoção de medidas em relação a essas consequências previstas.

No contexto específico da proteção de dados, Gellert (2017) identifica uma inflexão relevante: o risco passa a ser definido como a possibilidade de impacto sobre direitos e liberdades fundamentais dos titulares. Trata-se, portanto, de um deslocamento em relação a compreensões meramente regulatórias ou organizacionais do risco, centradas, por exemplo, em riscos de não conformidade. O foco da análise passa a recair sobre os efeitos concretos do tratamento de dados sobre os direitos dos indivíduos.

Essa distinção permite compreender que, no âmbito da GDPR, a análise de conformidade regulatória não seja a mesma coisa que a análise de risco, embora ambas estejam profundamente conectadas. Contudo, como destaca Gellert (2017), diversas manifestações de autoridades de proteção de dados e entendimentos da Working Party 29 e outros considerandos da GDPR tendem (apesar de diversas inconsistências) ao entendimento de que a conformidade jurídica integra a análise de risco na medida em que a violação das disposições legais pode representar, por si só, uma fonte de risco aos direitos dos titulares. No entanto, a conformidade não esgota a avaliação de risco: um tratamento pode estar adequado à lei e, ainda assim, gerar riscos aos direitos dos titulares, assim como a adoção de medidas de conformidade pode reduzir tais riscos a níveis considerados aceitáveis, sem eliminá-los por completo. Em outras palavras, o risco é algo inerente ao tratamento de dados pessoais.

A partir dessa construção, Gellert (2017) enfatiza a importância dos procedimentos e metodologias que permitem identificá-lo, avaliá-lo e tratá-lo. Nesse sentido, falar em risco no contexto de instrumentos como o DPIA e RIPD implica designar um conceito (risco como os potenciais impactos sobre direitos fundamentais de titulares) ao mesmo tempo que aponta para um conjunto de práticas e metodologias voltadas à sua operacionalização.

É justamente nesse ponto que se esclarece o papel da abordagem baseada em risco no direito à proteção de dados. Essa abordagem não autoriza o agente de tratamento a escolher se e quando cumprirá determinadas disposições legais em função do nível de risco identificado, mas de permitir que disposições abertas e gerais do tratamento de dados sejam concretizadas a partir de uma análise contextual das atividades de tratamento.

A avaliação de risco, nesse cenário, funciona como o mecanismo por meio do qual o agente de tratamento especifica e materializa os comandos normativos da lei. Ao identificar os possíveis impactos de suas operações sobre direitos e liberdades dos titulares, o agente é levado a interpretar, justificar e implementar medidas concretas de conformidade, ajustadas às particularidades do caso. Por essa razão, longe de representar um enfraquecimento da regulação, a abordagem baseada em risco tende a atuar como um vetor de intensificação da conformidade, na medida em que exige um engajamento ativo e contínuo dos agentes com os objetivos substantivos da proteção de dados. Muito embora a análise de Gellert (2017) esclareça o papel do risco em normas de proteção de dados, seu olhar é dedicado às disposições da GDPR e não abarca a LGPD.

Essa questão é aprofundada por Maria Cecília Gomes (2020) em *Entre o método e a complexidade: compreendendo a noção de risco na LGPD*. No artigo, a autora busca explicar a complexidade existente na noção de risco e seu sentido no âmbito da LGPD. Na questão do risco de forma ampla, Gomes (2020) estabelece diálogo com Gellert (2017) e concorda que a metodologia pelo qual um risco se torna visível é mais importante do que o conceito de risco em si. Principalmente quando a tomada de decisão frente ao risco é feita a partir da perspectiva pessoal do agente, não por meio de uma metodologia técnico-científica.

D

Contudo, ela demonstra a importância das metodologias por um caminho distinto, destacando como os modos pelos quais conceituamos o risco e as decisões tomadas a partir dele podem levar a crimes contra humanidade e violações sistemáticas de direitos humanos (Gomes, 2020). Essa perspectiva é ilustrada, por exemplo, pelo caso do Social Security Act, no qual a coleta de dados voltada à assistência social acabou intensificando a discriminação de grupos vulneráveis, e pelos censos populacionais holandeses, posteriormente instrumentalizados pelo regime nazista na perseguição de judeus. Dessa forma, a análise do risco precisa levar em consideração a redistribuição do risco para agentes afetados pelas atividades de tratamento.

Esse é o perigo que também está por trás de uma análise de risco que seja entendida como uma análise de risco regulatória na LGPD. Segundo a autora, esse tipo de entendimento faz com que a análise de riscos em proteção de dados seja predominantemente “[...] voltada ao risco (regulatório) da organização que trata dados pessoais, do que um exercício de mensuração dos possíveis efeitos adversos para o titular dos dados” (Gomes, 2020, p. 259). O que pode aumentar as chances de redistribuição dos riscos do tratamento para os titulares.

No caso da LGPD o risco não tem um conceito fechado, contudo, ele também não está conectado com o risco regulatório apenas. Em todas as menções na Lei, o risco aparece predominantemente relacionado com o RIPD e medidas de governança (Gomes, 2020).

O

Quadro 1 – Menções a risco na Lei Geral de Proteção de Dados

Indicação na Lei	Matéria	Quantas vezes é mencionado	Está relacionado à governança?
Art. 5º, XVII	Relatório de Impacto à Proteção de Dados Pessoais	2	Sim
Art. 11, § 5º	Tratamento de dados sensíveis – grupos de risco classificados pelas operadoras de planos privados de assistência à saúde	1	Não
Art. 38, parágrafo único	Relatório de Impacto à Proteção de Dados Pessoais	1	Sim
Art. 44, II	Responsabilidade dos Agentes de Tratamento	1	Sim
Art. 48, caput; Art. 48, § 1º, IV	Segurança	2	Sim
Art. 50, caput; Art. 50, § 1º; Art. 50, I, alínea “d”	Governança	3	Sim
Art. 55–J, § 2º, XIII	Obrigações da ANPD e Relatório de Impacto à Proteção de Dados Pessoais	1	Sim

Fonte: Gomes (2020, p. 262–263).

Dessa forma, o risco na LGPD permeia toda legislação, mas em diferentes contextos. Alguns casos estão relacionados à conformidade legal, como no caso do teste do legítimo interesse (LIA), e em outros voltados para análise de riscos a liberdades civis e direitos fundamentais, como no caso do RIPD. e isso o conecta com seu principal referencial: os riscos *‘às liberdades civis e aos direitos fundamentais’* dos titulares. Como o risco está condicionado às metodologias que o tornem visível, a principal preocupação deve ser se o referencial da metodologia adotada, seja ela qual for, é o titular de dados. Nas palavras de Gomes (2020, p. 265):

Portanto, o que será avaliado durante a realização da avaliação de impacto ou, especificamente, a avaliação de risco, é qual é a matriz de risco envolvida que está relacionada às liberdades civis e aos direitos fundamentais das pessoas naturais que são os titulares de dados (grifos nossos).

De qualquer forma, o RIPD é a principal ferramenta criada pela LGPD para que os agentes de tratamento façam uma análise mais detida das atividades de tratamento que tenha potencial de gerar maior risco para os direitos fundamentais dos titulares de dados. Portanto, para que o RIPD mobilize adequadamente a noção de risco a qual ele se presta, ele precisa adotar uma metodologia adequada. Para entender melhor metodologias de análise de risco, é preciso entender efetivamente o instrumento importante de análise de riscos da LGPD, o Relatório de Impacto à Proteção de Dados (RIPD).

2.2 INTRODUÇÃO AO RIPD

Se o sentido de risco na LGPD é predominantemente conectado ao RIPD, as metodologias de análise dele precisam levar em conta os contornos conceituais e institucionais do relatório. Esse instrumento faz parte de uma necessidade em um contexto onde leis de proteção de dados tanto no Brasil quanto na Europa entendem que a atividade de tratamento de dados é uma atividade de risco. Isso significa dizer que o manuseio de dados pessoais carrega a possibilidade de provocar consequências para os direitos de titulares de dados. É nesse sentido que muitas das disposições da LGPD visam à prevenção dos riscos e à adoção de medidas que consigam *mapeá-los, mitigá-los e, quem sabe, até eliminá-los*.

O RIPD, previsto no art. 5º, inciso XVII da LGPD, consiste em uma documentação elaborada pelo controlador que descreve os processos de tratamento de dados pessoais que podem gerar riscos aos titulares de dados, além de apresentar medidas, salvaguardas e mecanismos de mitigação desses riscos. Apesar de poder ser destinado à avaliação de riscos, o RIPD só é obrigatório para atividades de alto risco ou por meio de requisição da ANPD (art. 55-J, inciso XIII c/c art. 38 da LGPD). No caso das atividades de alto risco, o relatório precisa ser realizado anteriormente ao início do tratamento.

De acordo com Maciel e Gomes (2023), o RIPD tem como objetivo principal prevenir e mitigar riscos aos direitos dos titulares e não avaliar e mapear riscos regulatórios ou organizacionais que o controlador está sujeito. Essa interpretação está de acordo com a definição legal onde o relatório é uma documentação que descreve “[...] **processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais**” (Maciel; Gomes, 2023, p. 3, grifos nossos).

Para além disso, Gomes (2019) destaca que o relatório deve refletir a avaliação de impacto feita pelo controlador, expondo o processo pelo qual o agente de tratamento considerou os riscos de sua atividade e as ações tomadas em relação a eles. Tais avaliações de impacto podem ser usadas, por exemplo, para analisar o risco de incidentes de segurança, novas tecnologias ou produtos que possam gerar riscos aos titulares.

O RIPD também pode ser uma ferramenta de prestação de contas (accountability) em observação ao princípio previsto no artigo 6º, X da LGPD. O RIPD pode demonstrar que o controlador avaliou sua cadeia de tratamento de dados, adotando medidas para proteger os direitos dos titulares. Esse entendimento também foi publicado no Enunciado 679 da IX Jornada de Direito Civil:

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser entendido como uma medida de prevenção e de accountability para qualquer operação de tratamento de dados considerada de “alto risco”, tendo sempre como parâmetro o risco aos direitos dos titulares.

Tal entendimento também é reforçado pela prática da Agência Nacional de Proteção de Dados em solicitar a realização e apresentação de RIPD em diversas ações de fiscalização. No caso dos Microdados do Inep (Nota Técnica nº 46/2022/CGF/ANPD), cadastro e tratamento de dados de crianças e adolescentes no TikTok (Nota Técnica nº 6/2023/CGF/ANPD), o uso de dados pessoais para treinamento de inteligência artificial da Meta AI, (Voto nº 11/2024/DIR-MW/CD), a agência exigiu a apresentação de versão pública do RIPD justamente para tornar possível o controle social das escolhas feitas por esses agentes de tratamento sobre o sopesamento de riscos do tratamento de dados.

Nesse sentido, é possível ver que o RIPD desempenha funções conectadas a análise de riscos aos direitos fundamentais de titulares, bem como de prestação de contas da análise do controlador dos riscos relacionados ao tratamento de dados.

2.3 REQUISITOS E MELHORES PRÁTICAS NA ELABORAÇÃO DE UM RIPD

Para entender melhor quais os requisitos para a elaboração do RIPD, é preciso entender como sua própria definição na LGPD leva a deveres de registro e análise de riscos. Em *Relatório de Impacto à Proteção de Dados. Uma breve análise da sua definição e papel na LGPD*, Gomes (2019) sugere que o RIPD pode ser dividido em três eixos principais: 1) documentação do controlador; 2) descrição dos processos de tratamento e; 3) Medidas, salvaguardas e mecanismos de mitigação desses riscos.

Em relação ao primeiro, o RIPD deve ser um documento formal, elaborado pelo controlador, que atenda aos critérios estabelecidos pela LGPD. Embora a lei associe o RIPD ao controlador, uma interpretação sistemática sugere que operadores também podem elaborá-lo, dependendo das atividades de tratamento que realizam (Gomes, 2019). Afinal, ambos podem fazer o relatório em benefício de suas atividades de tratamento (Gomes, 2019).

Em segundo lugar, a LGPD não exige expressamente que o RIPD seja público, mas sua divulgação pode demonstrar transparência e compromisso com a proteção de dados (ANPD, 2023). Além disso, por se tratar de um instrumento de prestação de contas, a publicização do RIPD é uma forma de o controlador materializar este princípio e colocar a avaliação de risco realizada por ele, bem como as consequentes medidas de mitigação deste risco, sob escrutínio dos titulares, órgãos reguladores e terceiros.

No caso de órgãos públicos, essa questão deve ser analisada à luz do regime constitucional da publicidade e da transparência administrativa. O princípio da publicidade dos atos administrativos, previsto no art. 37 da Constituição, aliado às diretrizes da Lei de Acesso à Informação (Lei nº 12.527/2011) (Brasil, 2011), impõe como regra a divulgação de informações de interesse

coletivo, admitindo sigilo apenas em hipóteses excepcionais e legalmente fundamentadas. A publicação é obrigatória desde que não haja justificativa legal para sigilo e quando determinada pela ANPD. (art 32 da LGPD c/c Lei de Acesso à Informação nº 12.527, de 18 de novembro de 2011).

Em outras situações, a ANPD tem reiteradamente demandado a elaboração e apresentação de versão pública de Relatórios de Impacto à Proteção de Dados (RIPD) em diferentes processos de fiscalização. No caso dos Microdados do Inep (Nota Técnica nº 46/2022/CGF/ANPD), cadastro e tratamento de dados de crianças e adolescentes no TikTok (Nota Técnica nº 6/2023/CGF/ANPD), o uso de dados pessoais para treinamento de inteligência artificial da Meta AI, (Voto nº 11/2024/DIR-MW/CD), a agência exigiu a apresentação de versão pública do RIPD justamente para tornar possível o controle social das escolhas feitas por esses agentes de tratamento sobre o sopesamento de riscos do tratamento de dados.

Nesse contexto, o RIPD não pode ser compreendido apenas como um documento interno de governança, mas como um mecanismo de prestação de contas que concretiza a transparência pública. A elaboração de uma versão pública do relatório, ainda que com eventual adaptação para evitar exposição protegida por sigilo, decorre diretamente desse dever de publicidade, permitindo o controle social sobre a adequação das decisões tomadas pelo controlador.

Diante desse conjunto de entendimentos, é possível sustentar que, embora a LGPD não imponha expressamente a obrigatoriedade de divulgação pública do RIPD, a prática regulatória da ANPD vem consolidando a compreensão de que esse instrumento não se esgota em uma avaliação interna do controlador. Ao contrário, o RIPD assume função típica de prestação de contas, servindo não apenas à autoridade, mas também ao escrutínio público, o que reforça a necessidade de desenvolvimento de versões públicas capazes de materializar a transparência e permitir o controle social sobre a gestão de riscos realizada pelo controlador.

Neste sentido, a publicização do relatório de impacto à proteção de dados, especialmente àqueles elaborados por órgãos públicos e em atividades de tratamento de dados vinculadas à realização de políticas públicas, deve receber especial atenção. Isso significa que a divulgação de uma versão pública do RIPD não se deve limitar a uma análise de quais informações devem ser ocultadas para proteger segredos de negócio e informações que poderiam ser usadas abusivamente por agentes maliciosos, mas sim na criação de um documento que efetivamente informe ao público a autoavaliação feita pelo agente de tratamento e as maneiras que este encontrou para reduzir os riscos encontrados. Em outras palavras, existem formas mais sofisticadas de manejar transparência e segredos do que a decisão binária de revelar ou ocultar uma informação, passando por técnicas de generalização da descrição dos riscos mapeados de forma a não expor informações sensíveis.

Já com relação ao segundo eixo, o RIPD deve descrever os tratamentos de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais. Isso envolve uma análise detalhada de como os dados são tratados, incluindo fluxos de compartilhamento de dados, fontes de dados, objetivos da atividade de tratamento e riscos atuais (Gomes, 2019).

De acordo com o art. 38 da LGPD, o RIPD deverá conter: a) a descrição dos tipos de dados

— pessoais coletados ou tratados de qualquer forma; b) a metodologia usada para o tratamento e para a garantia da segurança das informações; e c) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

D É importante que o relatório seja suficientemente detalhado, para que a ANPD, os titulares e o próprio controlador tenham compreensão ampla de como ocorre o tratamento dos dados pessoais e os possíveis riscos associados a ele. Gomes sugere que a descrição do tratamento de dados deve responder a perguntas: como eles funcionam internamente em relação aos “tratamentos e fluxo de dados interno?”; “a forma como o agente de tratamento trata esses dados hoje é capaz de gerar riscos atuais?” (Gomes, 2019, p. 10-11).

A partir da combinação da LGPD com as contribuições da ANPD, Santos (2025) demonstra que é possível traçar um caminho para a descrição dos riscos no RIPD. Primeiramente, o RIPD deve identificar os agentes de tratamento e o encarregado. Isso inclui informações sobre o controlador ou operador, caso exista. Além disso, deve ser identificado o encarregado pelo tratamento de dados pessoais (DPO), responsável pela comunicação entre o controlador, os titulares e a ANPD. Além disso, é importante informar se outras partes interessadas/envolvidas foram consultadas na elaboração do RIPD e pareceres emitidos;

O relatório também deve descrever os processos de tratamento de dados, especificando os 1) tipos de dados tratados, como nome, CPF, endereço e e-mail, além de dados sensíveis, como dados de saúde, orientação sexual e convicções religiosas. Deve-se identificar as 2) categorias de titulares, como clientes, funcionários, idosos, crianças e adolescentes e justificar a 3) finalidade do tratamento. Também deve-se indicar a 4) fonte da coleta dos dados. Além disso, é necessário apresentar a 5) base legal que fundamenta o tratamento ou cada tratamento analisado e uma 6) análise dos princípios da LGPD.

Outras informações, como a estimativa do 7) volume de dados tratados e do número de titulares envolvidos, detalhes sobre o 8) compartilhamento de dados, incluindo 9) transferências internacionais e a 10) política de armazenamento com prazos de retenção e métodos de descarte são relevantes para a devida descrição do tratamento de dados.

Outro ponto essencial do RIPD é a descrição da metodologia utilizada para a análise dos riscos, detalhando as técnicas e processos aplicados ao tratamento de dados, bem como as medidas de segurança adotadas. Como vimos, a centralidade da metodologia não decorre apenas de uma exigência formal de organização do relatório, mas da própria forma pela qual o risco se torna visível no âmbito da proteção de dados.

— Nesse sentido, tanto Gellert (2017) quanto Gomes (2020) convergem ao indicar que o risco, por si só, não é um dado objetivo imediatamente acessível, mas uma construção dependente dos instrumentos analíticos utilizados para identificá-lo e avaliá-lo. Em Gellert (2017), isso se manifesta na ênfase sobre a necessidade de procedimentos capazes de traduzir a noção abstrata do impacto sobre direitos e liberdades fundamentais em categorias operacionais, que permitam sua identificação e tratamento. Já em Gomes (2020), essa preocupação tem uma dimensão crítica ao evidenciar que diferentes metodologias podem não apenas revelar riscos distintos, mas também produzir efeitos distributivos desiguais, deslocando ou invisibilizando

impactos sobre determinados grupos de titulares.

A consequência direta dessa compreensão é que a escolha metodológica adotada no RIPD condiciona quais riscos serão reconhecidos, como serão classificados e quais medidas serão consideradas adequadas para sua mitigação. Uma metodologia orientada predominantemente por parâmetros organizacionais ou de conformidade regulatória tende a privilegiar riscos institucionais, como sanções e danos reputacionais, em detrimento dos impactos concretos sobre os titulares. Por outro lado, uma abordagem que adota como referencial os direitos e liberdades fundamentais exige que a análise de risco seja construída a partir dos possíveis efeitos do tratamento sobre a vida dos indivíduos, considerando contextos de vulnerabilidade, assimetrias informacionais e potenciais externalidades negativas.

Todavia, a descrição da metodologia no RIPD tem outras funções para além da identificação de riscos. Tal descrição permite avaliar a consistência técnica da análise realizada pelo controlador, possibilitando que a ANPD e outros atores verifiquem a adequação dos critérios utilizados. De outro, pode viabilizar o controle social sobre as escolhas feitas no caso de um RIPD que seja publicamente disponível. Nesse sentido, a metodologia não se trata apenas de indicar ferramentas ou matrizes de risco, mas de *explicar os pressupostos, os critérios de avaliação e os limites da própria análise*.

Por essa razão, a metodologia deve ser capaz de articular, de forma coerente, a identificação de riscos, a avaliação de impactos sobre os titulares e a definição de medidas de mitigação, garantindo que o risco da atividade de tratamento mínimo e compatível com a proteção dos direitos fundamentais. Em última análise, é por meio dessa estrutura metodológica que o RIPD consegue cumprir sua função de materializar a abordagem baseada em risco da LGPD, transformando conceitos jurídicos abertos em decisões concretas, justificadas e passíveis de escrutínio.

Com relação ao terceiro eixo, sobre medidas, salvaguardas e mecanismos de mitigação de riscos, o RIPD deve apresentar ações afirmativas do controlador para gerenciar os riscos identificados. A partir das recomendações da ANPD, o relatório deve apresentar as medidas adotadas, como a minimização da coleta de dados, por exemplo. Além disso, devem ser descritas as salvaguardas técnicas e organizacionais, como firewalls, treinamentos e políticas de acesso, bem como os mecanismos de monitoramento contínuo dos riscos.

No entanto, a compreensão dessas medidas não deve se limitar a um repertório restrito de práticas de segurança da informação ou de proteção de dados em sentido estrito. A partir da abordagem baseada em risco, especialmente quando orientada pelos impactos sobre direitos e liberdades fundamentais, as estratégias de mitigação devem ser pensadas de forma mais ampla e contextualizada, considerando a própria configuração da atividade de tratamento e suas implicações sociais.

Nesse sentido, a contribuição de Gellert (2017) e Gomes (2020) são particularmente relevantes ao indicar que o risco diz respeito aos efeitos concretos do tratamento sobre os titulares. Isso implica reconhecer que as medidas de mitigação não podem se restringir a mecanismos internos de controle, devendo também abranger alterações na própria arquitetura do trata-

mento, nas finalidades perseguidas e, em alguns casos, na própria necessidade da atividade.

Um exemplo ilustrativo pode ser observado em sistemas de reconhecimento biométrico para controle de acesso a edifícios. Embora seja possível mitigar riscos por meio de medidas clássicas, como criptografia, controle de acesso e limitação de retenção de dados, uma análise orientada a direitos fundamentais pode indicar a necessidade de adoção de mecanismos alternativos de acesso, como cartões físicos ou autenticação multifatorial não biométrica. Isso porque, ainda que o sistema seja o mais seguro do ponto de vista da garantia da confidencialidade dos dados tratados, outros direitos como a autodeterminação informativa e o princípio da necessidade exigem meios alternativos de autenticação para acesso à própria casa em um condomínio. Nesse caso, a redução da exposição dos titulares a uma tecnologia potencialmente intrusiva ocorre pelo oferecimento de uma alternativa menos intrusiva para o morador.

Essa perspectiva evidencia dois pontos centrais. Primeiro, que os riscos mapeados no RIPD devem ultrapassar a dimensão estritamente informacional, incorporando impactos mais amplos sobre direitos fundamentais. Segundo, que, em razão disso, as medidas de salvaguarda também devem ser concebidas para além de soluções típicas de proteção de dados, podendo envolver decisões estruturais sobre o desenho da política, do serviço ou da tecnologia adotada.

Essa abordagem é reforçada pela experiência internacional. A Agência Espanhola de Proteção de Dados destaca que as medidas de mitigação devem ser analisadas de forma contextualizada ao ciclo de vida do tratamento de dados, considerando as diferentes fases do fluxo de dados, desde a coleta até o descarte (AEPD, 2021). Isso implica que a mitigação não é um momento isolado, mas um processo contínuo que acompanha toda a operação de tratamento, exigindo revisões periódicas e adaptações conforme mudanças no contexto ou na tecnologia utilizada.

Além disso, a Agência amplia a noção de mitigação ao incorporar elementos robustos de governança e accountability, especialmente na relação entre controlador e operador (AEPD, 2021). Nesse sentido, ganham relevância mecanismos contratuais que estabelecem padrões de segurança, critérios de seleção de operadores com garantias suficientes de proteção de dados, auditorias periódicas, revisões independentes e mecanismos de rastreabilidade das operações de tratamento, incluindo o controle de comunicações de dados e transferências internacionais.

Dessa forma, as medidas, salvaguardas e mecanismos de mitigação no RIPD devem ser compreendidos como um conjunto articulado de respostas que vão desde controles técnicos até decisões estruturais sobre o próprio tratamento de dados. Mais do que um checklist de conformidade, trata-se de um exercício de governança que busca reduzir, de maneira efetiva, os riscos aos direitos dos titulares, ao mesmo tempo em que torna essas escolhas transparentes, justificáveis e passíveis de controle.

A partir dessa análise, o RIPD deve trazer uma síntese dos resultados, indicando o novo nível do risco avaliado, após a implementação das medidas de mitigação e, a partir deste novo risco (risco residual), decidir se este risco residual apresenta um nível aceitável para que a atividade de tratamento possa prosseguir, ou, caso contrário, determinar a interrupção daquela atividade.

de até que outras formas mais eficazes de mitigação de risco possam ser implementadas. O documento também pode conter pareceres internos das áreas envolvidas, como jurídico, da Tecnologia da Informação (TI) e compliance, além da aprovação formal dos responsáveis pela sua elaboração e revisão.

03 RISCOS E BENEFÍCIOS

03 RISCOS E BENEFÍCIOS

3.1 METODOLOGIAS DE ANÁLISE DE RISCO

Nos capítulos anteriores, demonstramos que o risco não é um dado imediatamente evidente ou um elemento puramente objetivo da atividade de tratamento no contexto do Relatório de Impacto à Proteção de Dados. Na verdade, o risco só se torna visível a partir de escolhas metodológicas que orientam a identificação dos possíveis impactos sobre direitos e liberdades fundamentais de titulares e a definição das medidas de mitigação adequadas. Por isso, compreender metodologias de análise de risco é etapa indispensável para avaliar como o RIPD pode cumprir sua função de proteção efetiva dos titulares de dados.

Essa constatação é relevante na medida em que não existe uma única metodologia de análise de risco aplicável à proteção de dados pessoais. Diferentes modelos podem partir de pressupostos distintos, privilegiar variáveis diversas e produzir formas de compreender o que deve ser protegido.

Assim, este subcapítulo analisa três abordagens metodológicas relevantes para a avaliação de riscos em proteção de dados pessoais. A primeira corresponde ao modelo mais recorrente de matriz de risco, baseado na combinação entre probabilidade de ocorrência e impacto do risco. A segunda refere-se à avaliação de impacto baseada em direitos humanos desenvolvida por Alessandro Mantelero, que direciona o foco da análise para os efeitos do tratamento sobre pessoas, grupos e direitos fundamentais. A terceira consiste na metodologia de gestão de riscos do NIST *Privacy Framework*, voltada à incorporação e aprimoramento da privacidade em processos organizacionais.

A análise dessas metodologias permitirá compreender que a escolha do método condiciona quais riscos serão percebidos, quais impactos serão considerados relevantes e quais respostas serão reputadas suficientes. Em outras palavras, a análise permitirá descrever o 'Paradigma' pelo qual os riscos são percebidos e impedem com que a análise seja excessivamente subjetiva.

O uso do termo '*Paradigma*' nesse contexto é similar ao utilizado por Thomas Kuhn em "*A Estrutura das Revoluções Científicas*". De acordo com a historiografia da ciência avaliada por Kuhn (2018), os paradigmas são conjuntos de pressupostos pelos quais uma ciência se torna possível. Da mesma forma, a análise das metodologias de análise de risco permite ver o conjunto de pressupostos pelos quais a comunidade de governança de dados adotou para visualizar as atividades de tratamento de dados bem como seus riscos possíveis. Não se trata de descobrir a 'teoria' de análise dos riscos, mas de entender seus pressupostos e limitações.

Probabilidade e impacto

Talvez a matriz de risco mais comum seja a de probabilidade x impacto. Nesse tipo de metodologia, busca-se avaliar o risco de um tratamento a partir da probabilidade de sua ocorrência e seu impacto caso ocorra. Quanto maior a probabilidade e impacto, maior o risco. Essa definição do risco pode ser resumida na seguinte operação:

$$\text{Risco} = \text{Probabilidade (P)} \times \text{Impacto (I)}$$

De acordo com esse desenho metodológico, primeiro se estabelece o risco corrente de uma atividade de tratamento e na sequência define-se medidas de mitigação ou eliminação dos riscos. Uma vez definido as medidas, é preciso realizar novamente uma avaliação do grau do risco de forma a tornar possível a decisão do responsável pelo tratamento de dados de continuar ou não com aquela atividade de tratamento.

Na maioria dos casos a probabilidade é determinada com base nas possibilidades existentes de materialização do risco. Já o impacto é determinado com base no efeitos que o risco pode ter no titular de dados afetados. Tanto probabilidade quanto impacto são classificados em escalas que geralmente estabelece o que pode ser considerado uma probabilidade e impactos alto e baixo.

Por ser um método de avaliação qualitativo e valorativo do risco, uma das limitações desse método é a dificuldade de quantificação (Gomes, 2020). Ao invés de termos uma operação matemática ou categorias fixas de riscos, se busca falar “[...] em classificações de risco como (muito) alto, médio e baixo, mas não em termos de quantificação, de forma a definir os níveis adequados, aceitáveis e inaceitáveis” (Silva, 2023, p. 61).

No Brasil, o *Guia/Modelo de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais* elaborado pelo Ministério da Gestão e da Inovação em Serviços Públicos (Brasil, 2023) divide os riscos em uma escala 3x3 cuja classificação fica restrita entre alta, média e baixa. Sendo os valores tidos como baixo o valor (5), os médios, com valor (10) e os altos, com valor 15.

Dessa forma, multiplica-se o valor atribuído ao grau da probabilidade e dos impactos aos titulares de dados pessoais, conforme imagem abaixo:

Figura 1 - Matriz probabilidade x impacto

Probabilidade (P)	Impacto (I)			Fonte: Brasil [2023]
	05	10	15	
	75	150	225	
	50	100	150	
05	25	50	75	

No mesmo guia, os conceitos de probabilidade e impacto são os mesmos da norma ISO/IEC 31000:2009. Nesse sentido, se define a variável probabilidade como a “chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos” (Brasil, 2013, p. 22). Ao passo que o impacto é compreendido como um “resultado de um evento que afeta os objetivos”. Muito embora essas categorias sejam importantes balizas para a definição dos riscos segundo essa metodologia, elas carecem de uma definição mais clara e em escala com as 3 categorias de risco. Nesse sentido, faltam critérios para definir o que seria um impacto ou probabilidade média, baixa ou alta. Afinal, o que faz uma probabilidade ser baixa? Qual tipo de impacto pode ser médio?

Por outro lado, autoridades como a *Agencia de Acceso a la Información Pública de Argentina (AAIP)* e *Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay*, abordam a análise de riscos de uma forma levemente diferente daquela apresentada pelo guia de relatório de impacto brasileiro. O fundamento metodológico permanece o mesmo na hora de avaliar riscos, mas com uma dimensão mais concreta para definir critérios de classificação dos graus de impacto e probabilidade.

□

Nestes documentos, a escala da probabilidade de probabilidade e impacto do risco tem sua classificação dividida em 4: baixa, média, alta e muito alta. Além disso, existem descrições de critérios para considerar uma probabilidade ou impactos de acordo com as 4 classificações.

A probabilidade é definida como a chance do risco se concretizar no tempo. Nesse sentido, uma probabilidade baixa representa que o risco pode acontecer em circunstâncias excepcionais, ao passo que tanto a probabilidade alta quanto muito alta manifestam a possibilidade do risco de se concretizar pelo menos uma vez ou várias vezes ao ano.

Já em relação ao impacto, se define a variável enquanto a medida do quão um risco afeta o titular de dados e qual a dificuldade de superar determinada situação gerada pela concretização do risco.

Quadro 2 - Matriz de risco de probabilidade inspirada em autoridades do Uruguai e Argentina

	BAIXA	MÉDIA	ALTA	MUITO ALTA
PROBABILIDADE	Pode acontecer apenas em circunstâncias excepcionais	É um evento raro e pouco frequente, embora não improvável	É possível que ocorra uma vez ao ano	É possível que ocorra várias vezes ao ano
	BAIXO	MÉDIO	ALTO	MUITO ALTO
IMPACTO	Os titulares dos dados não serão afetados ou sofrerão apenas alguns inconvenientes, que poderão resolver sem muitas dificuldades	Os titulares dos dados serão afetados de forma significativa, podendo superar a situação com alguma dificuldade	Os titulares dos dados serão afetados de forma significativa e só poderão superar a situação com grandes dificuldades	Os titulares dos dados serão afetados com consequências gravíssimas e irreversíveis que talvez não possam superar

□

Fonte: AAIP; URCDP [2020].

Figura 2 – Matriz probabilidade x impacto inspiradas em autoridades do Uruguai e Argentina

P R O B A B I L I D A D E	Muito Alta (3)	4	8	12	16
	Alta (3)	3	6	9	12
	Média (2)	2	4	6	8
	Baixa (1)	1	2	3	4
		Baixa (1)	Média (2)	Alta (3)	Muito Alta (4)
		I M P A C T O			

Fonte: AAIP; URCDP [2020].

Como vimos, a classificação do risco de forma corrente é só a primeira parte da avaliação. Uma vez que tais riscos estão classificados, é preciso escolher medidas de mitigação adequada deles e reavaliar seu grau novamente. Tal metodologia tem a vantagem de operacionalizar a análise de risco pensando de forma concreta na possibilidade de um acontecimento e seus efeitos.

Análise de impacto baseada em direitos humanos

A metodologia de *Human Rights Impact Assessment (HRIA)* desenvolvida por Alessandro Mantelero e Maria Samantha Esposito (2021) parte de uma preocupação semelhante àquela apresentada por Gellert (2017) e Gomes (2020): transformar a referência abstrata a direitos e liberdades fundamentais em uma metodologia capaz de tornar os riscos visíveis e a tomada de decisão baseada neles. No artigo *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*, os autores propõem uma metodologia de avaliação de impacto em direitos humanos voltada especialmente para sistemas de inteligência artificial e aplicações intensivas em dados.

Um dos principais diferenciais dessa metodologia é seu caráter baseado em evidências. Mantelero e Esposito (2021) se basearam em mais de 700 decisões e documentos de autoridades europeias de proteção de dados para identificar, a partir da prática institucional, quais direitos e liberdades já vêm sendo afetados por sistemas intensivos em dados. Essa base empírica foi utilizada no desenvolvimento dessa tecnologia e direciona a principal mudança dessa metodologia, seu foco em como tecnologias de inteligência artificial pode afetar pessoas e grupos.

A metodologia proposta pelos autores é organizada em duas grandes etapas. A primeira é a fase de planejamento e delimitação do escopo. Nessa etapa, deve-se descrever o produto, serviço ou sistema analisado, mapear os fluxos de dados, identificar as finalidades do tratamento, os titulares afetados, os agentes envolvidos, o contexto jurídico aplicável e os agentes (stakeholders)

relevantes. Também devem ser considerados os controles já existentes e a forma como fornecedores, parceiros e terceiros participam da cadeia de tratamento (Mantelero; Esposito, 2021).



A segunda etapa é a coleta e análise de dados. Nela, o avaliador deve identificar quais direitos podem ser afetados pela atividade, estimar a probabilidade e a severidade dos impactos e definir medidas de mitigação. Essa análise abrange qualquer prejuízo ao exercício de direitos e liberdades. Por isso, o risco é compreendido como a possibilidade de uma restrição, limitação ou afetação indevida de direitos fundamentais, ainda que não se traduza imediatamente em dano ou em violação formal de uma obrigação legal. Para operacionalizar essa avaliação, Mantelero e Esposito propõem um modelo mais detalhado do que a matriz simples de probabilidade e impacto.

A probabilidade é descrita em dois elementos: a chance de ocorrência do risco e a exposição, isto é, a quantidade de titulares potencialmente afetados. Já a severidade é composta pela gravidade do prejuízo e pelo esforço necessário para superar ou reverter seus efeitos em um sentido parecido com a variável ‘impacto’ na metodologia de riscos e benefícios.

Figura 3 - Escala do elemento exposição da metodologia

Table 3 – Exposure.		
Exposure		
Low	Few or very few of the identified population of rights-holders are potentially affected	1
Medium	Some of the identified population are potentially affected	2
High	The majority of the identified population is potentially affected	3
Very high	Almost the entire identified population is potentially affected	4



Fonte: Mantelero e Esposito (2021, p. 19).

Com isso, a avaliação passa a considerar não apenas se um risco pode ocorrer, mas também quantas pessoas podem ser afetadas, qual a intensidade do prejuízo e quão difícil será reparar ou mitigar suas consequências (Mantelero; Esposito, 2021). Uma determinada tecnologia de Inteligência Artificial (IA) pode ter baixa probabilidade de gerar determinado impacto, mas atingir um número muito elevado de titulares. Da mesma forma, um risco pode afetar poucas pessoas, mas produzir consequências graves ou de difícil reversão, especialmente quando envolver grupos vulneráveis. A metodologia baseada no impacto aos direitos humanos permite explicitar essas diferenças e permitem uma visualização dos riscos de forma mais completa.



Após a identificação e classificação dos riscos, a metodologia prevê a adoção de medidas de mitigação e a avaliação do risco residual, comparando o risco inicial com o risco residual, permitindo verificar se as salvaguardas propostas são suficientes ou se a atividade deve ser reformulada, restringida ou interrompida (Mantelero; Esposito, 2021).

A metodologia também reforça a importância da participação de stakeholders. Em siste-

mas que afetam direitos fundamentais, a avaliação não deve ser conduzida apenas a partir da perspectiva interna do controlador. A depender do caso, devem ser ouvidos grupos afetados, especialistas, organizações da sociedade civil, autoridades públicas, associações profissionais, fornecedores e outros atores relevantes. Essa participação permite identificar riscos que poderiam permanecer invisíveis em uma análise puramente organizacional, especialmente quando o tratamento afeta grupos vulneráveis ou produz impactos coletivos.

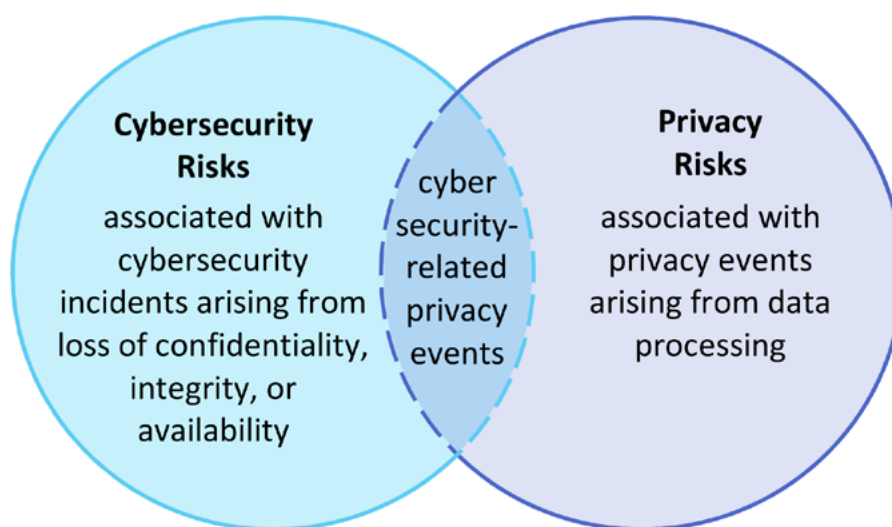
Metodologia *Privacy Framework* do National Institute of Standards and Technology (NIST)

Outra metodologia que pode ser uma inspiração relevante para a análise de riscos em proteção de dados é a do National Institute of Standards and Technology (NIST) chamada de *Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*. Diferentemente da metodologia de Mantelero, que organiza a avaliação a partir de uma perspectiva mais diretamente orientada por direitos humanos, o NIST *Privacy Framework* parte de uma abordagem de gestão organizacional de riscos de privacidade. Seu objetivo é oferecer uma ferramenta flexível, voluntária e adaptável a diferentes organizações, setores, tecnologias e jurisdições, permitindo que a privacidade seja incorporada ao desenho, desenvolvimento e operação de sistemas, produtos e serviços. Tal ferramenta tem um direcionamento para impactos da organização e menos nos impactos para os titulares. Nesse sentido, ainda que formalmente essa metodologia possa ser útil para pensar a análise de riscos no contexto de um RIPD, ela precisa ser adaptada para privilegiar a análise de riscos dos titulares e não dos riscos da organização.

O documento do NIST parte da constatação de que os benefícios decorrentes do uso de dados convivem com potenciais consequências negativas para indivíduos, sociedade e organizações. Para a instituição, indivíduos muitas vezes não conseguem compreender plenamente as consequências do tratamento de seus dados, ao passo que as organizações também podem não perceber a extensão desses efeitos sobre pessoas, grupos e sobre sua própria atividade institucional. Por isso, o framework busca apoiar práticas de *privacy by design*, facilitar o cumprimento de obrigações regulatórias e melhorar a comunicação sobre práticas de privacidade entre organizações, titulares, parceiros comerciais, avaliadores e reguladores (NIST, 2020).

Um ponto central da metodologia é a distinção entre risco de privacidade e risco de segurança cibernética (NIST, 2020). Embora incidentes de segurança possam gerar eventos de privacidade, o NIST destaca que os riscos de privacidade não se limitam à perda de confidencialidade, integridade ou disponibilidade da informação. Eles também podem surgir de operações ordinárias de tratamento de dados, ainda que o sistema esteja funcionando conforme planejado. É por isso que o documento adota a noção de *data action*, isto é, qualquer operação do ciclo de vida dos dados, como coleta, retenção, geração, transformação, uso, compartilhamento, transmissão e descarte. O conjunto dessas ações forma o tratamento de dados (*data processing*).

Figura 4 - Relação entre riscos de privacidade e cibersegurança definidos pelo NIS



Fonte: [NIST, 2020]

A partir dessa perspectiva, o risco de privacidade é compreendido como a probabilidade de que indivíduos experimentem problemas decorrentes do tratamento de dados, combinada com o impacto (NIST, 2020) caso esses problemas ocorram. Esses problemas são chamados de *problematic data actions*, ou ações problemáticas de dados, e podem envolver efeitos diversos, desde constrangimento, estigmatização e sensação de vigilância até consequências mais concretas, como discriminação, perda econômica ou dano físico. A metodologia do NIST amplia a análise para além dos incidentes de segurança e permite considerar situações em que a atividade de tratamento cotidianas podem produzir impactos adversos para os indivíduos.

A estrutura do NIST Privacy Framework é composta por três elementos principais: *Core*, *Profiles* e *Implementation Tiers*. O *Core* reúne atividades e resultados esperados para a gestão de riscos de privacidade, organizados em funções, categorias e subcategorias. Os *Profiles* permitem que a organização compare sua situação atual com o estado desejado de gestão de privacidade, identificando lacunas e prioridades. Já os *Implementation Tiers* indicam o grau de maturidade da organização na gestão de riscos, variando de práticas parciais e reativas até práticas adaptativas, integradas e continuamente aprimoradas.

Essa divisão demonstra que a metodologia do NIST busca estruturar um programa organizacional contínuo de gestão de privacidade, conectando inventário de dados, governança, controles, comunicação e proteção. Nesse sentido, o framework opera quase como uma ferramenta de gestão do ciclo de vida do tratamento de dados, permitindo que a privacidade seja incorporada desde o desenvolvimento de sistemas até sua operação.

A metodologia também atribui papel importante aos *Profiles*. A organização pode construir um perfil atual, que representa as práticas de privacidade já implementadas, e um perfil-alvo, que representa os resultados desejados. A comparação entre esses dois perfis permite identificar lacunas, definir prioridades, estimar recursos necessários e elaborar um plano de ação

(NIST, 2020). Essa lógica permite que a avaliação de riscos avance para a definição de medidas concretas de melhoria, mitigação e monitoramento em um sentido parecido com as metodologias analisadas anteriormente.

Outro elemento relevante são os Implementation Tiers, que indicam o nível de maturidade da organização na gestão de riscos de privacidade. O NIST divide esses níveis em quatro: parcial, informado por risco, repetível e adaptativo (NIST, 2020). No primeiro nível, as práticas tendem a ser informais, reativas e pouco integradas. No segundo, já há consciência organizacional sobre riscos, embora ainda sem abordagem plenamente institucionalizada. No terceiro, os processos são formalizados, revisados e aplicados de forma consistente. No quarto, a organização adapta continuamente suas práticas a novos riscos, tecnologias e aprendizados decorrentes de eventos de privacidade.

Nesse ponto, a metodologia do NIST se aproxima das matrizes de probabilidade e impacto, de forma específica para riscos de privacidade em organizações. Um destaque vai para o aspecto da resposta ao risco. O NIST prevê quatro formas principais de resposta (NIST, 2020): mitigar, transferir ou compartilhar, evitar ou aceitar o risco. A mitigação ocorre quando a organização adota medidas técnicas ou organizacionais para reduzir o risco a um nível aceitável. A transferência ou compartilhamento de riscos pode ocorrer por contratos, avisos de privacidade ou mecanismos de consentimento. A evitação ocorre quando a organização conclui que os riscos superam os benefícios e decide não realizar ou interromper o tratamento. Já a aceitação ocorre quando os problemas esperados são mínimos ou improváveis, de modo que os benefícios justificam a continuidade da atividade.

A contribuição do NIST para a discussão sobre metodologias de risco no RIPD está em oferecer uma perspectiva de gestão de riscos de privacidade orientada à governança organizacional. Ao estruturar essa análise por meio de funções, perfis, níveis de maturidade e respostas ao risco, o NIST oferece uma metodologia útil para fortalecer a governança de organizações e aproximá-lo de uma prática contínua de gestão de riscos de privacidade.

A análise dessas metodologias demonstra que a avaliação de riscos é uma tarefa diversa e no sentido de tornar visíveis os possíveis impactos do tratamento de dados pessoais sobre os titulares de dados. A matriz de probabilidade e impacto permite classificar riscos a partir de sua chance de ocorrência e de seus efeitos; a metodologia de Mantelero amplia essa análise para o campo dos direitos humanos; e o NIST Privacy Framework contribui ao estruturar a análise de risco como uma dimensão da gestão organizacional.

Em iniciativas de transparência pública, a proteção de dados pessoais precisa ser harmonizada com publicidade, o acesso à informação e permitir o controle social. Dessa forma, a proteção de dados não pode ser tratada apenas como um óbice à transparência pública, assim como a transparência não pode ser presumida como automaticamente preponderante sobre os direitos dos titulares.

O desafio metodológico, portanto, está em construir uma avaliação capaz de considerar conjuntamente esses dois valores: transparência pública e proteção de dados pessoais. Ambos possuem relevância jurídica própria e ambos se conectam à proteção de direitos fundamen-

tais. Uma metodologia adequada deve permitir identificar os riscos aos titulares, propor medidas de mitigação e, ao mesmo tempo, explicitar os benefícios públicos esperados da abertura de dados.

É nesse ponto que a metodologia de riscos e benefícios pode ser útil. O objetivo é superar uma lógica binária e “tudo ou nada” entre publicar ou restringir, substituindo-a por uma análise contextual, documentada e proporcional, capaz de maximizar os benefícios da transparência pública e reduzir os riscos do tratamento aos titulares de dados.

3.2 A METODOLOGIA DE RISCOS E BENEFÍCIOS

Os trabalhos analisados por esse relatório que desenharam e aplicaram a metodologia de riscos e benefícios, o fizeram na tentativa de solucionar dificuldades encontradas em programas de dados abertos municipais. Isto pois tais programas precisam lidar com valores diferentes quando a abertura de dados acontece. Por um lado, tais políticas de abertura de dados têm benefícios claros em permitir pesquisa aplicada, desenvolvimento de políticas públicas voltadas ao desenvolvimento do mercado, promoção de direitos e combate à violência. Por outro, a sua divulgação pode afetar negativamente os cidadãos, ao permitir com que informações sobre sua vida sejam facilmente acessíveis, o que por sua vez pode levar a riscos de golpes financeiros, perseguição online, dentre outros.

Dessa forma, é possível dizer que benefícios e risco normalmente caminham juntos em políticas de dados abertos. Nesse sentido, uma metodologia capaz de visualizar essas duas dimensões permite uma tomada de decisão mais consciente, contextual e capaz de maximizar os benefícios e reduzir ou eliminar os riscos.

Em termos esquemáticos, a metodologia de riscos e benefícios propõe dois momentos. O primeiro seria a definição dos graus de risco e benefícios. Como veremos, esses graus são definidos a partir da mesma lógica de metodologias de probabilidade impacto, ou seja, para saber do risco ou de um benefício é preciso ver a probabilidade com que eles podem se materializar e os impactos após a sua materialização.

Risco = Probabilidade (P) x Impacto (I)

Benefício = Probabilidade (P) x Impacto (I)

O segundo momento da análise consiste na comparação entre o grau do benefício e o grau do risco previamente identificados. Essa comparação permite avaliar se a atividade analisada apresenta uma relação justificável entre os efeitos positivos esperados e os efeitos negativos possíveis.

Nesse sentido, quanto maior for o benefício em relação ao risco, menor tende a ser o risco da atividade analisada. Por outro lado, quando o risco e o benefício forem iguais, o risco tende a ser médio e quando o grau do risco supera o do benefício, a atividade deve ser classificada como de risco alto, pois os efeitos positivos esperados não são suficientes para afastar ou compensar adequadamente os possíveis impactos negativos. A razão pode ser explicada no quadro abaixo.

Quadro 3 – Matriz de risco e benefícios

RISCO X BENEFÍCIO		BENEFÍCIO		
		Baixo	Médio	Alto
RISCO	Baixo	Médio risco x benefício	Baixo risco x benefício	Baixo risco x benefício
	Médio	Alto risco x benefício	Médio risco x benefício	Baixo risco x benefício
	Alto	Alto risco x benefício	Alto risco x benefício	Médio risco x benefício

Fonte: Green et al. [2017].

O desenho dessa metodologia foi dado de forma substancial pelos pesquisadores do *Centro de Pesquisa Berkman Klein para Internet e Sociedade*, na publicação '*Open Data Privacy*'. O relatório teve como objetivo oferecer um modo de análise capaz de derivar processos protetivos da privacidade em programas de abertura de dados municipais, a metodologia de riscos e benefícios.

O trabalho parte da premissa das dificuldades de se abrir dados, principalmente da relação entre os riscos à privacidade e os benefícios do acesso aos dados de municípios. Quanto mais detalhado e granular o dado, maior tende a ser seu valor para transparência, pesquisa, inovação e controle social; ao mesmo tempo, maior também tende a ser o risco de reidentificação, inferências indevidas e exposição de informações sensíveis (Green et al., 2017). A título de exemplo, os autores mencionam que a forma como dados sobre violência doméstica são liberados podem aprofundar casos dessa natureza. De acordo com os autores, a liberação descuidada desses dados pode inibir as vítimas de chamarem a polícia em casos de violência por medo de serem identificadas em portais de dados abertos.

Como forma de desenvolver uma metodologia adequada para medir os riscos e benefícios desses programas, os pesquisadores do estudo se inspiraram na estrutura de análise de riscos do National Institute of Standards and Technology (NIST, 2012). Cabe lembrar que essa estrutura não se confunde com a metodologia de análise de riscos em privacidade (NIST, 2020) analisados no capítulo anterior, ela é um modelo para análise de riscos de organizações de forma ampla sem conexão com riscos relacionados a tratamento de dados.

A estrutura do NIST para análise de riscos organizacionais leva em consideração 4 elementos: 1) Vulnerabilidade; 2) fontes de ameaças; 3) eventos de ameaça e; 4) impactos adversos (compostos pela probabilidade e impacto do risco).

A vulnerabilidade (1) corresponde à fragilidade que permite que determinado evento de ameaça produza efeitos negativos. Essa fragilidade pode ser técnica, organizacional, normativa ou procedimental. **As fontes de ameaça (2)**, por sua vez, dizem respeito aos agentes, condições ou circunstâncias capazes de iniciar uma situação de risco. Elas podem envolver agentes externos mal-intencionados ou até mesmo agentes que, por erro ou desconhecimento, podem criar riscos. **Os eventos de ameaça (3)** são os acontecimentos concretos que podem ocorrer a partir dessas fontes de ameaça.

Os impactos adversos (4) representam as consequências negativas resultantes desses eventos, o 'risco'. Tal risco é compreendido a partir da combinação entre a probabilidade de ocorrência do evento e a gravidade do impacto adverso produzido, assim como nas metodologias de análise de riscos de probabilidade e impacto. Embora essa estrutura funcione para a análise de riscos, os pesquisadores do instituto Berkman Klein propuseram a repetição dessa estrutura para os riscos e a inspiração do mesmo processo para a medição de benefícios.

Os pesquisadores adaptaram esses momentos para a análise de riscos e benefícios. Para a análise dos benefícios, a metodologia define 4 momentos: vantagens (1), eventos de vantagem (2), fontes de vantagem (3) e o grau do benefício (4), composto pela probabilidade de sua ocorrência e seu impacto. No caso dos riscos, os elementos são quase os mesmos da estrutura do NIST: vulnerabilidades (1), eventos de ameaça (2), fontes de ameaça (3) e grau do risco(4) Composto pela probabilidade e impacto de sua ocorrência. Abaixo detalhamos o significado dado

Quadro 4 - Quadro de conceitos para análise de riscos e benefícios desenvolvida pelos pesquisadores do Berkman Klein Center for Internet & Society

Conceito	Risco	Benefício
Características (vulnerabilidades ou vantagens)	Vulnerabilidades são atributos que aumentam a suscetibilidade de uma organização a resultados negativos, isto é, a eventos de ameaça.	Vantagens são atributos que aumentam a capacidade de uma organização de produzir resultados positivos, isto é, eventos de vantagem.
Eventos (eventos de ameaça ou eventos de vantagem)	Eventos de ameaça são resultados negativos que surgem a partir de vulnerabilidades.	Eventos de vantagem são resultados positivos que surgem a partir de vantagens.
Fontes (fontes de ameaça ou fontes de vantagem)	Fontes de ameaça são pessoas ou organizações que buscam iniciar eventos de ameaça.	Fontes de vantagem são pessoas ou organizações que buscam iniciar eventos de vantagem.
Probabilidade	Probabilidade é a chance de que um evento de ameaça ocorra por meio de uma fonte de ameaça que explore com sucesso uma vulnerabilidade.	Probabilidade é a chance de que um evento de vantagem ocorra por meio de uma fonte de vantagem que explore com sucesso uma vantagem.

Impacto	Impacto é o efeito negativo causado por um evento de ameaça. Esse é um fator composto tanto pela escala, isto é, o número de pessoas afetadas, quanto pela gravidade, isto é, o dano causado a cada pessoa.	Impacto é o efeito positivo causado por um evento de vantagem. Esse é um fator composto tanto pela escala, isto é, o número de pessoas afetadas, quanto pela gravidade, isto é, a utilidade fornecida a cada pessoa.
Grau / Resultado (risco ou benefício)	Risco é uma síntese da probabilidade e do impacto que descreve o perigo geral para uma organização.	Benefício é uma síntese da probabilidade e do impacto que descreve a oportunidade geral para uma organização.

Fonte: Green et al. (2017).

a cada um desses elementos:



No contexto do documento, essa primeira camada da metodologia permite que os municípios combinem diferentes componentes para avaliar, de forma estruturada, os benefícios e os riscos associados a programas de dados (Green et al., 2017).

No caso dos riscos, a análise parte das características dos dados, especialmente da identificação das vulnerabilidades presentes. As vulnerabilidades são características que aumentam a suscetibilidade da organização à ocorrência de resultados negativos, isto é, de eventos de ameaça. Um dado de identificação atrelado a um dado de saúde tem uma vulnerabilidade de revelar informações sensíveis, por exemplo.

Para cada vulnerabilidade identificada (1), o município listaria os eventos de ameaça (2) que poderiam surgir a partir dela, bem como as fontes de ameaça (3), entendidas como pessoas ou organizações que poderiam iniciar tais eventos. Mantendo o exemplo dos dados de saúde, os eventos de ameaça poderiam ser incidentes de segurança que tenham acesso e cópia não autorizada desses dados de saúde. Nesse sentido, as fontes de ameaças poderiam ser criminosos cibernéticos interessados na venda desses dados.

Em seguida, atribuiria a cada evento de ameaça uma probabilidade de ocorrência (incidente de segurança), considerando a chance de que uma fonte de ameaça (cyber-criminosos) explore com sucesso uma vulnerabilidade, e um impacto esperado (reidentificação, execução de golpes), correspondente ao efeito negativo causado por esse evento. Esse impacto envolve tanto a escala, isto é, o número de pessoas afetadas, quanto a gravidade do dano causado a cada pessoa. Por fim, com base na combinação entre probabilidade e impacto, o município poderia sintetizar esses elementos para determinar o grau geral de risco (4) associado àqueles dados.



O mesmo procedimento seria aplicado à análise dos benefícios, utilizando-se os termos correspondentes. Nesse caso, a avaliação partiria da identificação das vantagens potenciais dos dados a serem divulgados. (1) No caso dos dados de saúde, a identificação do titular pode facilitar o atendimento clínico e outros direitos. As vantagens são atributos que aumentam a

capacidade da organização de produzir resultados positivos, isto é, eventos de vantagem. A partir delas, o município listaria os eventos de vantagem (2), compreendidos como resultados positivos que poderiam surgir dessas vantagens (atendimento em saúde facilitado), bem como as fontes de vantagem (3), isto é, pessoas ou organizações que poderiam iniciar tais eventos. O que no caso de dados de saúde poderiam ser os próprios cidadãos atendidos, bem como da cadeia de saúde pública que poderia utilizar essas informações para pesquisas e aprimoramento do atendimento em saúde.

Em seguida, atribuiria a cada evento de vantagem uma probabilidade de ocorrência (uso dos dados para atendimento), considerando a chance de que uma fonte de vantagem explore com sucesso uma vantagem (cidadão, órgãos de saúde), e um impacto esperado, correspondente ao efeito positivo causado por esse evento (atendimento adequado e facilitado em órgãos de saúde). Esse impacto também envolve uma dimensão de escala, isto é, o número de pessoas afetadas, e uma dimensão de gravidade, entendida aqui como a utilidade proporcionada a cada pessoa. Por fim, com base na combinação entre probabilidade e impacto, o município poderia sintetizar esses elementos para determinar o grau geral de benefício (4) associado à divulgação daqueles dados.

Vale notar que nessa metodologia, tanto o grau dos riscos quanto dos benefícios são definidos a partir da probabilidade de sua ocorrência e impacto caso ela se materialize.

Esse desenho metodológico, embora bem estruturado, ainda não apresentava escalas suficientemente detalhadas para orientar a classificação dos riscos e dos benefícios como baixos, médios ou altos. A escala apresentada no estudo diz respeito a um processo específico voltada a incorporar a opinião pública e as expectativas sociais na avaliação da publicação de dados (Green et al., 2017).

D

A formulação de escalas para riscos e benefícios foi posteriormente apresentada pelo Future of Privacy Forum (FPF, 2018), ao aplicar a metodologia ao projeto de dados abertos da cidade de Seattle.

Uma das principais alterações realizadas pelo FPF (2018) foi a ampliação da escala de análise. Enquanto o modelo proposto pelos pesquisadores do Berkman Klein Center trabalhava com uma matriz 3x3, na qual riscos e benefícios podiam ser classificados apenas como baixos, médios ou altos, o FPF (2018) adotou uma matriz 5x5. Agora, os riscos e benefícios poderiam ter grau muito baixo, baixo, médio, alto e muito alto.

Essa mudança busca distinguir situações intermediárias e captar com mais precisão diferentes graus de risco e de benefício. Assim, a análise deixou de operar apenas com três categorias amplas e passou a contemplar uma gradação maior, o que pode tornar o processo decisório mais sensível às particularidades de cada caso. Abaixo deixamos os quadros com as escalas de probabilidade e impacto para riscos e benefícios da FPF (2018):

Quadro 5 – Escala de grau de probabilidade dos riscos desenvolvida pela Future of Privacy Forum traduzida e adaptada pela Data Privacy Brasil

Probabilidade	Valor	Risco	Benefício
Muito alto	10	O risco é quase certo de ocorrer.	O benefício é quase certo de ocorrer.
Alto	8	O risco é altamente provável de ocorrer.	O benefício é altamente provável de ocorrer.
Moderado	5	O risco é razoavelmente provável de ocorrer.	O benefício é razoavelmente provável de ocorrer.
Baixo	2	O risco é improvável de ocorrer.	O benefício é improvável de ocorrer.
Muito baixo	0	O risco é altamente improvável de ocorrer.	O benefício é altamente improvável de ocorrer.

Fonte: Adaptado e traduzido de FPF (2018, p. 38–41).⁷

Quadro 6 – Escala de grau de impacto de benefício desenvolvida pela Future of Privacy Forum traduzida e adaptada pela Data Privacy Brasil

Impacto	Valor	Risco	Benefício
Muito alto	10	O conjunto de dados provavelmente produzirá múltiplos efeitos adversos graves ou catastróficos sobre indivíduos, comunidade, outras organizações ou a sociedade.	O conjunto de dados provavelmente produzirá múltiplas utilidades relevantes e importantes para indivíduos, comunidade, outras organizações ou a sociedade.
Alto	8	O conjunto de dados provavelmente produzirá efeito adverso grave ou catastrófico sobre indivíduos, comunidade, outras organizações ou a sociedade.	O conjunto de dados provavelmente produzirá utilidade relevante e importante para indivíduos, comunidade, outras organizações ou a sociedade.

⁷ No original as escalas de benefícios e riscos são duas tabelas separadas. Contudo, como elas contam com os mesmos critérios, unimos elas para melhor visualização da construção feita pela Future of Privacy Forum.

Moderado	5	O conjunto de dados provavelmente produzirá efeito adverso sério sobre indivíduos, comunidade, outras organizações ou a sociedade.	O conjunto de dados provavelmente produzirá utilidade clara para indivíduos, comunidade, outras organizações ou a sociedade. Embora a utilidade seja evidente, ela não é tão urgente quanto uma utilidade de nível alto.
Baixo	2	O conjunto de dados provavelmente produzirá impacto adverso limitado sobre indivíduos, comunidade, outras organizações ou a sociedade.	O conjunto de dados provavelmente produzirá utilidade limitada para indivíduos, comunidade, outras organizações ou a sociedade.
Muito baixo	0	O conjunto de dados provavelmente produzirá impacto adverso negligenciável sobre indivíduos, comunidade, outras organizações ou a sociedade.	O conjunto de dados provavelmente produzirá utilidade negligenciável para indivíduos, comunidade, outras organizações ou a sociedade.

Fonte: FPF [2018, p. 37–40].⁸

Uma vez definido o grau do benefício e risco, a metodologia avança para sua segunda fase: a comparação entre eles. Nessa análise, o grau de risco é definido da seguinte forma: *Quanto mais alto o benefício e menor o risco, o grau do risco é mais baixo. Quanto mais alto o risco em relação ao benefício, mais alto é o risco. Se tanto risco quanto o benefício tem o mesmo valor, o grau do risco é médio.* No caso da análise feita pela Future of Privacy Forum, o resultado dessa análise deveria indicar a publicação ou não desses dados. Contudo, no modelo desenhado pelos pesquisadores do Berkman Klein Center propõem um passo além. A adoção de medidas de mitigação para melhor calibrar os riscos e benefícios.

Nesse passo seguinte, uma vez que esse risco inicial é realizado, deve-se verificar medidas de mitigação que mantenham ou aumentem o grau do benefício e reduzam o grau dos riscos identificados. Essa é uma tarefa delicada quando o assunto é abertura de dados, na medida em que certas medidas que dificultam riscos de reidentificação também podem diminuir a qualidade da abertura dos dados para pesquisas, transparência pública etc.

⁸ No original as escalas de benefícios e riscos são duas tabelas separadas. Contudo, como elas contam com os mesmos critérios, unimos elas para melhor visualização da construção feita pela Future of Privacy Forum.

Os pesquisadores do Berkman Klein Center destacam que os municípios deveriam ter um conjunto de medidas de mitigação definidas no nível dos dados, ou seja, na forma como eles serão disponibilizados e armazenados. Isso pode envolver medidas como a agregação dos dados, anonimização por meio da não disponibilização de certos campos de informação etc. Como os pesquisadores estavam focados em metodologias para programas de dados abertos, seu principal foco era a redução de riscos à privacidade, razão pela qual tal preocupação com medidas ao nível dos dados têm prioridade.

Contudo, também entendem ser importante a implementação de medidas de mitigação de riscos no nível técnico ou contratual por meio de softwares que irão disponibilizar os dados e contratos ou acordos de compartilhamento de dados entre órgãos municipais (Green et al., 2017). Outro procedimento importante para aumentar o grau do benefício dos dados é a adoção de medidas de promoção dos benefícios como ações de conscientização sobre o funcionamento de plataformas de dados abertos (Green et al., 2017). Nesse caso, ao informar adequadamente dos possíveis usos de uma ferramenta de dados abertos, a probabilidade de seu uso por pesquisadores e organizações aumenta, ampliando o grau de benefício da abertura desses dados.

Da mesma forma que é preciso combinar tipos diferentes de medidas de mitigação, não basta escolher uma medida que reduza riscos ou aumente o benefício de forma abstrata. É preciso verificar se tal medida é adequada aos riscos e benefícios concretos presentes naquele contexto de tratamento de dados e testar sua efetividade.

Um exemplo utilizados pelos autores foi o da divulgação de dados sobre táxis feito pela cidade de Nova York (Green et al., 2017). Na ocasião, a cidade disponibilizou informações sobre horários e locais de embarque e desembarque, placa dos táxis e licença para dos motoristas envolvidos em cada corrida. Para proteger a identidade dos motoristas de táxi, a cidade de Nova York utilizou uma técnica de anonimização que produziam códigos criptografados com base nos números das licenças do motorista e das placas de seus carros. Essa técnica impedia a identificação direta dos motoristas pois era impossível de fazer o caminho reverso, ou seja, descobrir qual placa e qual licença o código gerado ele se referia.

Na ocasião, o cientista de dados Vijay Pandurangan percebeu a lógica dos códigos gerados e a partir do formato padronizado das placas e dos números de licença, comprometeu essa proteção. Segundo ele, essa proteção chamada hash MD5, é uma técnica muito útil para dificultar o acesso aos dados que seriam anonimizados. Entretanto, quando se conhece o formato dos dados que seriam anonimizados, é possível fazer o caminho reverso e identificar o que não deveria ser reidentificado.

Nesse exemplo, teria sido mais seguro substituir os números das placas e das licenças por identificadores aleatórios, sem relação com os números originais. Como esses novos identificadores seriam atribuídos de forma aleatória, sem seguir a estrutura ou a ordem dos dados originais, não haveria um caminho previsível para reconstruir os números verdadeiros. Dessa forma, os dados poderiam ser publicados eliminando ainda mais o risco de reidentificação.

Embora os documentos analisados demonstrem que a metodologia de riscos e benefícios

oferece um caminho relevante para lidar de forma mais efetiva com os riscos e os benefícios envolvidos na abertura de dados, existem situações em que, ainda que o benefício seja igual ou até superior ao risco, determinados efeitos não podem ser admitidos em nenhuma circunstância.

Essa suposta omissão não é proposital ou falha das metodologias, mas um sinal da dificuldade de estimar, de forma abstrata, quais são esses limites. Afinal, os riscos considerados inaceitáveis em uma sociedade não decorrem apenas de uma operação metodológica, mas são construídos historicamente e representados por leis, direitos fundamentais, garantias institucionais e valores comuns compartilhados. Dessa forma, toda análise de riscos precisa levar em consideração o que esses diplomas sugerem, de forma a evitar que uma análise de risco, ainda que bem feita, os redistribua ou crie novos riscos aos titulares de dados.

Colocando em movimento

No exemplo *Sexual assault locations for 911 data* (Green et al., 2017)⁹, a metodologia é aplicada a uma base de dados composta por registros de chamadas ao serviço de emergência relacionados a ocorrências de violência sexual. A característica analisada é a presença de informações sobre a localização desses incidentes, isto é, dados que indicam onde os eventos foram registrados.

Em um primeiro momento, realiza-se a análise dos riscos. A vulnerabilidade (1) central está no fato de que a localização dos incidentes pode permitir a identificação ou a falsa identificação de vítimas. Mesmo que a base não contenha nomes ou outros identificadores diretos, a informação de dados de localização pode ser combinada com outros dados disponíveis, como notícias, relatos locais ou redes sociais, ampliando a possibilidade de exposição indevida. Os eventos de ameaça (2) identificados, portanto, são a reidentificação de vítimas ou a reidentificação errônea das vítimas. As fontes de ameaça (3), que no caso seriam os agentes que poderiam abusar dessa possibilidade de reidentificação, podem incluir hackers cívicos, grupos comunitários, indivíduos, jornalistas e pesquisadores. A partir da combinação entre a probabilidade de ocorrência e o impacto potencial desses eventos, a metodologia aplicada pelos pesquisadores indica um risco alto (4).

Em seguida, realiza-se a análise dos benefícios. A divulgação da base pode gerar vantagens relevantes para o interesse público, pois permite compreender padrões de criminalidade, identificar tendências, subsidiar políticas públicas, orientar a alocação de recursos e possibilitar maior transparência sobre a atuação estatal. Os eventos de vantagem indicados são a possibilidade de compreender padrões criminais e de examinar detalhes de casos específicos. As fontes de vantagem também incluem atores como hackers cívicos, indivíduos e jornalistas, que poderiam utilizar os dados para produzir análises, investigações, reportagens ou ferramentas de acompanhamento público. Com base na probabilidade de realização desses benefícios e no impacto positivo esperado, o benefício é classificado como médio.

⁹ Na ocasião, adaptamos o caso para o formato textual, uma vez que o caso foi sendo apresentado direto no modelo de avaliação de riscos do documento.

Depois dessas duas avaliações, a metodologia passa à comparação entre risco e benefício. Nesse momento, verifica-se que a divulgação da base em sua forma original apresenta um dilema. Embora exista benefício público na abertura dos dados, o risco associado à exposição da localização dos incidentes é alto. Como o risco inicial supera o benefício identificado, a divulgação integral da base, sem qualquer tratamento, não seria adequada. A metodologia avança e proõe a avaliação de medidas de mitigação capazes de reduzir o risco sem eliminar completamente a utilidade pública dos dados.

Na etapa de mitigação, são consideradas diferentes medidas possíveis, como remover campos, remover registros, agregar dados, generalizar dados, anonimizar identificadores ou adotar outras salvaguardas. No exemplo, a medida escolhida é a remoção dos campos de dados de localização dos incidentes reportados. Essa solução atua diretamente sobre a vulnerabilidade principal da base, pois retira o elemento que mais facilitava a reidentificação ou a falsa identificação das vítimas.

Após a adoção da medida, realiza-se uma nova avaliação da relação entre riscos e benefícios, agora considerando o risco residual. Com a remoção das localizações dos incidentes de violência sexual, o risco deixa de ser alto e passa a ser médio, pois a possibilidade de associação direta entre a ocorrência e uma pessoa, por meio de sua localização é reduzida. Ao mesmo tempo, o benefício permanece médio, já que os dados ainda podem ser úteis para compreender aspectos gerais das ocorrências, ainda que percam parte de seu valor para análises territoriais mais detalhadas.

O resultado final da metodologia é a recomendação de divulgar os relatórios de crimes com a remoção das localizações dos incidentes de violência sexual. O exemplo demonstra que a metodologia de riscos e benefícios é capaz de mediar o embate entre os valores associados à transparência pública e os riscos relacionados aos direitos dos titulares de dados, como a privacidade.

Os desafios brasileiros de abertura de dados públicos podem se beneficiar da metodologia de riscos e benefícios justamente porque ela permite superar uma lógica binária entre publicar ou restringir o acesso aos dados. Ao considerar simultaneamente os benefícios da transparência pública e os riscos à aos titulares de dados, essa abordagem oferece um caminho mais adequado para decisões proporcionais e responsáveis.

No entanto, sua aplicação ao cenário brasileiro não pode ocorrer por meio de uma simples transposição. É necessário adaptá-la às especificidades jurídicas, institucionais e sociais do país, especialmente à centralidade constitucional da publicidade administrativa, ao regime da Lei de Acesso à Informação e à Proteção de Dados Pessoais. É o que iremos propor no próximo capítulo.

04 UMA METODOLOGIA DE CUSTO-BENEFÍCIO

04 UMA METODOLOGIA DE CUSTO-BENEFÍCIO

Como visto, o risco é um elemento de difícil mensuração uma vez que sua definição depende de uma série de conhecimentos acerca do fenômeno que permitam a abstração de eventos futuros e seus impactos. Contudo, mais importante do que o conceito do risco, é a forma como os tornamos visíveis. Diante desta tarefa, vimos que uma forma mais adequada de visualizar os riscos é a partir de uma metodologia técnico-científica, onde o risco possa ser vislumbrado e modificado por meio de medidas do agente que tem interesse em administrar esse risco.

No caso do relatório de impacto à proteção de dados previsto pela LGPD, o risco tem um contorno claro. Trata-se do risco aos direitos e liberdades fundamentais dos titulares. Vimos como diferentes metodologias ensinam que o risco pode ser constituído por meio da análise da probabilidade de sua ocorrência e dos impactos caso ele se materialize, pelos riscos a direitos humanos, riscos relacionados à privacidade. A dimensão do risco na governança de dados parece bem justificada e o procedimento de escolha e aplicação de medidas de controle do risco são bem estruturadas.

Na sequência, vimos que embora tais metodologias sejam relevantes para a visualização dos riscos, elas podem ter dificuldades em lidar com dimensões em disputa em um tratamento de dados. No caso desse relatório, as dimensões abordadas dizem respeito à transparência pública de dados e à proteção de dados pessoais. Foi nesse contexto que abordamos as metodologias de riscos e benefícios como uma resposta para a mensuração do risco que fosse para além dele mesmo. Que fizesse com que os riscos e benefícios de um tratamento fossem vislumbrados e os impactos de medidas tomadas sobre o benefício daquela atividade de tratamento. Em outras palavras, uma metodologia que permitisse uma visão mais holística dos impactos na disponibilização de dados.

Tal metodologia está em consonância com os objetivos da Lei Geral de Proteção de Dados no sentido de que os benefícios dos tratamentos de dados podem e devem ser aproveitados por toda a sociedade, ao mesmo tempo que os riscos precisam ser reduzidos ao máximo possível.

Dessa forma, a partir das influências trabalhadas nesse trabalho, apresentamos a metodologia de custo-benefício. Ela é fruto das influências das metodologias apresentadas neste trabalho e uma proposta para o dilema da construção de soluções de aumento de transparência pelo Estado em harmonia com a Lei Geral de Proteção de Dados. A metodologia busca permitir a tomada de decisão adequada acerca de programas de dados abertos e outras iniciativas de aberturas de dados pelo Estado Brasileiro.

De forma geral, sua estrutura é baseada na metodologia de riscos e benefícios do capítulo anterior, com modificações para melhor adaptação do contexto brasileiro bem como das in-

suficiências das metodologias analisadas até então. Em outras palavras, é possível dizer que a metodologia de custo-benefício pode ser descrita 6 passos:

1. Definição do tratamento de dados voltado para a disponibilização de dados pessoais
2. Análise do Valor e do Risco iniciais
3. Definição do grau do custo-benefício
4. Adoção de medidas de mitigação
5. Definição do custo-benefício residual
6. Decisão sobre a disponibilização dos dados

Abaixo, detalhamos cada uma desses passos e as escolhas metodológicas que subsidiaram este desenho

Passo 1 - Definição do tratamento de dados voltado para a disponibilização de dados pessoais



Devem ser descritos os principais elementos que estruturam a disponibilização dos dados. Em primeiro lugar, deve-se identificar quais dados serão disponibilizados, indicando os tipos de dados pessoais ou categorias de dados envolvidos, o nível de detalhamento da base, a existência de dados sensíveis, identificadores diretos ou indiretos, bem como eventuais critérios de seleção, exclusão ou organização das informações.

Em segundo lugar, deve-se descrever a política, programa ou iniciativa que subsidia a abertura dos dados, indicando seus objetivos, fundamentos jurídicos e institucionais, como leis, atos normativos, contratos, convênios, termos de cooperação ou instrumentos congêneres. Essa descrição também deve abranger os meios técnicos utilizados para a disponibilização, como sistemas, softwares, plataformas, APIs, painéis, portais ou outras interfaces por meio das quais os dados serão acessados pelo público ou por grupos específicos.

Quanto melhor o grau da descrição, mais fácil e justificada será a análise dos riscos e benefícios. Uma vez descrita a atividade de tratamento, é preciso definir o seu valor para o benefício e o seus riscos relacionados ao tratamento.

Passo 2 - Análise do Valor e do Risco iniciais

Valor

Para a análise do benefício da divulgação de dados é preciso entender o grau do valor dessa disponibilização. '*Valor*' nesta metodologia é definido como o tipo de resultado esperado pela abertura de dados. Pode envolver o aumento do controle social sobre aquele tema, produção de pesquisa, criação ou melhoria de bens e serviços, entre outros. Também precisa destacar quais os públicos beneficiados pelo valor da disponibilização dos dados.



A adoção do termo '*valor*' ocorre pois designa a análise em abstrato dos potenciais benefícios da abertura de dados. Diferentemente de um benefício, onde falamos da sua concretização.

Dessa forma, é possível entender que valor é a definição em abstrato de um benefício, enquanto o benefício é a materialização do valor da disponibilização de dados. Nesse sentido, diferencia-se de metodologias de riscos e benefícios tradicionais por meio de uma nomenclatura que diferencie os benefícios descritos e os concretizados após a disponibilização dos dados.

Para melhor definir o grau do valor, é preciso trabalhar no sentido de estabelecer 1) que valor é esperado da abertura de dados e 2) os públicos beneficiados. No caso do valor esperado, deve-se estabelecer as potencialidades dessa divulgação. Seriam os resultados possíveis daquela abertura de dados. Se determinados dados promovem o exercício de direitos, se promovem o controle social, dão guarida à investigações ou pesquisas são exemplos desse valor esperado.

No caso dos públicos beneficiados, é preciso definir quais grupos estão associados ao benefício esperado da abertura de dados. Jornalistas, órgãos de fiscalização, pesquisadores, organizações da sociedade civil, cidadãos em situações específicas são alguns exemplos. Nesse caso, sublinhamos a expressão ‘públicos associados ao benefício esperado’ que pode parecer redutora à primeira vista, afinal, a disponibilização de dados em portais de dados abertos podem oferecer valor para múltiplos públicos, inclusive aqueles que não irão manejar esses dados diretamente.



Contudo, a definição serve para que o controlador concretize o máximo possível desse benefício de forma a demonstrar quais benefícios são esperados da abertura e quais grupos poderão ser alcançados por esses benefícios. Ou seja, como forma de aprimorar a análise de riscos e não excluir da análise grupos beneficiados por ela. Como o grau de qualidade da descrição do valor facilita a definição de seu grau de riscos, recomendamos que essa análise passe por situações concretas e com lastro histórico para melhor fundamentar a análise dos riscos.

Grau do valor:

Para delimitar o grau do valor na disponibilização dos dados é preciso avaliar a probabilidade com que ele pode se realizar e seus impactos caso o valor se materialize. Nesse sentido:

Valor = [P] Probabilidade x [I] Impacto.

A matriz de risco adotada por esse trabalho é de 3x3, onde tanto impacto quanto probabilidade são classificados entre baixo, médio e alto. Sendo o grau baixo tendo valor (5); o médio, valor (10) e; o alto, de (15). A escolha por manter a matriz nesses termos serve para funcionar mais diretamente com o modelo de análise de riscos no RIPD recomendado e divulgado pelo Ministério da Gestão e Inovação em Serviços Públicos (Brasil, 2023). Dessa forma, as metodologias podem ser ‘interoperáveis’, uma vez que partilham de uma linguagem aproximada.



Entretanto, de nada adianta propor a fórmula sem critérios para facilitar a análise do valor pelos controladores. Nesse sentido, sugerimos os seguintes critérios em que combinamos as

contribuições das metodologias de análise de riscos e benefícios (Green et al., 2017; FPF, 2018) com as contribuições das autoridades uruguaia, argentina (AAIP; URCDP, 2020) e espanhola (AEPD, 2021) de proteção de dados. A ideia é manter as escalas de probabilidade e impacto com critérios adequados e instrumentalizáveis para a análise dos riscos.

Para definir melhor a Probabilidade do valor, sugerimos os seguintes critérios:

Quadro 7 - Índices de probabilidade do valor

	BAIXA [5]	MÉDIA [10]	ALTA [15]
PROBABILIDADE DO VALOR	O valor pode se realizar apenas em circunstâncias excepcionais	O valor pode se realizar de forma rara e pouco frequente, embora não improvável	O valor pode se realizar de forma frequente e comum.

Fonte: Elaboração própria.

Nesse caso, o desenho é simples. Quanto mais fácil a disponibilidade de dados em realizar o valor, mais fácil é a sua concretização. No caso de dados abertos, podem existir ocasiões nas quais a sua disponibilização ocorra de forma faseada ou com períodos de tempo específicos. Nesse sentido, a chance de concretização do valor da disponibilidade desses dados pode ser reduzida ou aumentada por diversos fatores da política de divulgação de dados.

D

Para definir melhor o impacto do valor, propomos uma solução que exige a averiguação do potencial do impacto e a possibilidade do titular explorar o valor da divulgação do dado. Por exemplo, dados de vacinação podem ficar disponíveis em um portal sem divulgação do governo e a forma com que os dados são publicados são de um formato que somente especialistas em tecnologias da informação são capazes de extrair o benefício daquele dados. Nesse caso, embora o impacto da divulgação de dados de saúde seja grande, a forma como foi disponibilizado dificulta muito a exploração desse benefício por jornalistas e pesquisadores, por exemplo, afetando a probabilidade negativamente.

Abaixo, deixamos os critérios e alguns exemplos para melhor concretização do impacto do valor:

Quadro 8 – Índices do impacto do valor

IMPACTO DO VALOR	BAIXO [5]	MÉDIA [10]	ALTA [15]
	Os públicos beneficiados serão afetados de forma insignificante pelo valor da disponibilidade dos dados e só poderão se aproveitar da abertura dos dados com grandes dificuldades OU Os públicos beneficiados não serão afetados pelo valor da disponibilidade dos dados e não poderão conseguir se aproveitar da abertura dos dados.	Os públicos beneficiados serão afetados de forma significativa pelo valor da disponibilidade dos dados mas somente poderão se aproveitar da abertura dos dados com alguma dificuldade	Os públicos beneficiados serão afetados de forma significativa pelo valor da disponibilidade dos dados e poderão se aproveitar da abertura dos dados com facilidade

Fonte: Elaboração própria.

Quadro 9 – Exemplos para o grau do impacto do valor

Classificação: Baixa [5]	
Critério	Os públicos beneficiados não serão afetados ou serão afetados de forma insignificante pelo valor da disponibilização dos dados, com grande dificuldade para aproveitá-la.
Exemplos	1. Divulgação de dados pouco compreensíveis, não interoperáveis, sem documentação ou metadados adequados. 2. Base pública que não permite análises relevantes para os titulares ou para grupos afetados. 3. Dados disponibilizados em formato pouco acessível, dificultando seu uso por cidadãos, pesquisadores ou organizações. Exemplo: Divulgação de informações sobre compra de remédios. São divulgadas planilhas em formato de PDF, limitando o processamento por máquina. Além disso, todas as informações estão em siglas e abreviações, mas não há um dicionário dos dados. Por fim, os dados não têm um cronograma de atualização definido, de forma que ficam meses sem qualquer revisão.

Classificação: Média (10)	
Critério	Os públicos beneficiados serão afetados de forma significativa pelo valor da disponibilização dos dados, mas só poderão se aproveitar dela com alguma dificuldade.
Exemplos	1. Os dados são divulgados, mas a forma prejudica sua análise ou processamento das informações conforme necessidade do público beneficiado, como dados sem licença aberta, sem interoperabilidade ou com restrições legais ao uso.. 2. Base de dados pública que permite análises sobre um determinado tema ao público interessado, mas com certas limitações, como necessidade de conhecimentos técnicos ou outras informações não disponibilizadas. 3. Dados sobre execução de políticas públicas, úteis para organizações sociais, mas não imediatamente compreensíveis para o público afetado. Exemplo: Os dados sobre aquisição de remédios são disponibilizados em formato de planilha, não mais em PDF. Além disso, há um dicionário de dados explicando cada uma das colunas e abreviações. A equipe responsável criou um cronograma de atualização mensal e cumpre os prazos definidos.
Classificação: Alta (15)	
Critério	Os públicos beneficiados serão afetados de forma significativa pelo valor da disponibilização dos dados e poderão se aproveitar dela com facilidade.
Exemplos	1. Dados estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento. 2. As informações disponíveis consideram os principais usos do público interessado, permitindo análises aprofundadas sobre o tema – seja por meio de painéis de dados, ou mesmo APIs com documentação pública. 3. Dados apresentados de forma compreensível, permitindo comparação, reivindicação de direitos e melhoria da ação de agentes públicos, ou mesmo a produção de conhecimento técnico, científico e produtos.. Exemplo: Os dados sobre aquisição de remédios são disponibilizados via API pública, com atualização diária e automatizada. Além disso, há um painel de dados disponível para visualização sem necessidade de cadastro ou conhecimentos técnicos, permitindo análise com filtros e download dos dados abertos.

Fonte: Elaboração própria.

Uma vez definidos a probabilidade e o impacto, o grau de valor deve ser calculado pela multiplicação entre esses dois fatores. Considerando a escala adotada, em que cada dimensão pode receber os valores 5, 10 ou 15, o resultado da matriz de valor varia entre 25 e 225. O valor 25 representa o menor grau possível, decorrente da combinação entre baixa probabilidade e baixo impacto, enquanto o valor 225 representa o grau mais elevado, resultante da combinação entre alta probabilidade e alto impacto.

Figura 5 - Matriz Probabilidade x Impacto

Probabilidade (P)	15	75	150	225
	10	50	100	150
	05	25	50	75
		05	10	15
		Impacto (I)		

Fonte: Brasil (2023)

A análise deve ser realizada individualmente para cada valor identificado. Em seguida, para a definição de um grau global de valor da atividade analisada, recomenda-se a utilização de uma média simples dos graus de valor obtidos. Assim, todos os graus de valor devem ser somados e, posteriormente, divididos pelo número total de valores identificados.

$$\text{Valor Global} = \frac{\text{Soma dos Valores Identificados}}{\text{Quantidade de Valores Identificados}}$$

Risco Inicial

O risco corresponde ao tipo de consequência negativa que pode se concretizar a partir da disponibilização dos dados pessoais. Ele pode envolver, por exemplo, reidentificação de titulares, discriminação, exposição indevida, constrangimentos, fraudes, perda de controle sobre os dados, uso secundário incompatível, vigilância, exclusão de acesso a serviços ou outros impactos sobre direitos, liberdades e interesses dos titulares.

Assim como na análise do valor, a análise do risco inicial deve identificar quais são os riscos esperados a partir da abertura dos dados, quais titulares ou grupos podem ser afetados e quais circunstâncias tornam esses riscos mais prováveis ou mais graves. Essa etapa deve considerar tanto as características dos dados disponibilizados quanto o contexto em que eles serão divulgados, incluindo a possibilidade de cruzamento com outras bases, o grau de detalhe das informações, o público que poderá acessar os dados e as finalidades previsíveis de reutilização.



No caso de políticas de dados abertos, a reidentificação é um risco comum e conectado às demais consequências da reidentificação e devem ser avaliados de forma integrada. Pode ser que a reidentificação seja já pressuposta no caso de abertura de dados com identificação pessoal, e isso não ser um problema uma vez que, como abordado no capítulo 1, a reidentificação pode ser esperada e parte do valor da disponibilização de dados e não seu risco. Dessa forma, é preciso descrever as possíveis consequências dessa identificação da forma mais concreta possível.

Em Nota Técnica sobre o caso Inep, a ANPD reforça esse entendimento informando os impactos da reidentificação precisam ser avaliados com base em evidências e em cenários objetivos da realidade. Dessa forma é possível averiguar que um risco de identificação pode ter impactos maiores ou menores aos titulares. De acordo com a Agência:



[...] se a eventual reidentificação abranger dados sensíveis, as salvaguardas devem ser diferenciadas. Já a identificação de informações triviais relativas a uma pessoa pública, ou a mera confirmação de informações previamente divulgadas por esta pessoa constitui, a princípio, um fator de risco de menor impacto, que pode demandar salvaguardas mais simples e flexíveis (ANPD, 2022, p. 9).



Dessa forma, o risco de reidentificação pode ter consequências cujo risco pode ser alto, médio ou baixo de forma independente do grau de risco da reidentificação.

Grau do risco

Para delimitar o grau do risco na disponibilização dos dados, é preciso avaliar a probabilidade de sua ocorrência e o impacto que ele poderá produzir caso se materialize. Nesse sentido:

Risco = [P] Probabilidade x [I] Impacto.

Novamente, a matriz de risco adotada é de 3x3, em que tanto a probabilidade quanto o impacto são classificados entre baixo, médio e alto. O grau baixo recebe valor 5, o médio recebe valor 10 e o alto recebe valor 15.



Assim, o grau do risco poderá variar entre 25 e 225, sendo 25 o menor grau de risco possível e 225 o maior grau de risco possível. Para definir melhor a probabilidade do risco, sugerimos os seguintes critérios:

Quadro 10 - Probabilidade do risco

	BAIXA	MÉDIA	ALTA
PROBABILIDADE DO RISCO	O risco pode acontecer apenas em circunstâncias excepcionais	O risco pode se manifestar de forma rara e pouco frequente, embora não improvável	É possível que o risco se realize de forma frequente e comum.

Fonte: Elaboração própria.

De forma parecida com a definição da probabilidade do valor, o grau do risco depende do quanto um risco pode se materializar. Para definir melhor o **impacto do risco**, a análise deve considerar a gravidade da consequência para os titulares dos dados e a capacidade de superação dos efeitos negativos produzidos pela disponibilização dos dados. Isso significa avaliar a gravidade dos impactos de um risco após se materializar e da dificuldade de um titular de superar tal situação.

Por exemplo, um titular passa a receber mensagens de email com ofertas de serviços e produtos. Tais anúncios foram feitos a partir da agregação de informações do titular em portais públicos. Ainda que esse risco se materialize, a gravidade de seu impacto pode ser menor pois não impede o exercício de direitos ou acesso a benefícios, bem como a sua superação pode ser fácil pelo titular que pode bloquear a fonte dos emails ou se descadastrar para recebê-los, algo que seria considerado de impacto baixo.

Diferentemente é o uso de dados de telefone coletados em bases públicas para a publicidade por meio de ligações de telefone. Nesse caso, o impacto costuma ser mais significativo na medida em que as ligações excessivas podem fadigar o titular e o fazer não utilizar plenamente seu serviço de telefonia contratado, ao passo que há uma dificuldade significativa em parar de receber as ligações diante do reduzido número de interfaces em que um titular pode impedir de ser comunicado por seu número de celular. Nesse caso, o impacto poderia ser considerado médio.

Quadro 11 - Impacto do risco

	BAIXO (5)	MÉDIA (10)	ALTA (15)
IMPACTO DO RISCO	Os titulares dos dados não serão afetados ou sofrerão apenas alguns inconvenientes, que poderão resolver sem muitas dificuldades	Os titulares dos dados serão afetados de forma significativa, podendo superar a situação com alguma dificuldade	Os titulares dos dados serão afetados de forma significativa e só poderão superar a situação com grandes dificuldades OU serão afetados com consequências gravíssimas e irreversíveis que talvez não possam superar.

Fonte: Elaboração própria.

Quadro 12 - Exemplos para o grau do impacto do risco

Classificação: Baixa (5)	
Critério	Os titulares não serão afetados ou sofrerão apenas inconvenientes que poderão resolver sem muitas dificuldades.
Exemplos	1. Recebimento de comunicações indesejadas ou abordagens pontuais de publicidade após reutilização da base. 2. Pequena perda de tempo para corrigir informação imprecisa ou solicitar retirada de dado. 3. Incômodo limitado decorrente de exposição de informação pouco sensível e de baixo potencial discriminatório.
Classificação: Média (10)	
Critério	Os titulares serão afetados de forma significativa, podendo superar a situação com alguma dificuldade
Exemplos	1. Exposição de informação que gere constrangimento, estigma social ou tratamento desigual. 2. Uso dos dados para perfilamento, propaganda direcionada abusiva ou exclusão injustificada de oportunidades. 3. Reidentificação de grupo vulnerável, exigindo medidas administrativas ou jurídicas para contenção do dano.
Classificação: Alta (15)	
Critério	Os titulares serão afetados de forma significativa e só poderão superar a situação com grandes dificuldades, ou sofrerão consequências gravíssimas e irreversíveis.
Exemplos	1. Exposição de vítimas de violência, crianças, adolescentes ou pessoas em situação de vulnerabilidade. 2. Divulgação que possa gerar perseguição, discriminação grave, ameaça à segurança pessoal ou violência. 3. Reidentificação de dados sensíveis de saúde, orientação sexual, convicção religiosa, raça/cor ou situação socioeconômica em contexto de alto potencial discriminatório e produção de danos irreversíveis.

Fonte: Elaboração própria.



A partir dessa análise, o responsável pela avaliação deverá atribuir um valor à probabilidade e outro ao impacto, multiplicando ambos para chegar ao grau do risco inicial. Por exemplo, se determinado risco possui probabilidade média (10) e impacto alto (15), o grau do risco será 150 (alto). Caso outro risco tenha probabilidade baixa (5) e impacto médio (10), o grau do risco será 50 (baixo).

A análise deve ser realizada individualmente para cada valor identificado. Em seguida, para a definição de um grau global de valor da atividade analisada, recomenda-se a utilização de uma média simples dos graus de valor obtidos. Assim, todos os graus de valor devem ser somados e, posteriormente, divididos pelo número total de valores identificados.

Essa classificação permite comparar diferentes riscos associados à disponibilização dos dados e identificar quais deles exigem maior atenção. Riscos com grau mais elevado devem receber prioridade na definição de medidas de mitigação, especialmente quando envolverem titulares em situação de vulnerabilidade, dados sensíveis, informações altamente detalhadas ou possibilidade relevante de reidentificação.

$$\text{Risco Global} = \frac{\text{Soma dos Riscos Identificados}}{\text{Quantidade de Riscos Identificados}}$$



Passo 3 - Descobrindo o grau do custo-benefício

Depois de definidos o grau do valor inicial e o grau do risco inicial, a metodologia avança para a comparação entre os dois resultados para a produção do grau do custo-benefício. Essa etapa busca verificar se a disponibilização dos dados, tal como inicialmente planejada, apresenta uma relação adequada entre os benefícios esperados e os riscos identificados. A análise deve orientar a tomada de decisão, mas precisa ser interpretada à luz do contexto, dos titulares afetados, da natureza dos dados, da finalidade da abertura e da existência de medidas de mitigação possíveis.



De modo geral, a lógica da comparação pode ser descrita da seguinte forma: quanto maior o valor e menor o risco, maior o custo-benefício e mais favorável será a disponibilização dos dados. Quanto maior o risco em relação ao valor, o custo benefício será ruim e mais problemática será a disponibilização dos dados. Quando valor e risco possuem o mesmo grau, trata-se de um médio custo-benefício. A situação recomenda a adoção de medidas de mitigação dos riscos, ainda que exista equilíbrio entre a oportunidade gerada pela abertura e o perigo associado à divulgação.

Assim, a comparação entre valor e risco permite classificar a situação inicial da disponibilização dos dados e indicar se ela pode seguir adiante, se depende de ajustes ou se deve ser evitada, caso os ajustes não sejam suficientes. Para fins metodológicos, a comparação pode seguir a seguinte lógica:

Quadro 13 - Relação entre valor e risco

Relação entre valor e risco	Interpretação
Valor maior que o risco	Trata-se de um ótimo custo-benefício. A disponibilização tende a ser justificável, desde que os riscos sejam monitorados e mitigados quando necessário.
Valor igual ao risco	Trata-se de um médio custo-benefício. A disponibilização exige cautela, pois os benefícios e os riscos estão em equilíbrio. Devem ser avaliadas medidas de mitigação antes da decisão final.
Risco maior que o valor	Trata-se de um custo-benefício ruim. A disponibilização, tal como planejada, não é recomendável. É necessário adotar medidas de mitigação ou rever a forma de abertura dos dados.

Fonte: Elaboração própria.

Quadro 14 - Matriz de custo-benefício

CUSTO-BENEFÍCIO		VALOR		
		Baixo	Médio	Alto
RISCO	Baixo	Médio custo-benefício	Ótimo custo-benefício	Ótimo custo-benefício
	Médio	Custo-benefício ruim	Médio custo-benefício	Ótimo custo-benefício
	Alto	Custo-benefício ruim	Custo-benefício ruim	Médio custo-benefício

Fonte: Elaboração própria.

A metodologia permite observar, caso a caso, se a divulgação realmente produz valor público suficiente e quais riscos podem recair sobre os titulares. A depender do grau do custo-benefício, é possível instruir melhor se é possível a abertura dos dados ou se é preciso de medidas de mitigação para reduzir os riscos e manter o valor da publicação dos dados.

Passo 4 – Adoção de medidas de mitigação

Uma vez identificado o risco inicial, devem ser avaliadas medidas de mitigação capazes de reduzir os riscos sem eliminar ou reduzir o valor da disponibilização dos dados.

No contexto da abertura de dados pessoais, essa etapa é altamente relevante. Algumas medidas que reduzem riscos, como anonimização, agregação, generalização ou remoção de campos, também podem diminuir a utilidade dos dados para pesquisa, transparência pública, controle social ou a possibilidade de uso desses dados para formulação de políticas públicas.

Por isso, a mitigação deve buscar um equilíbrio: reduzir os riscos identificados, mas preservar o máximo possível do valor público da base.

Entre as medidas possíveis, podem ser consideradas:

Quadro 15 – Tipos de medidas de mitigação

Tipo de medida	Exemplos
Minimização dos dados	Remover campos desnecessários, como nome, CPF, endereço completo, telefone ou outros identificadores diretos.
Agregação	Divulgar dados por bairro, município, faixa etária, período ou categoria, em vez de registros individualizados.
Generalização	Reduzir a precisão de informações, como substituir data completa por mês/ano ou endereço por região.
Supressão de registros	Remover registros raros, únicos ou muito específicos que possam facilitar a reidentificação.
Anonimização ou pseudonimização	Aplicar técnicas, para além das elencadas acima, que dificultem a associação dos dados a uma pessoa identificada ou identificável.
Controle de acesso	Disponibilizar dados apenas em ambiente controlado, mediante credenciamento, termo de uso ou justificativa.
Governança e auditoria	Criar regras de uso, registro de acessos, prestação de contas, revisão periódica e mecanismos de responsabilização.

Fonte: Elaboração própria.



A escolha da medida deve estar diretamente relacionada ao risco e valor identificado. Se o risco decorre da localização precisa, por exemplo, pode ser necessário generalizar ou remover a localização. Se o risco decorre da granularidade dos registros, pode ser necessário agregar os dados. Se o risco decorre da combinação de variáveis, pode ser necessário remover ou modificar algumas colunas da base. Cabe lembrar que as medidas mencionadas aqui tem caráter exemplificativo e não devem limitar os controladores

A adoção de medidas de mitigação devem, em primeiro lugar, ser voltadas à redução dos riscos identificados. Nessa etapa, o objetivo principal é diminuir a probabilidade de ocorrência do risco, reduzir seu impacto ou, quando possível, atuar simultaneamente sobre essas duas dimensões.

Após a definição das medidas de redução de riscos, deve-se verificar quais efeitos essas medidas produzem sobre o valor da divulgação dos dados. Isso é necessário porque, em alguns casos, a mitigação pode preservar integralmente o valor da abertura e em outros, pode reduzi-lo. Por exemplo, a remoção de identificadores diretos pode reduzir riscos sem comprometer de forma significativa a utilidade de uma determinada base de dados de saúde. Já a agregação excessiva dos dados pode diminuir sua utilidade para pesquisas, controle social ou formulação de políticas públicas.



Caso a medida de mitigação reduza o risco sem comprometer o valor da divulgação, ela poderá ser adotada sem maiores ajustes. No entanto, se a medida de mitigação diminuir o valor da disponibilização dos dados, deve-se avaliar a possibilidade de adoção de medidas de promoção do valor. Essas medidas têm a finalidade de recuperar, preservar ou ampliar a utilidade pública da base, sem reintroduzir riscos desnecessários aos titulares.

Essa ordem é relevante pois evita-se que a tentativa de ampliar o benefício da abertura dos dados acabe aumentando novamente os riscos já identificados. Em outras palavras, as medidas de promoção do valor devem ser pensadas a partir do novo cenário produzido pela mitigação do risco.

O processo de mitigação não se limita à redução abstrata dos riscos. Ele exige uma análise dinâmica entre risco e valor: cada medida adotada deve ser observada tanto pelos seus efeitos protetivos quanto pelos seus impactos sobre a finalidade pública da divulgação. Por isso, ao final dessa etapa, devem ser recalculados o grau do risco e o grau do valor, considerando o cenário resultante das medidas aplicadas. A partir desses novos valores, realiza-se novamente a análise de custo-benefício, agora com base no risco residual e no valor remanescente ou promovido da disponibilização dos dados.



Passo 5 - Definição do custo-benefício final

Depois da definição das medidas de mitigação, a metodologia exige uma nova avaliação de custo-benefício. Nessa etapa, deve-se verificar os impactos das medidas de mitigação no valor e nos riscos para definir qual será o custo-benefício final.

O *valor final* corresponde ao valor que permanece após a adoção das medidas de mitigação.

O risco residual corresponde ao risco que permanece após a adoção das medidas de mitigação. Ao comparar os dois, se tem o custo-benefício final;

Essa reavaliação é essencial porque uma medida de mitigação pode reduzir o risco, mas também pode reduzir o valor da abertura dos dados. Nesse sentido, a análise residual deve responder a algumas situações principais.

Caso o risco continue alto, mesmo após a mitigação, a disponibilização deve ser revista. Caso o valor seja completamente eliminado, a abertura pode não fazer sentido. O objetivo é encontrar uma forma de divulgação em que o risco seja reduzido e o valor da divulgação do dado permaneça.

Passo 6 - Decisão sobre a disponibilização dos dados

Ao final da metodologia, a decisão sobre a disponibilização dos dados deve considerar o custo-benefício residual após a mitigação.

D

Com base nessa análise, a decisão pode seguir três caminhos principais:

Quadro 16 - Indicadores de custo-benefício

Resultado da análise	Decisão possível
Ótimo custo-benefício	A disponibilização dos dados pode ser realizada.
Médio custo-benefício	A disponibilização pode ocorrer, contudo, é preciso de monitoramento adequado para verificar eventual evolução dos riscos e diminuição do valor com o tempo.
Custo-benefício ruim	A disponibilização não deve ocorrer ou deve ser profundamente reformulada.

Fonte: Elaboração própria.

Essa decisão deve ser justificada de forma clara, indicando por que determinada forma de abertura foi escolhida, quais riscos foram identificados, quais medidas foram adotadas e qual risco permanece após a mitigação.

Essa justificativa deve ser apresentada independentemente do resultado da análise, pois a metodologia não possui caráter definitivo sobre a decisão a ser tomada. Seu resultado deve ser compreendido como um elemento de apoio à tomada de decisão, capaz de qualificar a avaliação do controlador, mas não de substituir a necessidade de fundamentação, ponderação e responsabilidade institucional sobre a disponibilização dos dados.

O

Limitações

Ainda que a metodologia de riscos e benefícios seja especialmente útil para uma tomada de decisão informada para programas de dados abertos, ela não informa riscos intoleráveis. Tipos de risco que mesmo que os benefícios sejam os melhores, não podem ser tomadas.

Em geral, essas situações estão definidas por leis e atos normativos dos órgãos controladores dos dados e que definem as políticas de uso de dados. No caso do poder público, a indicação desses riscos intoleráveis deve ser feita por meio de orientações internas de cada órgão em combinação com as emitidas pela Controladoria-Geral da União (CGU). Atualmente, a Instrução Normativa Conjunta 01/ 2016 da CGU dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

CONCLUSÃO

CONCLUSÃO

O presente trabalho apresentou uma metodologia que equilibrasse transparência pública e proteção de dados pessoais na abertura de dados públicos.

A partir da revisão bibliográfica, entrevistas com gestores públicos e análise de casos concretos, verificou-se uma lacuna relevante no campo: a sobreposição de medidas de privacidade sobre o potencial interesse público na divulgação de dados. Alguns casos emblemáticos, como os microdados do Censo Escolar e Exame Nacional do Ensino Médio, do Inep, apontam a importância do tema. A partir do diagnóstico de potencial reidentificação de titulares de dados, o Instituto retirou toda a série histórica do acesso público, com efeitos para uma série de atores públicos e privados. A atuação da ANPD reforça a importância do tema e de uma análise mais complexa, que considere a reidentificação e a exposição de dados pessoais não como um elemento por si só intolerável ou abusivo, mas como um primeiro passo para se analisar quais riscos de fato são decorrentes desta reidentificação. Para isso, a Agência recomendou que um relatório de impacto à proteção de dados fosse conduzido, com objetivo de analisar os riscos de forma mais específica e, a partir desta análise, tomar decisões informadas acerca da melhor forma de disponibilização ou não de dados pessoais.

Mediante o diagnóstico, buscou-se qualificar o debate público acerca de dois direitos fundamentais inserindo os benefícios provenientes da disponibilização de dados – inclusive pessoais. Adotando critérios já estabelecidos pelo MGI em seu modelo de RIPD e referências do campo da análise de riscos e proteção de dados, o relatório propõe uma metodologia de custo-benefício para a abertura de dados pelo poder público brasileiro. A proposta supera uma visão exclusiva de risco à proteção de dados, incluindo o valor como variável a ser considerada durante o processo decisório. Para tanto, valor e risco devem ser considerados a partir da probabilidade de ocorrência, bem como o impacto causado.

Como resultado, tem-se não apenas uma reflexão teórica sobre o tema, mas um instrumento metodológico que apoie a tomada de decisões do poder público diante de casos complexos envolvendo transparência e proteção de dados. Para isso, desenvolveu-se uma planilha automatizada com o objetivo de ser utilizada por agentes públicos na abertura de dados.

Dois casos paradigmáticos foram utilizados como exemplo de aplicação da metodologia proposta: dados do ICMBio relativos a áreas embargadas, e a plataforma Divulga Cand Contas, do Tribunal Superior Eleitoral. Ainda que com ressalvas - tratam-se de dados já abertos e disponíveis publicamente - o objetivo foi demonstrar a viabilidade do projeto.

Esperamos que esta contribuição traga segurança jurídica a servidores e servidoras engajados na agenda de governo aberto, balanceando a proteção de dados pessoais e compromisso com transparência pública. A documentação de tal processo decisório fortalece a transparência do Estado brasileiro, cumprindo os princípios não apenas da administração pública, mas também da proteção de dados pessoais.

REFERÊNCIAS

AAIP - Agencia de Acceso a la Información Pública de Argentina; URCDP - Unidad Reguladora y de Control de Datos Personales de Uruguay. **Guía de Evaluación de Impacto en la Protección de Datos**. 2020. Disponível em: https://www.argentina.gob.ar/sites/default/files/guia_final.pdf. Acesso em: 26 mai. 2026.

AEPD - AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Gestión del riesgo y evaluación de impacto en tratamientos de datos personales**. Madrid: AEPD, 2021. Disponível em: <https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>. Acesso em: 26 mai. 2026.

AGU - ADVOCACIA GERAL DA UNIÃO. **Parecer nº 00156/2023/CAI/PFE-ICMBIO/PGF/AGU**. 2023. Disponível em: <https://buscalai.cgu.gov.br/busca/6192510>. Acesso em: 27 mai. 2026.

ANPD - AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo: hipóteses legais de tratamento de dados pessoais – legítimo interesse**. Brasília, DF: ANPD, 2024.

ANPD - AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 12/2023**. Processo SEI nº 00261.000730/2022-53. Brasília, DF: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-12-2023-cgf-anpd-inep.pdf/@@display-file/file>. Acesso em: 26 mai. 2026.

ANPD - AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 46/2022/CGF/ANPD**. Processo SEI nº 00261.000730/2022-53. Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/sei_00261-000730_2022_53-nt-46.pdf/@@display-file/file. Acesso em: 26 mai. 2026.

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Perguntas e respostas sobre relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. ANPD, 6 abr. 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 26 mai. 2026.

BIONI, B. R. **Regulação e proteção de dados pessoais: o princípio da accountability**. São Paulo: Forense, 2022.

BIONI, B; SILVA, P; MARTINS, P. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU, [S.l.], n. 1, p. 8-19, 2022**. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504. Acesso em: 25 mai. 2026.

BRASIL. **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: 26 mai. 2026.

BRASIL. **Decreto nº 6.514, de 22 de julho de 2008.** Dispõe sobre as infrações e sanções administrativas ao meio ambiente, estabelece o processo administrativo federal para apuração destas infrações, e dá outras providências. Brasília, DF: Presidência da República, 2008. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6514.htm. Acesso em: 26 mai. 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 [...]. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 26 mai. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Presidência da República, DF: Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/l13709.htm. Acesso em: 25 mai. 2026.

BRASIL. **Lei nº 6.938, de 31 de agosto de 1981.** Dispõe sobre a Política Nacional do Meio Ambiente, seus fins e mecanismos de formulação e aplicação, e dá outras providências. Brasília, DF: Presidência da República, 1981. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6938.htm. Acesso em: 26 mai. 2026.

BRASIL. **Lei nº 9.605, de 12 de fevereiro de 1998.** Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9605.htm. Acesso em: 26 mai. 2026.

BRASIL. **Medida provisória nº 954, de 17 de abril de 2020.** Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 26 mai. 2026.



BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Guia/ Modelo de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais.** Brasília: Ministério da Gestão e da Inovação em Serviços Públicos, maio 2023. v. 2.

BRASIL. Ministro do Planejamento, Orçamento e Gestão. **Instrução normativa conjunta MP/CGU No 01, de 2016.** Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Disponível em: <https://basedeconhecimento.cgu.gov.br/server/api/core/bitstreams/dc705804-b-175-432f-afc9-7828031dcb3f/content>. Acesso em: 26 mai. 2026.

CGU - CONTROLADORIA GERAL DA UNIÃO. **Nota Técnica 136/2022/CGAT/DTC/STPC.** Processo nº 00190.104126/2022-86. 2022. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/noticias/2022/05/cgu-monitorea-publicacao-de-microdados-de-alunos-pelo-inep/SEI_CGU2376783NotaTcnica.pdf/@@download/file. Acesso em: 27 mai. 2026.

EQUIPE FIQUEM SABENDO. **Relatório analisa o impacto da LGPD no acesso à informações públicas.** Fiquem Sabendo, 6 mai. 2024. Disponível em: <https://fiquemsabendo.com.br/transparencia/relatorio-lgpd/>. Acesso em: 25 mai. 2026.

FACIO, R. N. A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil. **Revista Euro-**

latinoamericana de Derecho Administrativo, [S.l.], v. 10, n. 2. 2023. Disponível em: https://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S2362-583X2023000200007. Acesso em: 27 mai. 2026.



FPF - FUTURE OF PRIVACY FORUM. **City of Seattle Open Data Risk Assessment: final report. Washington, DC: Future of Privacy Forum, 2018.** Disponível em: <https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf>. Acesso em: 20 mai. 2026.

GELLERT, R. **Understanding the notion of risk in the General Data Protection Regulation.** Computer Law & Security Review, [S. l.], v. 34, n. 2, p. 279-288, abr. 2017. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364917302698>. Acesso em: 26 mai. 2026.

GOMES, M. C. O. **Relatório de Impacto a Proteção de Dados. Uma breve análise da sua definição e papel na LGPD.** Revista dos Advogados de São Paulo, São Paulo, n. 144, p. 6-15, 2019. Disponível em: https://mariaceciliagomes.com.br/wp-content/uploads/2022/01/Relatorio_de_Impacto_a_Protecao_de_Dados.pdf. Acesso em: 26 mai. 2026.

GOMES, M. C. O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In: PALHARES, F. (Coord.). **Temas atuais de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2020. p 245-271.

GREEN, B. et al. **Open Data Privacy.** Cambridge: Berkman Klein Center for Internet & Society, 2017. Disponível em: <https://dash.harvard.edu/entities/publication/73120379-064c-6bd4-e053-0100007fdf3b>. Acesso em: 26 mai. 2026.

KUHN, Thomas S. **A estrutura das revoluções científicas.** Tradução Beatriz Vianna Boeira e Nelson Boeira. São Paulo. Perspectiva Editora, 2018.

MACIEL, E. R. H.; GOMES, M. C. O. **Dossiê Relatório de Impacto e Risco.** São Paulo: Data Privacy Brasil Ensino, 2023.

MANTELERO, A.; ESPOSITO, M. S. **An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems.** Computer Law & Security Review, v. 41, p. 105561, jul. 2021. DOI: 10.1016/j.clsr.2021.105561. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364921000340>. Acesso em: 26 mai. 2026.

MENDES, L. S. F. **Autodeterminação informativa a história de um conceito.** Pensar Revista de Ciências Jurídicas, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. DOI: [https://doi.org/10.5020/2317-2150.2020.10828]. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828>. Acesso em: 25 mai. 2026.



MENKE, F. **As origens alemãs e o significado da autodeterminação informativa.** Migalhas. 30 out. 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa>. Acesso em: 26 mai. 2026.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guide for Conducting Risk Assessments.** Gaithersburg: NIST, 2012.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Privacy Framework: a tool for**

improving privacy through enterprise risk management, version 1.0. Gaithersburg, MD: National Institute of Standards and Technology, 2020.

RIBEIRO, E.; MACHADO, B. **Privacidade e transparência: aplicação dos testes de dano e interesse público em recursos da LAI.** Revista Jurídica da Presidência, Brasília, v. 21, n. 125, p. 615-643, out./jan. 2020. Disponível em: <https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/2028>. Acesso em: 27 mai. 2026.

SANTOS, P. H. **Relatório de inteligência: relatório de impacto à proteção de dados.** Revisão: Pedro Martins. São Paulo: Data Privacy Brasil; Clube Data, 2025

SILVA, P. G. F. O risco como elemento do sistema normativo de proteção de dados pessoais. In: BENTES, Anna et al. **Para além da proteção de dados: uma coletânea.** São Paulo: Data Privacy Brasil Ensino, 2023. p. 55-71. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/2b1c6bd8-6a55-4af-9-a151-e6424bab8ed1/content>. Acesso em: 26 mai. 2026.

STJ - SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial n. 1857.098 – MS. Ementa: processual civil.** Administrativo. Incidente de assunção de competência (IAC N. 13/STJ) [...]. Brasília, DF: STJ, 2022.

ZANATTA, R. **Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?** In: ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro. Anais [...]. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2017.

D

O

APÊNDICE A

APLICAÇÃO DA METODOLOGIA

Para a aplicação da metodologia, foram selecionados dois casos relevantes em que há a disponibilização de dados pessoais de forma aberta e que não tivessem um nível excessivamente elevado de complexidade, para facilitar a demonstração do modelo de forma mais clara.

O primeiro debruça-se sobre a abertura de dados do DivulgaCandContas, uma plataforma destinada a compilar dados sobre candidatos políticos. Já o segundo refere-se ao caso da abertura de dados de embargos e autos de infração do ICMBio, elencado no início deste relatório.

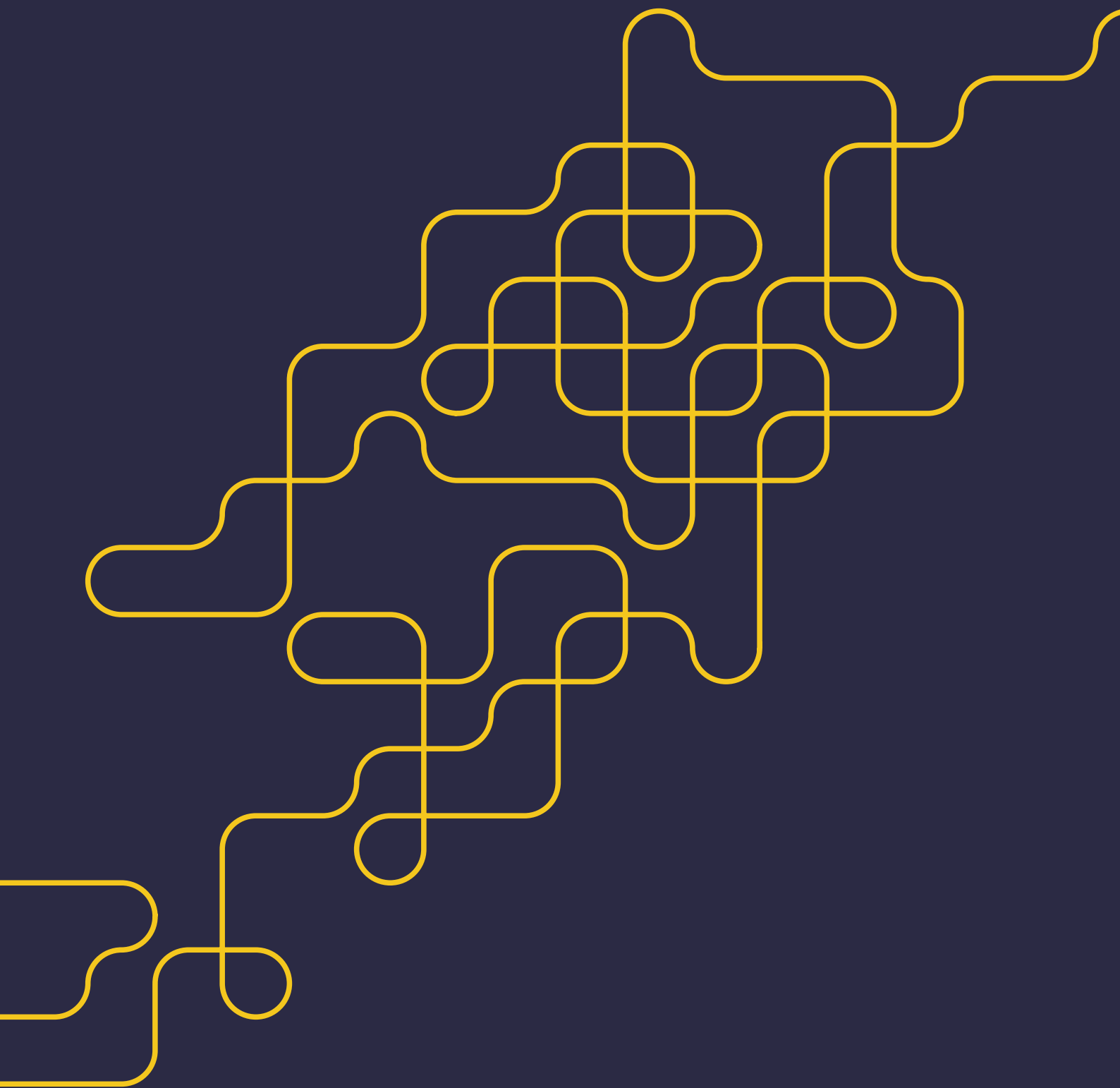
Os casos trazem perspectivas distintas uma vez que 1) os titulares lidam com níveis distintos de expectativa de privacidade - tratando-se primeiro de pessoas públicas, e em segundo, de proprietários de terras infratores que costumam não ter seus dados abertamente disponibilizados, mas que podem esperar algum nível de publicidade visto que os processos em que estão envolvidos são públicos; 2) são bases de dados distintas, no DivulgaCandContas contendo um número mais elevado de dados pessoais em relação às planilhas do ICMBio que divulga apenas nome e CPF; 3) o cenário em si é significativamente diferente, um é o contexto eleitoral, de auditoria de candidatos e das doações recebidas, e o outro relaciona-se à uma prestação de contas da administração pública frente a suas obrigações de controle e proteção ambiental.

Quanto aos benefícios da transparência destas bases de dados, o que une tais casos é a relevância das informações para o interesse público, sendo dados essenciais para o controle social, mas também podendo beneficiar outros setores da sociedade, por exemplo para o fomento à pesquisa científica, garantia do acesso à informação, fortalecimento do desenvolvimento de políticas públicas etc.

A análise teve essencialmente um objetivo exemplificativo da metodologia, a fim de testá-la e aprimorá-la. Portanto, a aplicação da metodologia se baseou apenas nos dados fornecidos pela plataforma do DivulgaCandContas e pelas planilhas de excel disponibilizadas pelo ICMBio, não sendo utilizados documentos extras com informações mais aprofundadas sobre como o tratamento de dados é conduzido internamente por cada órgão. Assim, cabe a ressalva de que os exemplos apresentados nos documentos de aplicação da metodologia tratam-se de uma simulação e não uma reprodução fidedigna das decisões tomadas pelos respectivos órgãos competentes. No mais, vale lembrar que por se tratarem de bases de dados já existentes e divulgadas a lógica de preenchimento é ligeiramente diferente de quando o tratamento de divulgação ainda está sendo idealizado, ou seja, quando o exercício imaginativo sobre os valores e riscos deverá ser mais intenso.

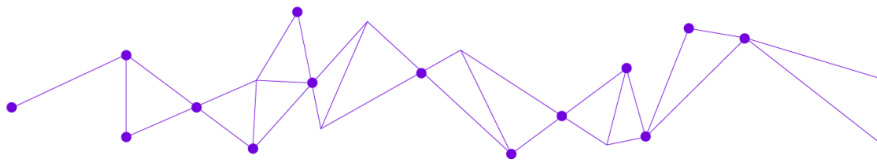
Os documentos que compõem este Apêndice são 3 planilhas:

1. Modelo - planilha sem preenchimento para ser utilizada como base para análise de custo-benefício de abertura de dados pessoais;
2. DivulgaCand - planilha com a simulação considerando o caso do Divulga Cand Contas; e
3. ICMBio - planilha com a simulação considerando o caso de divulgação de dados de infratores ambientais com terras embargadas e autos de infração.



The background of the entire page is a vibrant, high-tech image. It features a collage of four diverse professionals (two women and two men) looking upwards with expressions of hope and ambition. They are overlaid with glowing digital lines, circles, and data points. In the foreground, there is a glowing, circular digital interface with concentric rings and a bright light in the center, resembling a futuristic control panel or data visualization. The overall color palette is dominated by deep blues and purples, with bright highlights from the digital elements.

**Contribuições Softex –
consulta pública
Guia de Transparência
e Proteção de
Dados Pessoais**



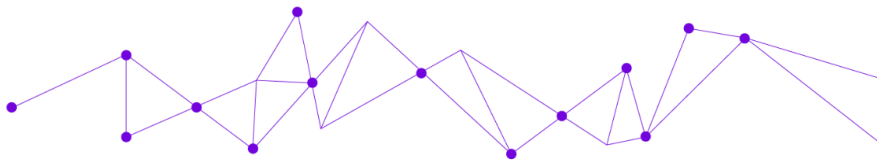
Contribuições à Guia de Transparência e Proteção de Dados Pessoais

Apresentação

A consulta pública sobre o Guia de Transparência e Proteção de Dados Pessoais, elaborado pela Controladoria-Geral da União (CGU) e pela Agência Nacional de Proteção de Dados (ANPD), representa uma oportunidade relevante para o aprimoramento das orientações destinadas a conciliar o direito de acesso à informação com a proteção da privacidade e dos dados pessoais. O documento constitui importante instrumento para fortalecer a transparência, a segurança jurídica e a atuação responsável da Administração Pública no tratamento e na divulgação de informações.

A Softex apresenta contribuições técnicas ao Guia com base em sua experiência na execução de políticas públicas, na produção de estudos e indicadores e na articulação de iniciativas de inovação, transformação digital, formação de talentos e desenvolvimento tecnológico. As propostas buscam favorecer o acesso responsável a dados para pesquisa e avaliação de políticas públicas, fortalecer a transparência e a segurança desde a concepção de sistemas e processos e estabelecer parâmetros mais claros para o uso de tecnologias, a contratação de soluções e a execução de iniciativas em parceria com terceiros.

Assim, a análise a seguir visa propor aprimoramentos técnicos ao texto-base, tornando suas orientações mais objetivas, previsíveis e aplicáveis aos diferentes contextos da Administração Pública.



Cap. 1 – Direito de acesso à informação e seus limites

Sugestão de contribuição estratégica 01

Contribuição: aprimoramento dos critérios utilizados para distinguir a simples extração e organização de dados já existentes da produção de nova informação pela Administração Pública.

Dispositivo do guia

Páginas 7, item 1.2 - Fundamentos administrativos para negativa de informação (Produção de informação)

Trecho original

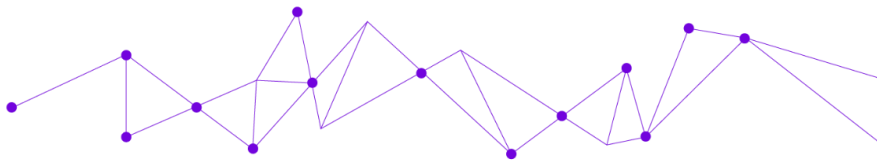
"Produção de informação: quando o atendimento exige que o órgão produza, analise, interprete, consolide ou trate dados que não existem da forma solicitada. Importante não confundir essa hipótese com o serviço da prestação da informação que inclui localizar, organizar e fazer explicação textual sobre a informação sob sua guarda. Ou seja, compilar documentos, localizar dados, montar uma resposta textual explicativa não é considerado trabalho de produção de informação."

Proposição

Recomenda-se esclarecer que a extração, filtragem, ordenação e o relacionamento de dados já armazenados em bases estruturadas não configuram, por si só, produção de nova informação. Quando o pedido puder ser atendido por consultas rotineiras, inclusive por relacionamento entre tabelas, deverá ser considerado atividade de localização e organização de dados. A caracterização de trabalho adicional deverá ficar restrita a situações que exijam desenvolvimento específico, integração de sistemas não interoperáveis, saneamento relevante, classificação manual, criação de metodologia, cálculo de indicador inédito ou esforço capaz de comprometer as atividades regulares do órgão. Nesses casos, a negativa deverá apresentar justificativa técnica e, sempre que possível, indicar alternativas de atendimento parcial.

Defesa técnica

O exemplo atual pode levar à interpretação de que qualquer cruzamento entre bases representa produção de informação. Em bancos de dados relacionais, contudo, filtros,



agrupamentos e relacionamentos entre tabelas são operações usuais de recuperação de dados já existentes. O art. 13, inciso III, do Decreto nº 7.724/2012 admite a negativa quando o pedido exige trabalhos adicionais de análise, interpretação, consolidação ou tratamento de dados (BRASIL, 2012, art. 13, III). A distinção, porém, deve considerar a complexidade efetiva da operação, e não apenas o uso de mais de uma tabela. A Lei de Governo Digital reforça a disponibilização de dados estruturados, legíveis por máquina e com maior granularidade (BRASIL, 2021, art. 29). A revisão proposta atualiza o Guia às arquiteturas atuais de dados, sem obrigar o órgão a produzir análises ou indicadores inexistentes.

Referências

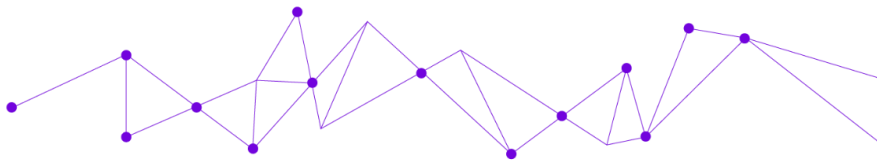
BRASIL. Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011. Diário Oficial da União: Brasília, DF, 16 maio 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. Diário Oficial da União: Brasília, DF, 30 mar. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm.



The background of the entire page is a vibrant, high-tech image. It features a collage of diverse professionals—men and women of various ethnicities—looking upwards with expressions of hope and ambition. Overlaid on this are glowing digital elements: concentric circles, data lines, and a futuristic interface at the bottom that resembles a control panel or a data visualization. The color palette is dominated by deep blues, purples, and magentas, with bright highlights from the digital effects.

**Contribuições Softex –
consulta pública
Guia de Transparência
e Proteção de
Dados Pessoais**



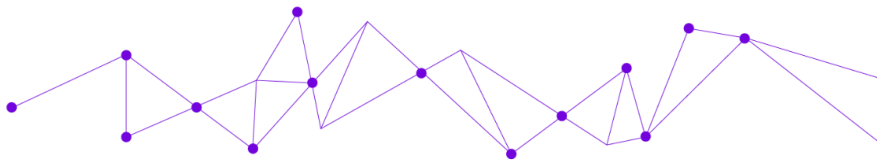
Contribuições à Guia de Transparência e Proteção de Dados Pessoais

Apresentação

A consulta pública sobre o Guia de Transparência e Proteção de Dados Pessoais, elaborado pela Controladoria-Geral da União (CGU) e pela Agência Nacional de Proteção de Dados (ANPD), representa uma oportunidade relevante para o aprimoramento das orientações destinadas a conciliar o direito de acesso à informação com a proteção da privacidade e dos dados pessoais. O documento constitui importante instrumento para fortalecer a transparência, a segurança jurídica e a atuação responsável da Administração Pública no tratamento e na divulgação de informações.

A Softex apresenta contribuições técnicas ao Guia com base em sua experiência na execução de políticas públicas, na produção de estudos e indicadores e na articulação de iniciativas de inovação, transformação digital, formação de talentos e desenvolvimento tecnológico. As propostas buscam favorecer o acesso responsável a dados para pesquisa e avaliação de políticas públicas, fortalecer a transparência e a segurança desde a concepção de sistemas e processos e estabelecer parâmetros mais claros para o uso de tecnologias, a contratação de soluções e a execução de iniciativas em parceria com terceiros.

Assim, a análise a seguir visa propor aprimoramentos técnicos ao texto-base, tornando suas orientações mais objetivas, previsíveis e aplicáveis aos diferentes contextos da Administração Pública.



Cap. 3 – Proteção de dados pessoais prevista na LAI

Sugestão de contribuição estratégica 01

Contribuição: aprimoramento das orientações sobre consentimento, representação e exercício de direitos relacionados às informações pessoais de titular morto ou ausente.

Dispositivo do Guia

Páginas 14 subitem 3.3. letra - a) Consentimento expresso do titular

Trecho original

"A Informação pessoal pode ser fornecida a terceiros mediante consentimento expresso do titular. Esse consentimento deve ser expresso e documentado, por exemplo, por meio de procuração ou declaração. Em caso de falecimento ou ausência do titular, o consentimento pode ser obtido junto ao cônjuge, companheiro, descendentes ou ascendentes."

Proposição 01

1ª Observação - Dúvida entre LGPD e Lei de Acesso à Informação (LAI)

O texto fundamenta a hipótese em "consentimento", mas a LAI já prevê hipóteses legais específicas para acesso a informações pessoais (art. 31). Misturar essas hipóteses com a base legal de consentimento da LGPD pode gerar insegurança jurídica.

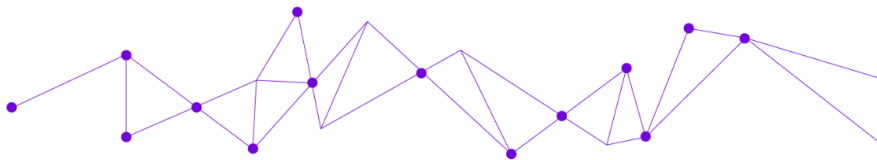
Risco: Confusão sobre qual regime jurídico está sendo aplicado. Interpretação de que o consentimento seria a única ou principal hipótese de acesso, quando a LAI estabelece outras possibilidades.

Sugere que o Guia deixe claro que o acesso decorre das hipóteses previstas na LAI e que o consentimento, quando utilizado, deve observar os limites da LGPD e da própria LAI.

Proposição 02

2ª Observação - Tratamento de dados de pessoa falecida

A LGPD protege dados de pessoas naturais vivas. Embora existam direitos da personalidade protegidos por outras normas (Código Civil, por exemplo), dizer que o



consentimento do cônjuge substitui o consentimento do falecido não encontra fundamento na LGPD.

Risco: Indução à interpretação de que existe uma sucessão automática do consentimento; e confusão entre proteção de dados pessoais e direitos sucessórios ou direitos da personalidade post mortem.

Sugere que o Guia separe completamente a situação de falecimento da situação de titular vivo. Exemplo: “Nos casos envolvendo informações de pessoa falecida, o acesso observará a legislação específica aplicável, não se fundamentando em consentimento substitutivo.”

Proposição 03

3ª Observação - Ausência do titular é um conceito extremamente aberto, o que se mostra preocupante, uma vez que o texto não explica o que significa “ausência”. Podendo gerar vários significados, tais quais: o titular pode estar viajando, hospitalizado, desaparecido ou declarado ausente judicialmente, conforme Código Civil, ou seja, cada hipótese produz consequências completamente diferentes. Risco: Acesso indevido a dados pessoais, interpretação extremamente ampla e até violação do princípio da autodeterminação informativa.

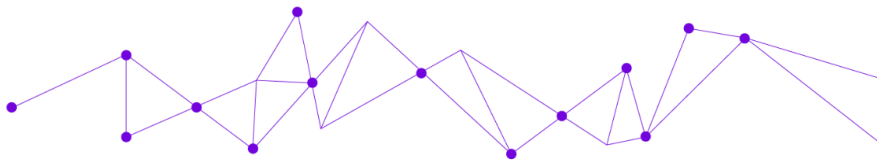
Sugere que o Guia defina objetivamente o conceito de ausência, ou restringir aos casos em que exista: representação legal; decisão judicial; procuração válida; curatela; ou outra forma legal de representação.

Proposição 04

4ª Observação - Consentimento por familiares

O texto praticamente cria uma ordem de pessoas autorizadas a consentir em nome do titular, mas isso não está previsto na LGPD, já que ser cônjuge, pai, mãe ou filho não transforma automaticamente alguém em representante legal. Além disso, mesmo admitindo alguma hipótese excepcional, o texto não expressa nenhuma verificação.

Risco: quebra da autonomia do titular; violação da autodeterminação informativa; acesso por familiares com interesses conflitantes; fraudes; engenharia social; acesso indevido a dados pessoais e até litígios familiares.



Recomenda-se que o Guia exija algum tipo de comprovação documental da relação; demonstração do interesse jurídico; registro da decisão administrativa ou a motivação expressa do acesso.

Proposição 05

5ª Observação - A Procuração está sendo tratada como consentimento, quando na verdade ela representa poderes de representação, ou seja, são institutos jurídicos diferentes.

Recomenda-se que o Guia separe claramente o consentimento prestado pelo próprio titular, do consentimento por representação de procurador regularmente constituído.

Sugestão de redação para o Guia considerando as observações e os riscos

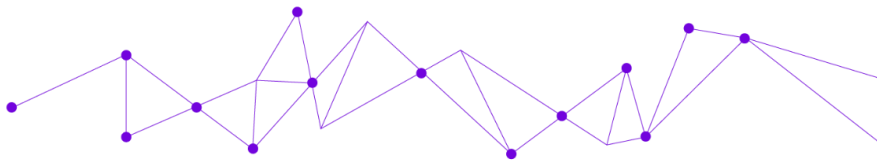
“A informação pessoal poderá ser fornecida a terceiros mediante consentimento expresso do titular, devidamente documentado, ou por intermédio de representante legal ou procurador regularmente constituído, observadas as hipóteses previstas na Lei nº 12.527/2011 e na legislação aplicável. Nos casos de falecimento do titular ou de impossibilidade de manifestação de vontade, o acesso às informações deverá observar a legislação específica, não sendo admitida autorização automática por cônjuge, companheiro, ascendentes ou descendentes, salvo quando houver representação legal ou previsão normativa expressa.”

Observação adicional

A expressão “ausência do titular” remete a um conceito jurídico já existente no Código Civil (arts. 22 a 39), que pressupõe um procedimento específico e, em determinadas fases, declaração judicial. Se a intenção da minuta não é fazer referência a esse instituto, o termo é tecnicamente inadequado e pode gerar interpretações equivocadas. Se a intenção é utilizá-lo no sentido jurídico, então o texto deveria remeter expressamente ao regime do Código Civil. Caso contrário, recomenda-se substituí-lo por uma expressão mais precisa, como “impossibilidade comprovada de manifestação de vontade”, acompanhada dos critérios objetivos para sua caracterização.

Defesa técnica

Isso pode ser considerado um problema de técnica normativa que pode gerar insegurança jurídica e aplicações divergentes pelos órgãos públicos.



Sugestão de contribuição estratégica 02

Contribuição: aprimoramento das orientações sobre verificação de identidade no atendimento de solicitações de acesso a informações pessoais, especialmente quando o tratamento dos dados ou a execução da política pública envolver entidades privadas atuando em nome da Administração Pública.

Dispositivo do Guia:

Página 13 subitem 3.2. Acesso pelo titular à própria informação pessoal.

Trecho original

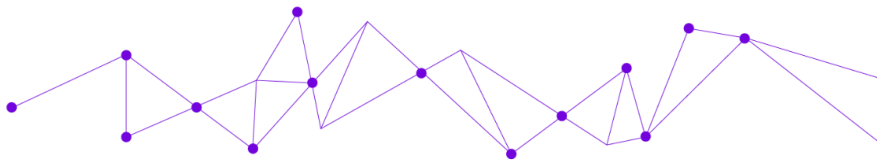
"O titular do dado pessoal pode utilizar a LAI para solicitar ao Estado suas próprias informações pessoais. O atendimento ao pedido, no entanto, é condicionado à comprovação da identidade do solicitante (art. 60 do Decreto no 7.724/2012). Essa comprovação pode ocorrer por apresentação presencial de documentos ou por utilização do Selo de Confiabilidade do Governo Federal nos níveis Ouro ou Prata, que asseguram a identidade do usuário no acesso aos sistemas governamentais."

Proposição

Identifica-se insegurança sobre quem pode realizar a autenticação, principalmente em casos em que não é a Administração Pública operando, mas sim uma entidade do terceiro setor. Tal lacuna gera um risco de acesso indevido, pois se não houver autorização para exigir mecanismos robustos de autenticação, a entidade pode acabar entregando dados pessoais a alguém que apenas afirma ser o titular. Além disso, pode gerar desigualdade de tratamento, pois o mesmo cidadão teria níveis de segurança diferentes dependendo de quem recebeu o pedido, se foi a Administração Pública ou uma entidade do terceiro setor.

Risco: isso aumenta o risco de fraude documental; engenharia social; vazamento de dados; e a responsabilização da entidade.

Nossa análise parte da premissa de que se determinada entidade executa atividade pública delegada ou contratada, tratando dados pessoais em nome da Administração Pública, os mecanismos mínimos de autenticação do titular também deveriam poder ser utilizados por essa entidade, respeitados os limites contratuais e a LGPD. Isso não significa transformar uma entidade executora em órgão público, mas permitir que ela adote o mesmo padrão de segurança para proteger o titular.



Recomenda-se que a orientação contemple também as entidades privadas que executam políticas públicas ou realizam tratamento de dados pessoais em nome da Administração Pública, especialmente na condição de operadoras ou executoras contratuais. Nessas hipóteses, deveria ser admitida a adoção dos mesmos mecanismos de verificação de identidade previstos para os órgãos públicos, observadas as atribuições contratuais e a legislação aplicável.

Dessa forma, o texto do Guia poderia contemplar as entidades privadas que realizem tratamento de dados pessoais em nome da Administração Pública, e autorizar que elas possam adotar mecanismos equivalentes de verificação da identidade do titular para atendimento de solicitações relativas às suas informações pessoais, observados os limites estabelecidos pelo controlador e pelas normas de proteção de dados pessoais.

Defesa técnica

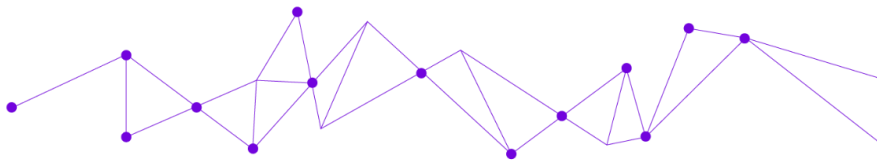
Tais observações são tecnicamente consistentes porque não amplia direitos nem cria bases legais de tratamento. Ela apenas busca garantir que as entidades que executam políticas públicas em nome do Estado possam aplicar o mesmo padrão de segurança previsto para a Administração Pública, protegendo tanto os titulares quanto as próprias entidades executoras.

Sugestão para o Guia considerando as observações e os riscos

Prever expressamente sua aplicação às entidades privadas que tratem dados pessoais em nome da Administração Pública, como operadoras ou executoras de políticas públicas, autorizando essas entidades a utilizar os mesmos critérios de verificação de identidade adotados pelos órgãos públicos, evitando assimetrias e reduzindo riscos de fraude, evitar mencionar exclusivamente o Gov.br Ouro/Prata ou a apresentação presencial de documentos, prevendo também “outros mecanismos que assegurem nível equivalente de confiabilidade na autenticação da identidade do titular”. Isso torna a norma mais resiliente à evolução tecnológica.

Sugestão de contribuição estratégica 03

Contribuição: padronização do acesso a dados para estudos e pesquisas de interesse público.



Dispositivo do guia

Páginas 14 e 15, item 3.3 d) Estatísticas e Pesquisas

Trecho original

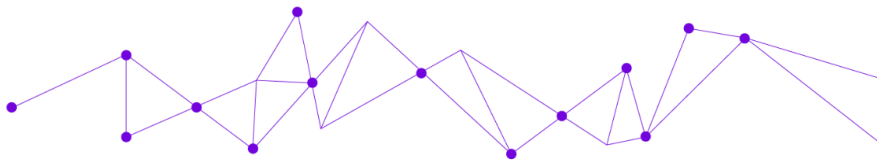
"A LAI permite o tratamento e a entrega de dados pessoais, sem consentimento, para fins estatísticos ou de pesquisa científica, mas exige o atendimento de requisitos específicos. A lei determina, por exemplo, que a pesquisa tenha objetivos de evidente interesse público ou geral. É importante destacar que, conforme entendimento da ANPD, a LGPD não estabeleceu a anonimização ou a pseudonimização como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais para fins de realização de estudos e pesquisas, devendo-se reconhecer, inclusive, que, em alguns casos, a identificação dos titulares pode ser imprescindível para os objetivos da pesquisa."

Proposição

Recomenda-se que os órgãos e entidades disponibilizem plataforma, formulário eletrônico ou canal institucional padronizado para solicitação e acompanhamento do acesso a dados pessoais destinados à realização de estudos e pesquisas de evidente interesse público ou geral. A solicitação deverá informar, no mínimo, a instituição e os pesquisadores responsáveis, os objetivos e a finalidade pública do estudo, as bases de dados, variáveis e períodos requeridos, a justificativa da granularidade e da necessidade estrita de cada variável para o estudo, os cruzamentos ou vinculações previstos, as pessoas autorizadas a acessar os dados, as medidas de segurança, o prazo de retenção, a forma de divulgação dos resultados e a formalização por meio de Termo de Responsabilidade. A plataforma também deverá permitir o registro de alterações relevantes no plano de uso dos dados, como a inclusão de novas variáveis, bases, cruzamentos, integrantes da equipe ou finalidades analíticas. Mudanças capazes de ampliar os riscos aos titulares deverão ser submetidas à nova avaliação pelo órgão responsável ou por um Comitê de Revisão/Acesso a Dados (DAC). Quando as informações apresentadas forem insuficientes, deverá ser oportunizada sua complementação antes da decisão final. A eventual negativa deverá ser motivada e, sempre que possível, indicar modalidade alternativa de acesso, priorizando o fornecimento de dados de forma anonimizada ou pseudonimizada.

Defesa técnica





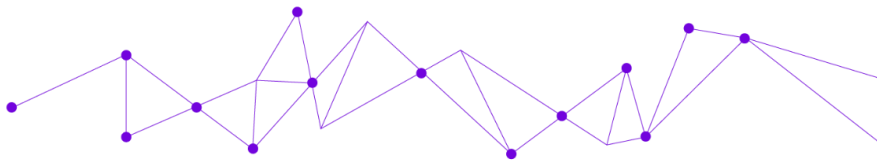
A minuta reconhece a possibilidade de fornecimento de dados pessoais para estudos e pesquisas de interesse público e apresenta requisitos fundamentais relacionados à instituição solicitante, aos dados requeridos, à exigência de Termo de Responsabilidade e à adoção de medidas de proteção. Entretanto, essas orientações não estão organizadas em um procedimento único que permita registrar e acompanhar todo o ciclo de vida dos dados na pesquisa. Durante a execução da pesquisa, frequentemente surgem necessidades de incluir novas variáveis, ampliar períodos, integrar outras bases ou realizar cruzamentos inicialmente não previstos (GARFINKEL, 2023). Essas alterações metodológicas podem modificar drasticamente o risco de reidentificação e a exposição dos titulares (risco inferencial), especialmente quando diferentes bases são vinculadas ou quando há aumento da granularidade das informações. A adoção de uma plataforma ou canal padronizado contribuiria para a rastreabilidade das decisões, a uniformização dos pedidos e o controle rigoroso das condições de acesso. Isso garante, por exemplo, a aplicação do princípio da minimização e necessidade, ao exigir que os pesquisadores justifiquem a inclusão de cada variável solicitada, prática adotada internacionalmente no acesso a microdados. Uma governança estruturada, preferencialmente apoiada pela criação de Comitês de Acesso a Dados (*Data Access Committees* - DACs ou *Disclosure Review Boards* - DRBs), também evitaria que uma autorização inicial fosse interpretada como permissão genérica para usos posteriores não informados (ONS; DFE, 2026), também evitaria que uma autorização inicial fosse interpretada como permissão genérica para usos posteriores não informado. A proposição visa assegurar que o órgão detentor disponha de todas as informações estruturadas necessárias para analisar a finalidade, a necessidade, a proporcionalidade e os riscos do tratamento, equilibrando a promoção e avanço da ciência com a proteção da privacidade dos titulares

Referências

GARFINKEL, Simson L.; NEAR, Joseph; DAJANI, Aref; SINGER, Phyllis; GUTTMAN, Barbara. De-identifying government datasets: techniques and governance. Gaithersburg, MD: *National Institute of Standards and Technology*, 2023. (NIST Special Publication 800-188). Disponível em: <https://doi.org/10.6028/NIST.SP.800-188>.

OFFICE FOR NATIONAL STATISTICS (ONS); DEPARTMENT FOR EDUCATION (DFS). *Researcher application guidance: access via the Secure Research Service (SRS)*. Version 1. [S. l.]: Office for National Statistics; Department for Education, fev. 2026. 11 p. Disponível em: <https://www.ons.gov.uk/file?uri=%2Faboutus%2Fwhatwedo%2Fstatistics%2Frequestingstatistics%2Fsecureresearchservice%2Fdiscoversecureresearchdata%2Fleoresearcherapplicationguidance.pdf>





Sugestão de contribuição estratégica 04

Contribuição: governança de dados públicos utilizados como insumo de treinamento de modelos de inteligência artificial.

Dispositivo do Guia

Página 14-15, item 3.3 (d) Estatísticas e Pesquisas.

Trecho original

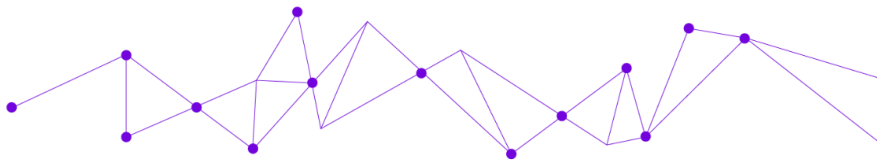
“A LAI permite o tratamento e a entrega de dados pessoais, sem consentimento, para fins estatísticos ou de pesquisa científica, mas exige o atendimento de requisitos específicos. A lei determina, por exemplo, que a pesquisa tenha objetivos de evidente interesse público ou geral. É importante destacar que, conforme entendimento da ANPD, a LGPD não estabeleceu a anonimização ou a pseudonimização como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais para fins de realização de estudos e pesquisas [...]”

Proposição

Recomenda-se que o Guia inclua orientação específica sobre o uso de dados pessoais constantes de bases públicas, inclusive os liberados em transparência ativa ou em resposta a pedidos de LAI, como insumo de treinamento, ajuste fino (*fine-tuning*) ou avaliação de modelos de inteligência artificial. Essa hipótese deve ser tratada separadamente da exceção de “estatísticas e pesquisas” (item 3.3.d), pois o treinamento de modelos por empresas de tecnologia, órgãos públicos ou desenvolvedores individuais frequentemente não se enquadra na definição legal de “órgão de pesquisa” (art. 5º, XVIII, da LGPD), que pressupõe finalidade não comercial ou institucional de pesquisa científica.

O Guia deveria orientar que, quando dados pessoais constantes de bases públicas forem utilizados para treinamento de modelos de IA:

- o órgão detentor avalie previamente se a base contém dados pessoais sensíveis, dados de grupos vulneráveis ou informações passíveis de reidentificação por combinação com outras bases (risco de vazamento por memorização do modelo, model inversion e membership inference);
- sejam priorizadas técnicas de minimização e anonimização compatíveis com a finalidade de treinamento, sem prejuízo do reconhecimento, já feito no próprio Guia, de que a anonimização não é condição obrigatória em todos os casos;



- seja registrada a finalidade específica do uso do dado como insumo de treinamento, distinta da finalidade original de coleta, com avaliação do princípio da adequação (art. 6º, II, da LGPD);
- terceiros que utilizem dados públicos para treinar modelos comerciais assinem instrumento equivalente ao Termo de Responsabilidade, com vedação à reidentificação de titulares e ao uso do dado para finalidade diversa da autorizada.

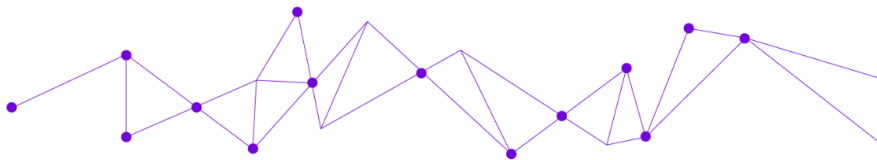
Defesa técnica

O Guia trata adequadamente do uso de dados pessoais para “estudos e pesquisas”, mas essa categoria foi pensada para pesquisa acadêmica, estatística ou científica tradicional, não para o cenário atual de treinamento de modelos de IA generativa, que pode ocorrer por atores privados com finalidade comercial. Essa distinção é relevante porque modelos de IA generativa podem reter e, em certas condições, expor trechos de dados de treinamento (fenômeno de memorização), o que cria um vetor de risco à privacidade dos titulares distinto da divulgação de um dado isolado, o risco se manifesta de forma indireta e potencialmente amplificada, através das respostas geradas pelo modelo.

O Marco Legal da Inteligência Artificial (PL nº 2.338/2023), aprovado pelo Senado Federal em dezembro de 2024 e em tramitação na Câmara dos Deputados, adota modelo de regulação baseado em risco e prevê exigências de transparência, avaliação de risco e responsabilização quanto a decisões automatizadas, o que reforça a oportunidade de o Guia já orientar os órgãos públicos sobre o tratamento cuidadoso de suas bases de dados quando usadas para esse fim, independentemente da conclusão da tramitação legislativa. De forma complementar, o *NIST AI Risk Management Framework* (AI RMF 1.0; NIST, 2023) já consolida, internacionalmente, boas práticas de governança de dados de treinamento como parte da gestão de riscos de sistemas de IA, servindo de referência técnica não vinculante, mas amplamente adotada.

A proposição não pretende impedir o uso de dados públicos para o desenvolvimento de soluções de IA, pelo contrário, busca viabilizá-lo com segurança jurídica, orientando os órgãos públicos a diferenciar, desde já, a finalidade de “pesquisa” da finalidade de “treinamento de modelo”, e a aplicar salvaguardas proporcionais ao risco de reidentificação indireta.

Referências



NIST. *AI Risk Management Framework (AI RMF 1.0)*. National Institute of Standards and Technology, 2023. Disponível em: <https://www.nist.gov/itl/ai-risk-management-framework>.

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Aprovado pelo Plenário do Senado Federal em 10 dez. 2024; em tramitação na Câmara dos Deputados. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>.





MINISTERIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

ARQUIVO NACIONAL

DIRETORIA DE GESTÃO DE DOCUMENTOS / DGD

RECOMENDAÇÕES AO GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

Brasil Participativo - Consulta Pública

27 de julho de 2026

ENCAMINHAMENTOS:

Observação: As recomendações de alteração ou inclusão de redação estão em itálico.

Capítulo 1: Direito de acesso à informação e seus limites

1.2. Exceções da transparência

Documentos preparatórios

a) Proposta de inclusão de texto sobre a diferença de documentos preparatórios (documentos formais) para os rascunhos e minutas, na p.5, como se segue:

...

Diferentemente dos sigilos legais, a possibilidade de restrição temporária a documentos preparatórios está prevista na própria LAI (§ 3º do art. 7º). Trata-se de informações ou documentos que subsidiam uma decisão ou ato ainda em processo de elaboração no âmbito do poder público.

[Proposta de inclusão] No âmbito da LAI, os documentos preparatórios são definidos como documentos formais, utilizados para fundamentar a tomada de decisão ou a formalização do ato administrativo. Como exemplos: temos os estudos preliminares, pareceres ou notas técnicas. Ou seja, os documentos preparatórios compõem o conjunto documental pertinente à atividade que resultarão na tomada de decisão. Não devem ser confundidos com rascunhos ou minutas, conceituados como esboços ou versões preliminares, sem valor arquivístico, de um documento a ser produzido.

....

Justificativa: O texto original não deixa claro o conceito de documento preparatório, o que faz com que o leitor confunda este com rascunhos ou minutas, sem valor arquivístico e sujeitos à eliminação sumária.

b) Proposta de alteração e inclusão de texto sobre a definição de gestão de documentos na p.7, como se segue:

Por fim, é importante destacar que o pleno exercício do direito de acesso à informação depende do constante **aprimoramento da gestão documental**, com sistemas e processos que viabilizem a adequada produção, organização, preservação e disponibilização das informações públicas, conforme determinam a Constituição Federal, a LAI *[Proposta de inclusão]* e a própria Lei de Arquivos (Lei 8.159, de 8 de janeiro de 1991). Ou seja, um órgão não pode se eximir indefinidamente de atender um pedido de informação por dificuldades operacionais; ele tem o dever de melhorar seus processos e sistemas para garantir que a sociedade tenha acesso às informações públicas, cumprindo os princípios da transparência, eficiência e interesse coletivo.

[Proposta de inclusão] Os documentos produzidos pela administração pública devem ser protegidos e submetidos a procedimentos e atividades de gestão de documentos, de acordo com a Lei n. 8.159, de 8 de janeiro de 1991, que também define, em seu art. 3º, a gestão de documentos como um “conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em idade corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente”.

Justificativa: É importante apresentar o conceito de gestão de documentos e sua previsão legal, uma vez que não se trata de uma ideia abstrata e subjetiva.

Capítulo 3: Proteção de dados pessoais prevista na LAI

3.3 Acesso por terceiros à informação pessoal protegida

g) Recuperação de fatos históricos

a) Proposta de inclusão de texto que contextualiza a recuperação de fatos históricos sobre a ótica da gestão de documentos, na p.16, como se segue:

Quando se tratar de documentos destinados à guarda permanente, caberá ao Arquivo Nacional ou aos arquivos públicos setoriais aplicar o mesmo procedimento.

[Proposta de inclusão] Destaca-se que são destinados à guarda permanente os documentos que, após avaliação, foram identificados, por seus valores históricos, probatórios ou informativos, para além da função para os quais foram originalmente criados e mantidos e que por isso foram considerados necessários a serem preservados permanentemente.

Justificativa: Se deve ter atenção ao uso do termo “valor histórico” quando se trata de documentos de arquivo. Entende-se que é um termo muito amplo, uma vez que é passível da interpretação subjetiva que se dá ao documento. Em linhas gerais, qualquer documento pode ter valor histórico, até um bilhete de “volto logo”, dependendo de seu contexto de produção. A arquivística persegue a ideia de valor

secundário, por meio de metodologia de avaliação, quando se tenta identificar se o documento, após cumprir a função original para qual foi criado, se pode a ele atribuir valor e interesse para a pesquisa, informação ou mesmo probatório, por exemplo. O Dicionário Brasileiro de Terminologia Arquivística (Resolução do CONARQ, nº 23 de 16 de junho 2006) apresenta a seguinte definição para o termo valor secundário: “Valor atribuído a um documento em função do interesse que possa ter para a entidade produtora e produtora outros usuários, usuários tendo em vista a sua utilidade para fins diferentes daqueles para os quais foi originalmente produzido”. Assim posto, entendemos a necessidade de aplicação cautelosa do termo “valor histórico” no guia.

Também recomendamos consulta a RESOLUÇÃO CONARQ Nº 54, DE 8 DE DEZEMBRO DE 2023, que “Estabelece diretrizes e regras para a aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), aos arquivos permanentes custodiados por pessoa física ou jurídica de direito público ou privado”. Esta Resolução do CONARQ pode ser inserida no Guia como referência, uma vez que esclarece e instrumentaliza as instituições arquivísticas públicas e aos arquivos privados considerados de interesse público e social.

Capítulo 4: Garantindo a transparência pública com proteção dos dados pessoais

4.3. Transparência por desenho

Revisar fluxos de trabalho e procedimentos

a) Proposta de exclusão de parágrafo que indica procedimentos a serem adotados para disponibilização de documentos por meio do SEI, na p.30, conforme se segue:

~~[Proposta de exclusão] Se o órgão usa do Sistema Eletrônico de Informações (SEI) como plataforma digital de gestão de documentos e processos administrativos, pode-se criar dois processos relacionados. O processo principal seria de acesso público, e referenciaria os documentos restritos que estariam no processo relacionado. Esse último seria categorizado como de acesso restrito. Outra opção é 31 armazenar duas versões de um documento que contém trechos restritos: uma que contém a informação na sua integralidade, e outra tarjada.~~

Justificativa: O SEI não é uma plataforma de gestão de documentos, com funcionalidades análogas a um Sistema Informatizado de Gestão Arquivística de Documentos – SIGAD. Para tanto, precisaria desenvolver um conjunto de procedimentos e operações técnicas característicos do sistema de gestão arquivística de documentos, sendo processado eletronicamente e aplicável em ambientes digitais ou em ambientes híbridos, isto é, em que existem documentos digitais e não digitais ao mesmo tempo (e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos, 2022). O SEI é uma plataforma digital concebida para a produção, controle e tramitação de processos administrativos, e não para difusão ou simples acesso a documentos. Ao sugerirem criar no SEI dois processos relacionados, com documentos ostensivos e outros com acesso restrito, conduzem à desconformidade com os procedimentos de protocolo, à duplicidade de informações e interferem na capacidade de processamento das informações e no volume de dados guardados desnecessariamente, comprometendo a performance do SEI. Compreendemos a intenção de transformar o SEI em uma ferramenta da transparência ativa, contudo o caminho apontado é inadequado. Custodiar e gerenciar dados sensíveis apartados dos documentos principais, como mencionado em parágrafos anteriores, é uma opção válida. Contudo, duplicar os processos SEI, na prática é inviável. Deve se levar em consideração a necessidade de cada órgão ou entidade analisar cada processo, volume a volume, descaracterizando documentos e duplicando em outros processos e considerando que será feito não somente em processos concluídos, mas nos ativos correntes, que seguem seu curso e diariamente são atualizados. Outro ponto é a temporalidade desse processo “cópia”: em certos casos, também deverá seguir os prazos de 52, 57, 100 anos de guarda, o mesmo do processo principal? Sim, a ideia é boa, mas impraticável.

Criar funcionalidades de consulta e extração de dados para ampla divulgação

b) Proposta de inclusão de texto que indica a vedação de cadastro prévio na transparência ativa, na p.31, conforme se segue:

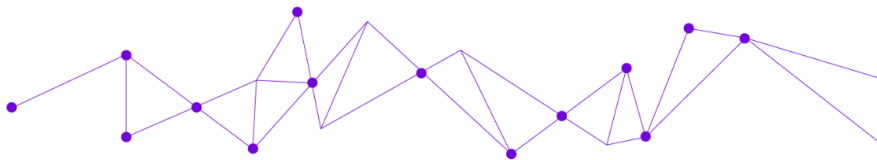
Também é uma alternativa permitir a consulta ou extração de dados agregados, sem a individualização que permita a identificação de dados pessoais protegidos. Essa prática é especialmente relevante em bases relacionadas a beneficiários de políticas públicas, controle de acesso a prédios públicos, cadastros administrativos e bases utilizadas para fins estatísticos ou de pesquisa, permitindo a divulgação de dados como valores, quantitativos, localidade ou datas, sem identificação direta dos titulares.

[Proposta de inclusão] Os portais das redes públicas governamentais que disponibilizam conjuntos de informações e documentos (data sets) por meio da Transparência Ativa e Dados Abertos, não deverão criar barreiras para o acesso do usuário por meio de mecanismos ou procedimentos de cadastro e identificação.

Justificativa: Tenta-se vedar que portais governamentais criem barreiras ao acesso a informações disponibilizadas por meio da transparência ativa com cadastro prévio e retenção de informações sensíveis que podem embaraçar ou causar constrangimento ao usuário em saber que o registro de acesso a determinada informação (já publicamente disponibilizada) poderá ser coletada e reutilizada.

The background of the entire page is a vibrant purple and blue gradient. Overlaid on this are several images of diverse professionals. In the upper right, a man and a woman look upwards with expressions of hope or contemplation. In the center, a woman with curly hair smiles warmly at the camera. To her left, a man looks off to the side. In the lower right, another man is seen holding a tablet. The bottom of the image features a glowing, futuristic circular interface with concentric rings and a bright light in the center, suggesting a digital or technological theme.

**Contribuições Softex –
consulta pública
Guia de Transparência
e Proteção de
Dados Pessoais**



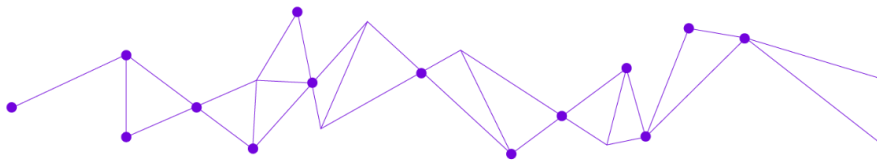
Contribuições à Guia de Transparência e Proteção de Dados Pessoais

Apresentação

A consulta pública sobre o Guia de Transparência e Proteção de Dados Pessoais, elaborado pela Controladoria-Geral da União (CGU) e pela Agência Nacional de Proteção de Dados (ANPD), representa uma oportunidade relevante para o aprimoramento das orientações destinadas a conciliar o direito de acesso à informação com a proteção da privacidade e dos dados pessoais. O documento constitui importante instrumento para fortalecer a transparência, a segurança jurídica e a atuação responsável da Administração Pública no tratamento e na divulgação de informações.

A Softex apresenta contribuições técnicas ao Guia com base em sua experiência na execução de políticas públicas, na produção de estudos e indicadores e na articulação de iniciativas de inovação, transformação digital, formação de talentos e desenvolvimento tecnológico. As propostas buscam favorecer o acesso responsável a dados para pesquisa e avaliação de políticas públicas, fortalecer a transparência e a segurança desde a concepção de sistemas e processos e estabelecer parâmetros mais claros para o uso de tecnologias, a contratação de soluções e a execução de iniciativas em parceria com terceiros.

Assim, a análise a seguir visa propor aprimoramentos técnicos ao texto-base, tornando suas orientações mais objetivas, previsíveis e aplicáveis aos diferentes contextos da Administração Pública.



Cap. 4 – Garantindo a transparência pública com proteção dos dados pessoais

Sugestão de contribuição estratégica 01

Contribuição: incorporação dos princípios do *Five Safes* no acesso controlado a dados restritos.

Dispositivo do guia

Páginas 19 a 21 do item 4.1

Trecho original

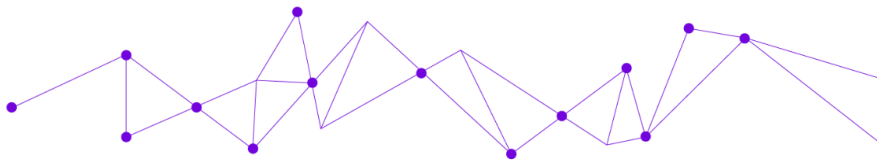
Não se aplica.

Proposição

Recomenda-se a inclusão, no item 4.1 do Guia, de diretrizes baseadas no referencial internacional *Five Safes* (Cinco Seguranças) para orientar a avaliação e a governança do acesso controlado a dados administrativos sob custódia do poder público que não sejam passíveis de divulgação aberta, especialmente em razão da presença de dados pessoais, da confidencialidade ou da elevada granularidade das informações. O modelo orienta que o risco não seja avaliado apenas pela sensibilidade do dado, mas por cinco dimensões conjuntas:

- Projetos Seguros: o uso da informação tem finalidade legítima e interesse público?
- Pessoas Seguras: os pesquisadores/agentes são confiáveis e assinaram termos de responsabilidade?
- Ambientes Seguros: o acesso se dará em salas seguras (físicas ou virtuais) que impedem a extração não autorizada?
- Dados Seguros: os dados receberam tratamento de desidentificação/pseudonimização adequado àquele contexto?
- Resultados Seguros: a publicação final da pesquisa garante que nenhum indivíduo possa ser reidentificado?

O modelo pode ser aplicado em conjunto com a legislação vigente, com o procedimento de análise do interesse público e com as demais medidas técnicas, administrativas e jurídicas de proteção.



Defesa técnica

A avaliação limitada às alternativas de “divulgar” ou “restringir” não contempla adequadamente a complexidade do uso de dados administrativos pelo Estado e por pesquisadores. A incorporação do referencial Five Safes permite que o risco seja analisado de forma multidimensional, considerando conjuntamente o projeto, as pessoas autorizadas, o ambiente de acesso, as características dos dados e os resultados produzidos (DESAI; RITCHIE; WELPTON, 2016). Essa abordagem evita que a proteção dependa exclusivamente da anonimização da base. A aplicação excessiva de técnicas de desidentificação pode reduzir a granularidade e comprometer a utilidade analítica dos dados, especialmente em estudos territoriais, longitudinais ou voltados a grupos populacionais específicos. O NIST recomenda que a desidentificação seja integrada a medidas técnicas e de governança compatíveis com o contexto de uso e com os riscos de reidentificação (GARFINKEL, 2023). Assim, quando dados detalhados não puderem ser divulgados abertamente, seu uso poderá ser viabilizado por meio de ambientes físicos ou virtuais controlados, acesso restrito a pessoas autorizadas, registro das operações e revisão dos resultados antes de sua divulgação. A combinação dessas salvaguardas permite preservar a utilidade dos dados para a produção científica e a avaliação de políticas públicas, sem afastar a proteção da privacidade e a responsabilidade do órgão custodiante.

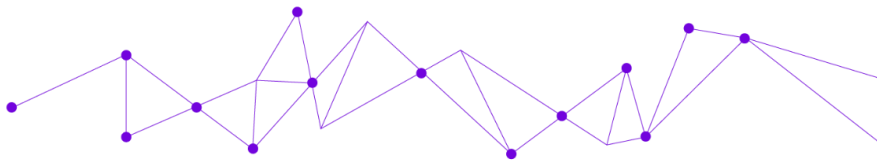
Referências

DESAI, Tanvi; RITCHIE, Felix; WELPTON, Richard. *Five Safes: designing data access for research*. Bristol: University of the West of England, 2016. (*Economics Working Paper Series*, n. 1601). Disponível em: <https://www2.uwe.ac.uk/faculties/BBS/Documents/1601.pdf>

GARFINKEL, Simson L.; NEAR, Joseph; DAJANI, Aref; SINGER, Phyllis; GUTTMAN, Barbara. *De-identifying government datasets: techniques and governance*. Gaithersburg, MD: *National Institute of Standards and Technology*, 2023. (NIST Special Publication 800-188). Disponível em: <https://doi.org/10.6028/NIST.SP.800-188>.

Sugestão de contribuição estratégica 02

Contribuição: inclusão de orientações sobre o uso responsável de inteligência artificial para ampliar a capacidade de tratamento de documentos e pedidos de acesso à



informação, preservando a supervisão humana, a rastreabilidade e a responsabilidade institucional.

Dispositivo do guia

Páginas 19 a 31, especialmente os itens 4.1 e 4.2, referentes ao roteiro de tomada de decisão, ao Teste de Interesse Público e ao registro da decisão final.

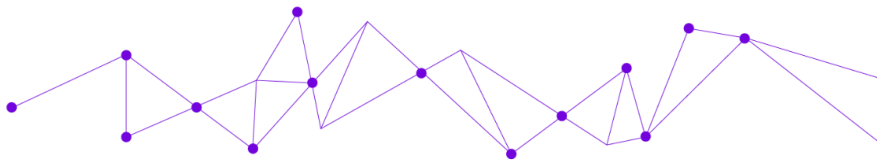
Trecho original

Não se aplica.

Proposição

Recomenda-se que o Guia inclua orientação específica sobre a utilização de sistemas de inteligência artificial (IA) ou de outras ferramentas automatizadas na identificação, triagem, classificação, anonimização, pseudonimização, tarjamento e recomendação de divulgação ou restrição de informações. Esses sistemas devem atuar como instrumentos de apoio à decisão administrativa, sem substituir a análise humana responsável, especialmente quando seus resultados puderem restringir o acesso a informações públicas ou expor dados pessoais. Sua utilização deverá ser precedida da definição e documentação da finalidade, do contexto de uso, das categorias de documentos e dados processados, dos riscos envolvidos e das responsabilidades dos agentes participantes. Os órgãos deverão assegurar, de forma proporcional ao risco:

- supervisão por pessoas com competência, treinamento, autoridade e condições efetivas para revisar, corrigir, desconsiderar ou interromper a utilização do sistema;
- registro da versão do sistema, das configurações utilizadas, das operações realizadas e das intervenções humanas;
- testes prévios e periódicos de precisão, incluindo a avaliação de falsos positivos e falsos negativos em amostras representativas dos documentos processados;
- monitoramento de desempenho e nova validação após atualizações relevantes do sistema;
- mecanismos de revisão das decisões e de comunicação e tratamento de falhas ou incidentes;
- proteção dos documentos processados, com controles de acesso, segurança, retenção e eliminação dos dados;



- regras contratuais que impeçam fornecedores de reutilizar documentos ou dados para treinamento ou outras finalidades não autorizadas.

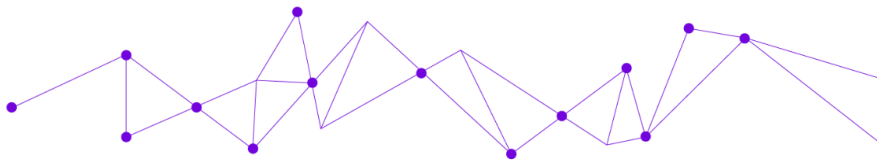
Quando o sistema de IA participar da análise de um pedido de acesso à informação, essa utilização deverá ser registrada no processo, com indicação de sua finalidade, do resultado produzido e da forma como esse resultado foi considerado pelo agente público. A decisão final e sua fundamentação permanecerão sob responsabilidade do órgão ou da autoridade competente. Quando uma decisão que afete os interesses do titular for tomada unicamente com base em tratamento automatizado de dados pessoais, deverá ser assegurado o direito de solicitar sua revisão, nos termos do art. 20 da LGPD, bem como o acesso, mediante solicitação, a informações claras e adequadas sobre os critérios e procedimentos utilizados, resguardados os segredos comercial e industrial. Como salvaguarda adicional, recomenda-se que o Guia oriente a realização da revisão por agente público com competência e autoridade para modificar a decisão. A LGPD assegura o direito de solicitar revisão, mas sua redação vigente não exige expressamente que ela seja conduzida por pessoa natural; por isso, a revisão humana deve ser apresentada como recomendação adicional do Guia.

Defesa técnica

O Guia da CGU/ANPD exige que as decisões administrativas sobre a divulgação ou restrição de informações pessoais sejam motivadas de forma clara e registradas. Contudo, à medida que a Administração Pública passa a adotar ferramentas tecnológicas para gerenciar grandes volumes de documentos e pedidos de acesso, torna-se necessário estabelecer parâmetros específicos para as situações em que uma ou mais etapas dessa análise sejam apoiadas ou executadas por sistemas automatizados.

Nesse contexto, erros sistêmicos podem afetar os dois direitos que o Guia procura compatibilizar. Falsos positivos podem levar ao tarjamento ou à restrição indevida de informações públicas, comprometendo a transparência e o direito de acesso; falsos negativos podem deixar de identificar dados pessoais protegidos, ocasionando sua divulgação indevida e possíveis danos aos titulares. Por essa razão, a avaliação do sistema não deve se limitar à taxa geral de acerto, devendo considerar separadamente os tipos de erro, seus impactos e o contexto de utilização.

Para endereçar esses desafios, o Regulamento Europeu de Inteligência Artificial (AI Act) oferece um referencial robusto. Para os sistemas classificados como de risco elevado, a norma estabelece requisitos de manutenção de registros, transparência sobre



capacidades e limitações, supervisão humana, exatidão, robustez e cibersegurança. Os responsáveis pela supervisão devem ter condições efetivas de interpretar os resultados, reconhecer limitações e anomalias, desconsiderar a saída do sistema ou interromper sua utilização (EUROPEAN UNION, 2024). Embora as ferramentas de triagem, classificação ou tarjamento mencionadas nesta contribuição não sejam automaticamente classificadas como sistemas de risco elevado pelo AI Act, os requisitos estabelecidos nos arts. 12 a 15 constituem referência técnica útil para sua adoção responsável pela Administração Pública, especialmente quando seu funcionamento puder afetar a transparência, a privacidade ou outros direitos fundamentais.

A supervisão humana, nesse contexto, não deve representar mera validação formal. O agente público precisa conhecer a finalidade e as limitações do sistema, ter acesso às informações necessárias para avaliar seu resultado e possuir competência e autoridade para alterá-lo. A decisão administrativa não pode ser atribuída de maneira opaca ao fornecedor ou ao sistema tecnológico, permanecendo o órgão responsável pela fundamentação, pela possibilidade de revisão e pelos efeitos produzidos.

Referências

EUROPEAN UNION. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence*. Official Journal of the European Union, L, 12 jul. 2024. Disponível em: <https://eur-lex.europa.eu/eli/reg/2024/1689>.

Sugestão de contribuição estratégica 03

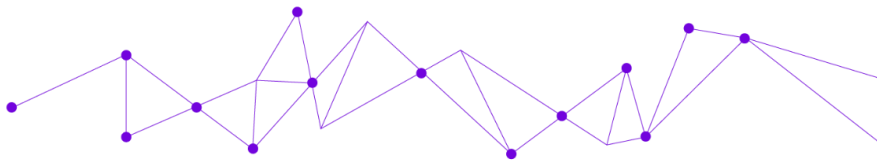
Contribuição: padrões técnicos de interoperabilidade e dados abertos como base para a transparência por desenho.

Dispositivo do Guia

Páginas 29-31, item 4.3 “Transparência por desenho”.

Trecho original

“A transparência por desenho consiste na incorporação, desde a fase de concepção de políticas públicas, sistemas de informação, bases de dados, processos administrativos e rotinas



institucionais, de critérios voltados à futura divulgação de informações públicas [...] Os sistemas eletrônicos devem permitir consultas ou extração de dados incorporando mecanismos técnicos de proteção, como mascaramento automático ou anonimização [...]"

Proposição

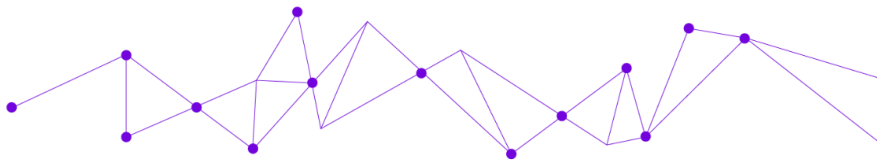
Recomenda-se que o item 4.3 faça remissão expressa à Política de Dados Abertos do Poder Executivo Federal (Decreto nº 8.777/2016) e à Infraestrutura Nacional de Dados Abertos (INDA), coordenada pela própria CGU, como instrumento operacional para viabilizar, na prática, a “transparência por desenho” já descrita conceitualmente pelo Guia.

Sugere-se incluir orientação de que, sempre que tecnicamente possível, os conjuntos de dados resultantes da aplicação do teste de interesse público (item 4.2) e das técnicas de minimização (item 4.3) sejam disponibilizados:

- Em formato de dados abertos (estruturado, processável por máquina, sob licença aberta), conforme padrões já definidos pela INDA e pela ePING (Padrões de Interoperabilidade de Governo Eletrônico);
- Por meio de interfaces de programação de aplicações (APIs) documentadas, e não apenas por arquivos estáticos, de modo a permitir atualização contínua e reduzir o retrabalho manual de anonimização a cada novo pedido de acesso; e
- Com metadados padronizados que indiquem, para cada campo, se o dado foi objeto de mascaramento, agregação ou anonimização, e com qual critério, dando rastreabilidade ao próprio processo decisório do capítulo 4.

Defesa técnica

Guia já orienta, de forma correta, que os sistemas sejam desenhados para permitir mascaramento automático, extração de dados agregados e geração de versões públicas. Entretanto, essas orientações permanecem em nível conceitual, sem remissão aos instrumentos normativos que já existem no âmbito federal especificamente para esse fim. Entre eles estão a Política de Dados Abertos, instituída pelo Decreto nº 8.777/2016 (BRASIL, 2016), a atribuição de sua gestão à Controladoria-Geral da União, estabelecida pelo Decreto nº 9.903/2019 (BRASIL, 2019), e a Infraestrutura Nacional de Dados Abertos (INDA). Essa lacuna é relevante porque a ausência de referência a um padrão técnico comum tende a gerar soluções heterogêneas entre os órgãos, com cada um definindo isoladamente seus próprios formatos de anonimização e disponibilização. A Política de



Dados Abertos prevê entre seus objetivos o intercâmbio, a reutilização, o acesso por pesquisadores e o desenvolvimento de novas tecnologias e negócios (BRASIL, 2016). A falta de padronização pode, portanto, dificultar o reuso e o cruzamento dos dados por pesquisadores, empresas de tecnologia e pela própria sociedade civil. A INDA reúne padrões, tecnologias, procedimentos e mecanismos de controle necessários à disseminação e ao compartilhamento de dados públicos em formato aberto (CONTROLADORIA-GERAL DA UNIÃO, 2023). Vincular o item 4.3 a esses padrões possui baixo custo de implementação, pois não cria nova obrigação, mas articula normas e instrumentos já vigentes. Essa integração também aumenta a viabilidade prática das contribuições apresentadas pela Softex sobre modalidades graduais de acesso e ambientes seguros de pesquisa, que dependem de infraestrutura técnica, padronização e interoperabilidade para funcionar em escala.

Referências

BRASIL. Decreto nº 8.777, de 11 de maio de 2016. Institui a Política de Dados Abertos do Poder Executivo federal. Diário Oficial da União: Brasília, DF, 12 maio de 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm.

BRASIL. Decreto nº 9.903, de 8 de julho de 2019. Altera o Decreto nº 8.777, de 11 de maio de 2016, para dispor sobre a gestão e os direitos de uso de dados abertos. Diário Oficial da União: Brasília, DF, 9 jul. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9903.htm.

CONTROLADORIA-GERAL DA UNIÃO. Plano de Ação da Infraestrutura Nacional de Dados Abertos 2023–2025. Brasília, DF: CGU, 2023. Disponível em: <https://basedeconhecimento.cgu.gov.br/handle/1/17536>.

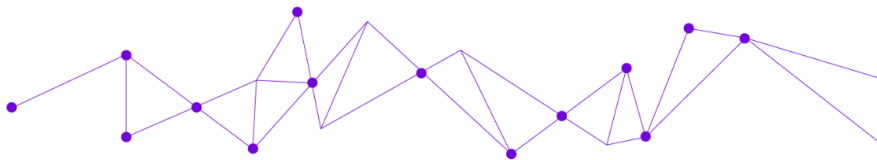
Sugestão de contribuição estratégica 04

Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como etapa recomendada do roteiro decisório para divulgações de alto risco.

Dispositivo do Guia

Páginas 21 a 28, item 4.2 “Identificando o interesse público e geral preponderante” (Teste de Interesse Público, etapas 1 a 6).





Trecho original

“Com base na análise conjunta desses elementos, o agente público deve formar um juízo sobre o risco final de dano, resultante da combinação entre o tipo de dano identificado, a probabilidade de sua ocorrência e o impacto que pode causar. [...] Trata-se de uma análise qualitativa, realizada caso a caso.”

Proposição

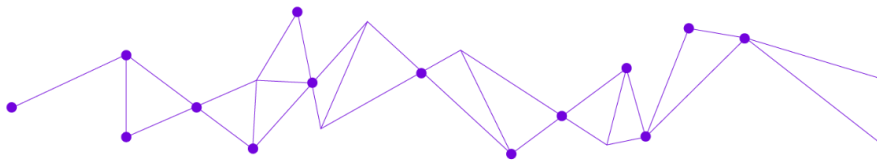
Recomenda-se que o Guia oriente a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) sempre que o Teste de Interesse Público (etapas 1 a 6, item 4.2) envolver:

- Dados pessoais sensíveis em grande volume ou de forma sistemática;
- Dados de titulares em situação de vulnerabilidade (crianças e adolescentes, vítimas de violência, beneficiários de programas de proteção); e
- Divulgação em transparência ativa (isto é, de alcance amplo e contínuo, e não apenas resposta a um pedido individual de acesso).

O RIPD, nesses casos, formalizaria e documentaria as etapas 1 a 5 já previstas no roteiro do item 4.2 (identificação do dado, mapeamento de benefícios, avaliação de risco, ponderação e minimização), funcionando como o próprio registro estruturado exigido na etapa 6, sem criar procedimento paralelo. Sugere-se, ainda, que o Guia esclareça que a exigência é proporcional ao risco (não se aplica a divulgações de baixo risco, como dados de agentes públicos em exercício de função) e que o modelo de relatório possa ser padronizado pela ANPD ou pela CGU, para reduzir custo de conformidade aos órgãos.

Defesa técnica

O item 4.2 já estabelece um roteiro de seis etapas para avaliação de risco e ponderação entre interesse público e privacidade, mas não o vincula expressamente ao instrumento de RIPD previsto no art. 38 da LGPD, que autoriza a ANPD a determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de tratamento. Vincular o roteiro do Guia a esse instrumento formal tem três vantagens práticas: (i) dá ao registro da decisão final (etapa 6) um formato já reconhecido e testado na prática regulatória de proteção de dados, facilitando eventual fiscalização pela ANPD; (ii) evita que cada órgão desenvolva um modelo próprio de documentação, replicando o problema de heterogeneidade já identificado em relação aos formatos de dados abertos; (iii) cria critério objetivo de



proporcionalidade, o RIPD seria exigido apenas nos casos de maior risco, evitando sobrecarga em decisões rotineiras de baixo impacto, como a divulgação do nome e cargo de um agente público.

A proposta não cria uma nova obrigação legal, apenas recomenda que os órgãos formalizem, para os casos de maior risco, uma prática já implícita no próprio roteiro do Guia, utilizando o instrumento que a LGPD já prevê para essa finalidade.

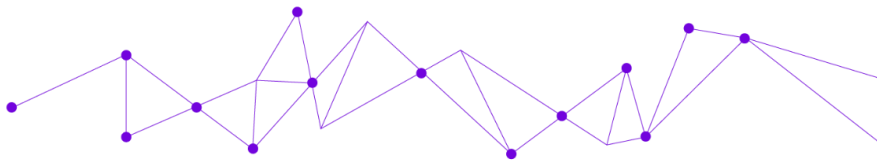
Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Art. 38. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm



The background of the entire page is a vibrant blue and purple gradient. Overlaid on this are several images of diverse professionals. In the center, a woman with dark curly hair smiles while holding a tablet displaying data charts. To her left, a man looks up thoughtfully. To her right, another man looks forward. In the upper right, a man looks upwards with a slight smile. The background is also decorated with abstract digital elements like glowing lines, circles, and a large, glowing circular pattern at the bottom center, resembling a stylized 'S' or a data visualization.

**Contribuições Softex –
consulta pública
Guia de Transparência
e Proteção de
Dados Pessoais**



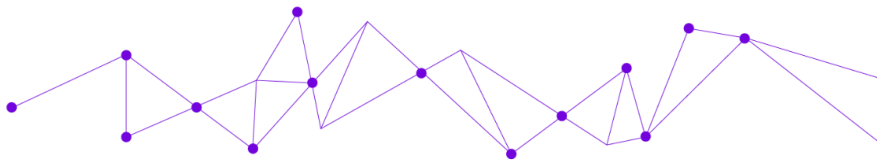
Contribuições à Guia de Transparência e Proteção de Dados Pessoais

Apresentação

A consulta pública sobre o Guia de Transparência e Proteção de Dados Pessoais, elaborado pela Controladoria-Geral da União (CGU) e pela Agência Nacional de Proteção de Dados (ANPD), representa uma oportunidade relevante para o aprimoramento das orientações destinadas a conciliar o direito de acesso à informação com a proteção da privacidade e dos dados pessoais. O documento constitui importante instrumento para fortalecer a transparência, a segurança jurídica e a atuação responsável da Administração Pública no tratamento e na divulgação de informações.

A Softex apresenta contribuições técnicas ao Guia com base em sua experiência na execução de políticas públicas, na produção de estudos e indicadores e na articulação de iniciativas de inovação, transformação digital, formação de talentos e desenvolvimento tecnológico. As propostas buscam favorecer o acesso responsável a dados para pesquisa e avaliação de políticas públicas, fortalecer a transparência e a segurança desde a concepção de sistemas e processos e estabelecer parâmetros mais claros para o uso de tecnologias, a contratação de soluções e a execução de iniciativas em parceria com terceiros.

Assim, a análise a seguir visa propor aprimoramentos técnicos ao texto-base, tornando suas orientações mais objetivas, previsíveis e aplicáveis aos diferentes contextos da Administração Pública.



Cap. 5 – Entendimentos sobre a publicidade de dados pessoais

Sugestão de contribuição estratégica 01

Contribuição: transparência e proteção de dados pessoais em programas de fomento à inovação (editais de fomento, *hackathons*, *sandboxes* regulatórios e Contratos Públicos para Solução Inovadora).

Dispositivo do Guia

Sugere-se nova seção no capítulo 5 (“Entendimentos sobre a publicidade de dados pessoais”), inserida após “Dados pessoais em processos licitatórios e contratos administrativos” (páginas 36-38).

Trecho original

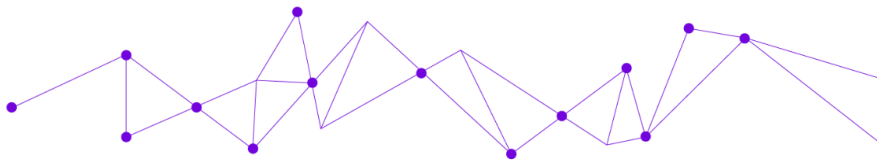
“Os processos licitatórios e os contratos administrativos são, em regra, públicos. A ampla divulgação das informações a eles relacionadas é essencial para combater a corrupção, coibir fraudes e desvios de recursos públicos, garantir a isonomia e justa concorrência entre os licitantes [...]”

Proposição

Recomenda-se que o Guia reconheça expressamente que os instrumentos de fomento à inovação, como editais de subvenção econômica, *hackathons* e maratonas de inovação, *sandboxes* regulatórios (art. 12 e seguintes da Lei Complementar nº 182/2021, Marco Legal das *Startups*) e Contratos Públicos para Solução Inovadora (CPSI), envolvem titulares de dados pessoais que não se enquadram integralmente nas categorias já tratadas pelo Guia (agente público, fornecedor tradicional ou beneficiário de programa social).

Sugere-se orientação específica prevendo que:

- Dados de proponentes, equipes técnicas, sócios de startups e participantes de *hackathons* e *sandboxes* regulatórios sejam tratados com o mesmo regime aplicável a fornecedores (nome, razão social, CNPJ, representante legal e CPF descaracterizado passíveis de divulgação; dados bancários, endereço pessoal e informações técnicas de propriedade intelectual protegidos, quando aplicável o sigilo industrial previsto no art. 22 da LAI);



- Durante a fase experimental do *sandbox* regulatório, seja admitida restrição temporária de acesso a dados operacionais e de desempenho da solução testada, de forma análoga ao tratamento dado pelo Guia aos documentos preparatórios (art. 7º, §3º, da LAI), preservando a competitividade e o sigilo empresarial legítimo durante o período de teste; e
- Finalizado o período experimental ou concluído o contrato de solução inovadora, os resultados agregados de desempenho e os critérios de seleção dos projetos sejam objeto de transparência ativa, permitindo o controle social sobre o uso de recursos públicos destinados a fomento à inovação.

Defesa técnica

O capítulo 5 do Guia trata detalhadamente de licitações e contratos administrativos tradicionais, mas os instrumentos de fomento à inovação têm natureza jurídica distinta: envolvem processos competitivos não licitatórios (editais de subvenção, hackathons), regimes de afastamento temporário de normas setoriais (*sandbox regulatório*) e contratação mediante procedimento licitatório especial e simplificado, com vigência de até 24 meses (CPSI, arts. 12 a 14 da Lei Complementar nº 182/2021). Essa diversidade de formatos gera dúvidas recorrentes para os órgãos que operam programas de inovação, como a própria Softex, sobre quais dados de proponentes e equipes podem ser divulgados em cada fase, especialmente quando a solução testada envolve segredo industrial ou dados de desempenho ainda não validados.

A ausência de orientação específica tende a gerar dois riscos opostos: exposição indevida de informações sensíveis de competitividade de startups em fase de teste, ou, no sentido inverso, sigilo excessivo que compromete o controle social sobre o uso de recursos públicos de fomento, problema já identificado pelo próprio Guia em relação a outros processos administrativos. A proposta busca aplicar, por analogia, os mesmos critérios de ponderação já adotados pelo Guia para documentos preparatórios e para sigilo industrial, adaptando-os à realidade dos programas de inovação.

Referências

BRASIL. Lei Complementar nº 182, de 1º de junho de 2021. Institui o marco legal das startups e do empreendedorismo inovador. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp182.htm.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Lei da Propriedade Industrial. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9279.htm.



OFÍCIO Nº ED-0023/2026

São Paulo, 24 de julho de 2026.

Autoridade Nacional de Proteção de Dados (ANPD)
Controladoria-Geral da União (CGU)

Aos cuidados da Diretoria de Articulação, Supervisão e Monitoramento de Acesso à Informação da Secretaria Nacional de Transparência e Acesso à Informação - DASAI/SNAI/CGU.

Ref.: Consulta pública para contribuições ao Guia de Transparência e Proteção de Dados Pessoais

Prezados,

1 A Federação Brasileira de Bancos ("FEBRABAN") e Associação Brasileira das Empresas de Cartões de Crédito e Serviços ("ABECS"), associações civis sem fins lucrativos representativas do setor financeiro, vêm apresentar suas considerações acerca do tema em referência, essencial à aplicação da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados Pessoais (LGPD).

2 Esperamos que nossas contribuições possam auxiliar qualitativamente na definição do Guia de Transparência e Proteção de Dados Pessoais, para que sejam oferecidos parâmetros e diretrizes que contribuam para decisões mais seguras, uniformes e alinhadas à legislação.

3 Permanecemos à disposição para quaisquer esclarecimentos ou contribuições que se façam necessários.

Respeitosamente, eduarda.jorge.davidovic@febraban.org.br



D4Sign
Assinado

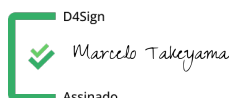
Eduarda Jorge Davidovic
Federação Brasileira de Bancos – FEBRABAN
Diretora Adjunta de Inovação e Tecnologia Bancária
marcelot@abecs.org.br

roberta.buso@febraban.org.br



D4Sign
Assinado

Roberta Gaspar Buso
Federação Brasileira de Bancos - FEBRABAN
Gerente Jurídica



D4Sign
Assinado

Marcelo Takeyama
Associação Brasileira das Empresas de Cartões de Crédito e Serviços - ABECS
Diretor Jurídico, Autorregulação e Compliance

1. Direito de acesso à informação e seus limites

a) Considerações gerais - necessidade de reforço da distinção entre Poder Público e particulares

O Guia de Transparência e Proteção de Dados Pessoais visa compatibilizar o entendimento sobre Lei de Acesso à Informação (Lei 12.527/2011) e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), de modo a equilibrar a transparência necessária para o atendimento ao interesse público com a proteção da intimidade dos titulares dos dados. Isto é, o Guia trata do desafio da divulgação de dados como dever da Administração Pública, especialmente no Item 5 (publicidade de dados pessoais e de agentes públicos).

Neste cenário, recomendamos explicitar que os deveres de transparência previstos na Lei de Acesso à Informação - LAI são aplicáveis ao Poder Público, não sendo automaticamente transferíveis a particulares contratados, como prestadores de serviços, instituições financeiras e terceiros.

Na prática, há risco de interpretação de que terceiros contratados, mediante acionamento do próprio Poder Público, estariam obrigados a realizar divulgação de dados pessoais, o que pode conflitar com a LGPD, sigilo bancário e deveres contratuais de confidencialidade.

De forma exemplificativa, no contexto de contratos administrativos que envolvam processamento de folha de pagamento ou gestão de benefícios, não devem ser solicitados ou divulgados dados bancários individuais de titulares (tais como número de conta, agência ou chaves de pagamento), por não serem necessários ao controle social e envolverem risco de fraude e uso indevido.

Assim, sugerimos explicitar que, em contratos firmados com terceiros, como por exemplo, mas não se limitando, com instituições financeiras, para folha de pagamento, não devem ser solicitados ou divulgados dados bancários individuais dos beneficiários, por não serem necessários à transparência e estarem sujeitos a confidencialidade e elevado risco de fraude.

Assim, para fins de fiscalização e controle social, mostrar-se-ia suficiente a divulgação de informações como identificação do beneficiário, vínculo com a Administração e valores pagos, não sendo justificável a ampliação do acesso a dados financeiros individualizados.

b) Comentários ao tópico “1.2. Exceções da Transparência” – subitem “sigilo legal”.

O Guia reconhece o sigilo bancário como hipótese de restrição de acesso. Neste ponto, cabe apenas reforçar que o sigilo bancário constitui limitação autônoma e prevalente à divulgação de dados, inclusive em contextos de transparência pública. No contexto de instituições financeiras, o sigilo bancário possui regime legal próprio, previsto na Lei Complementar 105/2001 e não pode ser relativizado por demandas genéricas de transparência.

b) Comentários ao tópico “1.2. Exceções da Transparência” – subitem “Dados pessoais”.

No trecho “Dados Pessoais”, constam as informações protegidas relativas a intimidade, vida privada, honra e imagem, no entanto, a LGPD protege as informações relacionadas a pessoa natural identificada ou identificável, logo, mais amplo do que os exemplos apresentados e que são da LAI. Este item é o que pode endereçar maior conflito entre as duas legislações (LGPD e LAI), recomenda-se diferenciar o alcance ou, ao menos, referenciar a tabela do item 3 do guia.

2. Direito à proteção de dados pessoais e da privacidade nos termos da Lei Geral de Proteção de Dados – LGPD

Cabe dar mais destaque ao contexto e intencionalidade da prevalência do direito ao acesso à informação no Enunciado CGU nº 4/22, que diz sobre a fundamentação dos processos de acesso à informação ser baseada na LAI, e não na LGPD, considerando que a LGPD é um diploma legal mais novo e que também versa sobre o tratamento de dados, de forma não específica.

Sugestão de inclusão ao item 2.2.: *“Instituições financeiras públicas e sociedades de economia mista que exerçam atividade bancária estão sujeitas aos deveres de transparência previstos na LAI em relação aos seus atos de gestão administrativa e demais atos administrativos. Entretanto, as operações típicas de intermediação financeira permanecem submetidas aos regimes legais específicos de confidencialidade, especialmente ao sigilo bancário previsto na Lei Complementar nº 105/2001, devendo a transparência ser compatibilizada com tais normas e com o disposto no art. 173, § 1º, II, da Constituição Federal.”*

a) Comentários ao subitem “3.3. Acesso por terceiros à informação pessoal protegida” – alínea “e - cumprimento de ordem judicial”.

Sugere-se avaliar se o texto merece esclarecimentos adicionais quanto à distinção entre ordens judiciais e outras hipóteses de compartilhamento de informações previstas em legislação específica. Embora o item destaque corretamente que ordem judicial não se confunde com solicitações formuladas por autoridades administrativas, a redação pode suscitar dúvidas quanto a requisições realizadas por órgãos que possuem competência legal própria para acesso a determinadas informações, como Banco Central do Brasil, Conselho de Controle de Atividades Financeiras (COAF), autoridades fiscais, Ministério Público no âmbito de inquérito civil e outros órgãos de supervisão e controle, observados os limites e requisitos estabelecidos em suas respectivas legislações. A questão merece aprofundamento para evitar interpretações de que toda e qualquer hipótese de compartilhamento de informações protegidas dependeria necessariamente de ordem judicial, quando determinadas situações possuem disciplina legal específica e autônoma.

3. Proteção de dados pessoais prevista na LAI

a) Comentário ao item “4.1. Roteiro para tomada de decisão”:

Revisar a sequência para que o último item (“há interesse público geral e preponderante?”) não seja uma flecha/seta, pois dá a entender que existirá um outro item. Além disso, onde constam informações de agentes públicos, recomenda-se deixar claro que devem ser em razão da sua função pública (ex. “remuneração recebida”).

b) Considerações sobre o tópico: “4.2. Identificando o interesse público e geral preponderante”.

O Guia prevê análise de base legal para tratamento de dados no setor público. Recomendamos incluir orientação expressa de que solicitações de acesso a dados a terceiros contratados devem estar acompanhados de fundamentação legal específica, não bastando invocação genérica de interesse público ou transparência, a fim de garantir segurança jurídica e evitar compartilhamentos indevidos por parte de contratados.

O Guia diferencia agentes públicos de demais titulares, indicando menor expectativa de privacidade para os primeiros.

Sugerimos inclusão expressa de orientação sobre dados de terceiros sem relação direta com a função pública de modo a evitar exposição indevida de terceiros.

c) Considerações sobre o tópico “4.3. – Transparência por desenho”.

O Guia já prevê a necessidade de divulgar apenas o mínimo necessário. Assim, sugerimos reforçar, de forma prática, quais são as recomendações aplicáveis.

O Guia deve esclarecer que eventuais obrigações de estruturação de dados para fins de transparência devem ser definidas pelo órgão público, não sendo automaticamente imputáveis aos contratados sem previsão legal ou contratual específica. Tal ação evitará transferência indevida de ônus operacional e regulatório ao particular.

4. Garantindo a transparência pública com proteção dos dados pessoais

Sem considerações.

5. Entendimentos sobre a publicidade de dados pessoais

a) Considerações gerais

No contexto de contratos administrativos, especialmente aqueles relacionados à folha de pagamento de servidores públicos ou gestão de benefícios, por exemplo, entende-se igualmente pertinente reforçar a vedação à solicitação e divulgação de dados de qualificação dos titulares que não sejam necessários à finalidade de transparência.

b) Considerações sobre o item “Dados pessoais de agentes públicos”

Observações sobre a tabela: Sempre que a regra geral for de divulgação descaracterizada (ex. número do CPF), deve constar na coluna “regra geral de divulgação” e não na coluna

de “observações”. Trata-se de mero ajuste de estrutura da tabela para padronização, para afastar o risco de interpretação divergente.

c) Considerações sobre o item “Dados pessoais sobre beneficiários de programas sociais”

O que dizem as normas?

Enunciado CGU nº 10/2023 - Informações financeiras a respeito de programas e benefícios sociais

Informações referentes a valores de benefícios pagos e a identificação de beneficiários de programas sociais, mesmo que operados por instituições financeiras, são de acesso público, em razão do disposto no art. 29, § 2º, XII, da Lei nº 14.129, de 29 de março de 2021, desde que respeitado a privacidade dos dados pessoais e dos dados sensíveis, sem prejuízo dos demais requisitos elencados, conforme a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Tais dados não são protegidos pelo sigilo fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional ou industrial, de que trata o art. 6º, I, do Decreto nº 7.724, de 16 de maio de 2012.

Neste caso, é importante deixar claro no Guia que a instituição financeira pagadora não é a destinatária adequada de pedido de LAI para divulgação da política pública; a legitimidade recai sobre o ente público responsável pela política.

Informações referentes a valores de benefícios pagos e à identificação de beneficiários de programas sociais, quando sob custódia do órgão ou entidade pública responsável pela política, são de acesso público nos termos do art. 29, §2º, XII, da Lei nº 14.129/2021, respeitados a LGPD e a proteção dos dados pessoais sensíveis. Permanecem integralmente protegidos pelo sigilo bancário os dados relativos à movimentação financeira, cartão e demais informações protegidas da relação bancária mantida entre o beneficiário e a instituição financeira pagadora, cujo acesso depende dos ritos previstos na própria Lei Complementar.

A própria LAI determina, no art. 22:

"O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público."

6. Considerações “O que dizem as normas?”

Registra-se, ainda, impropriedade formal no tratamento editorial conferido ao Enunciado CGU nº 10/2023, apresentado sob o título 'O que dizem as normas?', em equivalência com dispositivos legais e constitucionais ao longo do Guia. Enunciados da Controladoria-Geral da União constituem atos administrativos de caráter orientador, sem natureza de norma jurídica primária, não integrando o rol do art. 59 da Constituição Federal nem se qualificando como ato normativo apto a afastar sigilos legais protegidos por lei complementar, como o sigilo bancário previsto na LC nº 105/2001. Sugere-se, assim, (i) a reclassificação editorial dos Enunciados em box próprio, distinto daquele destinado às normas jurídicas; e (ii) a inclusão de ressalva expressa quanto à natureza meramente orientativa desses atos, evitando indução de agentes públicos a erro sobre a hierarquia das fontes aplicáveis.

Ofício ED-0023 - 260720 CP Guia de transparência e proteção de dados Abecs e FBB validado - vf p

Código do documento 3c89ed03-b684-479b-ba56-bb8ddc5f254f



Assinaturas



Eduarda Davidovic
eduarda.davidovic@febraban.org.br
Assinou



ROBERTA GASPAR BUSO
roberta.buso@febraban.org.br
Assinou



Marcelo Takeyama
marcelot@abecs.org.br
Assinou



Eventos do documento

24 Jul 2026, 14:36:28

Documento 3c89ed03-b684-479b-ba56-bb8ddc5f254f **criado** por PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b). Email: paula.mesquita@febraban.org.br. - DATE_ATOM: 2026-07-24T14:36:28-03:00

24 Jul 2026, 14:38:51

Assinaturas **iniciadas** por PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b). Email: paula.mesquita@febraban.org.br. - DATE_ATOM: 2026-07-24T14:38:51-03:00

24 Jul 2026, 14:40:39

ROBERTA GASPAR BUSO **Assinou** (5ddc9e9a-9c5d-493b-92ca-05a9e2f52f9c) - Email: roberta.buso@febraban.org.br - IP: 18.230.194.237 (ec2-18-230-194-237.sa-east-1.compute.amazonaws.com porta: 58104) - Documento de identificação informado: 306.633.378-79 - DATE_ATOM: 2026-07-24T14:40:39-03:00

24 Jul 2026, 14:58:33

EDUARDA DAVIDOVIC **Assinou** - Email: eduarda.davidovic@febraban.org.br - IP: 15.228.251.34 (ec2-15-228-251-34.sa-east-1.compute.amazonaws.com porta: 24660) - Documento de identificação informado: 118.211.957-36 - DATE_ATOM: 2026-07-24T14:58:33-03:00

24 Jul 2026, 16:02:27

MARCELO TAKEYAMA **Assinou** - Email: marcelot@abecs.org.br - IP: 186.204.162.161 (bacca2a1.virtua.com.br porta: 4772) - Documento de identificação informado: 255.964.638-25 - DATE_ATOM: 2026-07-24T16:02:27-03:00

Hash do documento original

(SHA256):d47fdc01f85c5a000cdb1fae957ed0cc25e2b3063d195f70d3b06fa3688f40f2

(SHA512):e742a33f981d3aa93b2ff9a8a2c077a22d2b650151a3190fb1d3e5e279d6e1f96793b21c7c3d98f12d823e2fd69a080f3ef845dfaa93d997e6f134d2fdd42272

Esse log pertence **única e exclusivamente** aos documentos de HASH acima



Esse documento está assinado e certificado pela D4Sign

Integridade certificada no padrão ICP-BRASIL

Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.

São Paulo, julho de 2026

Contribuições para consulta pública do Guia de Transparência e Proteção de Dados Pessoais

À Controladoria-Geral da União (CGU)
À Agência Nacional de Proteção de Dados (ANPD)

Assunto: Contribuições para consulta pública do Guia de Transparência e Proteção de
Dados Pessoais

Prezados/as,

A Open Knowledge (OKBR), organização da sociedade civil, atuante no campo dos direitos digitais, levando em conta tanto a perspectiva da transparência quanto da privacidade, vem apresentar suas contribuições para a consulta pública para o Guia de Transparência e Proteção de Dados Pessoais.

Nossas contribuições estão fundamentadas na necessidade de equilibrar dois direitos fundamentais: o direito de acesso à informação e à proteção de dados pessoais, considerando que a Lei de Acesso à Informação (LAI - Lei nº 12.527/2011) e a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) são complementares e devem caminhar juntas.

Além disso, ressaltamos a necessidade de aprofundar a discussão para edição e aprimoramento do guia, ampliando o diálogo com organizações da sociedade civil e de outros setores da sociedade com o objetivo de tratar questões de estrutura e conceitualizações do guia.

Seguem as contribuições:

Avenida Paulista, 37 - 4º andar - São Paulo, SP | CEP: 01311-902
Site: ok.org.br | Email: contato@ok.org.br

A) 2.3. LGPD e LAI: compatibilidade e complementaridade (p. 9)

“Nesse sentido, a presença de dados pessoais em documentos, processos ou bases de dados não implica, por si só, restrição automática de acesso. A decisão sobre a divulgação deve resultar de análise concreta e motivada, que considere a finalidade da transparência, a relevância do interesse público, o grau de exposição do titular e a possibilidade de adoção de medidas mitigadoras, como a anonimização, a pseudonimização ou a divulgação parcial da informação.”

Observação:

O guia deve indicar e referenciar quais são as metodologias de anonimização e pseudonimização mencionadas ao longo do material. Os órgãos e entidades governamentais competentes devem definir padrões e metodologias para publicar dados sem expor as pessoas. É urgente definir o desenvolvimento de métodos sobre como os órgãos devem tratar bases de dados para remover informações pessoais antes da publicação. Isso permite a publicização das informações sem identificar e expor os cidadãos titulares.

B) 3.3 Acesso por terceiros à informação pessoal protegida, item b) Previsão legal (p. 14)

“O acesso também pode ocorrer quando uma lei específica determina a divulgação do dado ou autoriza o seu fornecimento a terceiros, sem necessidade de consentimento do titular.

Nesses casos, o órgão deve identificar claramente o dispositivo legal aplicável e verificar se a hipótese legal se ajusta ao pedido recebido.”

Observação:

O guia deveria listar todas as legislações específicas que determinam a divulgação de informações pessoais sem a necessidade de consentimento.

C) 3.3 Acesso por terceiros à informação pessoal protegida, item d) Estatísticas e Pesquisas, quadro: Orientações para fornecer informações pessoais para pesquisa compatibilizando as disposições da LAI e da LGPD (p. 15)

Orientações para fornecer informações pessoais para pesquisa compatibilizando as disposições da LAI e da LGPD:

- As informações pessoais podem ser fornecidas para pesquisa, **preferencialmente** de forma anonimizada ou pseudonimizada.
- A demanda deve ser apresentada por representante de órgão de pesquisa. Segundo a LGPD, trata-se de órgão ou entidade da administração pública direta ou indireta, ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (definição trazida pelo art. 5º, inciso XVIII da LGPD).
- A demanda deve apresentar os dados pessoais requeridos, além de informações mínimas necessárias à avaliação do interesse público ou geral da pesquisa ou estudo. Não cabe avaliação da metodologia, mérito técnico ou científico da pesquisa.
- As pessoas que acessarão os dados pessoais devem assinar Termo de Responsabilidade, que indique que as informações serão de uso restrito à pesquisa, sob pena de responsabilização.
- Para pesquisas em saúde pública, os dados fornecidos serão tratados exclusivamente dentro do órgão, mantidos em ambiente controlado e seguro, que incluam, sempre que possível, a sua anonimização ou pseudonimização, e que considerem os devidos padrões éticos relacionados a estudos e pesquisas. Nesses casos, a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa poderá revelar dados pessoais.
- Quando as informações forem fornecidas de forma anonimizada ou pseudonimizada, sem possibilidade de reidentificação, a assinatura de termo de responsabilidade é dispensada.

Fonte: Brasil, 2026.

Observação:

O guia orientativo restringe quem pode apresentar demanda de informações pessoais para pesquisa a representante de órgão de pesquisa. No entanto, a Lei de Acesso à Informação (LAI, Lei n. 12.527/2011) não apresenta essa limitação. A medida exclui pesquisadores, jornalistas e organizações independentes além da cidadania em geral.

O guia orientativo requer a apresentação de justificativa da solicitação que é dispensada pela Lei de Acesso à Informação (LAI, Lei n. 12.527/2011).

O guia orientativo requer a assinatura de Termo de Responsabilidade que indique que as informações serão de uso restrito à pesquisa, sob pena de responsabilização. Deveria existir requisito apenas no caso da disponibilização de acesso à íntegra de dados pessoais considerados restritos (não anonimizados) sem a disponibilização para publicidade geral. Nesse caso de possibilidade de identificação de titulares dos dados, e não se tratando de dados essenciais para exercício do controle social sobre recursos públicos, é coerente haver orientações e acompanhamento da ANPD a respeito da governança e tratamento das informações

peçoais, o órgão de pesquisa passa a figurar como responsável pela segurança e tratamento dos dados e deveria elaborar Relatório de Impacto de Tratamento de Dados Pessoais que é um instrumento importante para identificação e mitigação de riscos, instrumento previsto pela Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709/2018).

D) 3.3 Acesso por terceiros à informação pessoal protegida, item f) Defesa dos Direitos Humanos (p. 14)

“A LAI autoriza a divulgação de informações pessoais, sem o consentimento do titular, para defesa de direitos humanos. Trata-se de hipótese aplicada apenas quando a manutenção da restrição representar risco à proteção da pessoa ou grupo envolvido.

Orientações gerais para fornecer informações pessoais para defesa de direitos humanos:

- Avaliar se a informação é necessária para defesa do direito humano ameaçado ou violado, considerando a necessidade indicada na demanda.
- Verificar se há indícios de que a restrição de acesso à informação pode prejudicar a proteção do direito humano.
- Considerar que a entrega da informação deve ser feita ao solicitante que possa atuar na defesa pretendida.
- Limitar a divulgação ao estritamente necessário.
- Exigir assinatura de Termo de Responsabilidade para restringir o uso à finalidade específica.”

Observação:

O guia pressupõe a apresentação de justificativa da solicitação que é dispensada pela Lei de Acesso à Informação (LAI, Lei n. 12.527/2011).

O guia orientativo requer a assinatura de Termo de Responsabilidade para restringir o uso à finalidade específica. Deveria existir requisito apenas no caso da disponibilização de acesso à íntegra de dados pessoais considerados restritos (não anonimizados) sem a disponibilização para publicidade geral. Nesse caso, de possibilidade de identificação de titulares dos dados, e não se tratando de dados essenciais para exercício do controle social sobre recursos públicos, é coerente haver orientações e acompanhamento da ANPD a respeito da governança e tratamento das

informações pessoais, o órgão de pesquisa passa a figurar como responsável pela segurança e tratamento dos dados e deveria elaborar Relatório de Impacto de Tratamento de Dados Pessoais que é um instrumento importante para identificação e mitigação de riscos, instrumento previsto pela Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709/2018).

E) 4. Garantindo a transparência pública com proteção dos dados pessoais (p.19)

Observação:

Quais são as referências metodológicas adotadas para o passo a passo do roteiro da tomada de decisão referente à divulgação ou restrição de acesso a informações pessoais e para o Teste de Interesse Público sobre a tomada de decisão sobre se há interesse público e geral preponderante para disponibilização do acesso à informação? O guia deve explicitar os materiais metodológicos de referência.

Além disso, o material deve referenciar o arcabouço de decisões sobre o acesso às informações que já foram adotadas pela Corte do Supremo Tribunal Federal. O guia também tem o papel de reunir entendimentos e decisões já consolidadas no campo.

F) 4.2. Identificando o interesse público e geral preponderante (p. 22)

“A lista acima é exemplificativa. Em cada caso concreto, outras situações podem caracterizar benefício público relevante. O importante nessa etapa é mapear quais benefícios em prol da coletividade são consequência clara e direta da abertura do dado analisado. Vale lembrar, ainda, que interesse coletivo é diferente de curiosidade geral.”

Observação:

Levantamos o questionamento sobre o que está sendo chamado de “curiosidade geral”, se a Lei de Acesso à Informação (LAI, Lei n. 12.527/2011) não requer a apresentação de justificativa da solicitação de informações.

Conclusão

A Open Knowledge Brasil reforça que a transparência deve ser a regra geral. O sigilo deve ser a exceção. A proteção de dados é um direito fundamental, mas não pode servir para apagar o direito ao acesso à informação. Também reforça a necessidade de aprofundamento e ampliação do diálogo a respeito do conteúdo do

Guia de Transparência e Proteção de Dados Pessoais com organizações da sociedade civil e de outros setores com o objetivo de tratar questões de estrutura e conceitualizações do guia.

Aguardamos retorno sobre o tratamento conferido a cada contribuição registrada na consulta pública visando dar transparência, integridade e efetividade ao processo de participação social.

A organização segue à disposição para dialogar e colaborar com a elaboração de uma nova versão do Guia de Transparência e Proteção de Dados Pessoais.

Atenciosamente,

Documento assinado digitalmente
 EDILAINÉ DOS SANTOS E SOUZA
Data: 24/07/2026 19:12:49-0300
Verifique em <https://validar.it.gov.br>

Edilaine Santos
Analista de Advocacy e Pesquisa

OPEN KNOWLEDGE BRASIL
CNPJ 19.131.243/0001-97

Referências

BRASIL. Controladoria-Geral da União; Agência Nacional de Proteção de Dados. **Guia de Transparência e Proteção de Dados Pessoais. Versão para consulta pública.**

Brasília: CGU/ANPD, maio 2026. Disponível em:

https://brasilparticipativo.presidencia.gov.br/rails/active_storage/blobs/redirect/eyJfc mFpbHMiOmsibWVzc2FnZSI6IkJBaHBBOUxaQVE9PSlslmV4cCI6bnVsbCwicHVyljoiYmxv Yl9pZCJ9fQ==--32d3944aee033b988ae2128c91e9ffff079f01a9/GuiaCGU-ANPD-vConsultaPublica.pdf. Acesso em: julho 2026

BRASIL. **Lei n.º 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. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: julho 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: julho 2026.

CONTRIBUIÇÃO À CONSULTA PÚBLICA

Minuta do “Guia de Transparência e Proteção de Dados Pessoais”

Controladoria-Geral da União (CGU) e Agência Nacional de Proteção de Dados (ANPD),
versão de maio de 2026

*Análise técnica dos riscos de restrição indevida ao direito fundamental de acesso à
informação e propostas de redação alternativa*

Entidades Signatárias Listadas ao Final deste Documento

Julho de 2026

Sumário

1. Introdução.....	4
1.1 Objetivo da contribuição.....	4
2. Premissas constitucionais e convencionais necessárias à discussão.....	6
2.1 A máxima divulgação como decisão do constituinte e do legislador.....	6
2.2 Ônus argumentativo e in dubio pro accessu.....	6
2.3 Autonomia do direito à proteção de dados não significa paridade de partida.....	7
2.4 O parâmetro interamericano, ausente da minuta.....	7
2.5 A jurisprudência do Supremo Tribunal Federal, ausente da minuta.....	8
3. Problemas estruturais da minuta.....	10
3.1 A afirmação de que “não há hierarquia prévia entre os direitos”.....	10
3.2 A aplicação de normas e entendimentos já estabelecidos deve preceder a análise casuística.....	11
3.3. A confusão do ponto de partida: a categoria do dado no lugar do contexto.....	12
3.4 A salada teórica entre LAI e LGPD e a ampliação do arbítrio estatal.....	14
3.5 Responsabilidade pessoal do agente público: a assimetria entre a sanção à opacidade e a ausência de proteção à boa-fé.....	19
3.6 Imprecisões jurídicas e técnicas presentes ao longo da minuta.....	20
3.7 Consequência dos problemas estruturais: o roteiro decisório deve ser reconstruído... 23	
4. Necessidade de centralização da governança em capítulo próprio e ajustes teóricos.....	25
4.1 O Termo de Responsabilidade como condição geral de acesso.....	25
4.2. Registro da ponderação na decisão.....	26
4.3 Publicidade centralizada das decisões de negativa.....	26
4.4 Consulta pública para retirada de bases e documentos de transparência ativa.....	27
4.5. Gestão do acervo de informações pessoais.....	28
4.6 Transparência por desenho: o risco da segregação sem revisão.....	29
5. Problemas específicos da minuta.....	30
5.1 A negativa por “pedido desproporcional” fundada no custo de triagem de dados pessoais.....	30
5.2 A hipótese de pesquisa: restrição subjetiva sem base na LAI e o problema da identificação.....	30
5.3 “Interesse coletivo é diferente de curiosidade geral”: o exame de motivação pela janela.....	32
5.4 As tabelas do Capítulo 5 como regras categóricas: necessidade de cláusula geral de presunção relativa.....	33
5.5 Terminologia das tabelas: substituir “pode” por “deve” nas hipóteses de transparência obrigatória.....	34
5.6. Ausente das tabelas: casos complexos já decididos.....	34
5.7 Redução da transparência da remuneração de agentes públicos.....	35
5.8. Agentes privados que gerenciam recursos públicos, prestam serviços ou possuem relação de interesse público com a administração pública: presunção de publicidade pouco ampla.....	35
5.9. Documentos preparatórios: a “regra simples” que simplifica demais.....	36
5.10 Registros de entrada em residências oficiais: o critério deve ser a natureza do	

encontro, não o local.....	41
5.11 A hipótese de defesa dos direitos humanos: o exame de motivação pela porta dos fundos.....	42
5.12 Dado tornado manifestamente público pelo titular: hipótese ausente no texto do Guia.....	43
6. Conclusão.....	44

1. Introdução

A presente contribuição é apresentada por organizações da sociedade civil e especialistas que prezam pela defesa do direito fundamental de acesso à informação pública e ao fortalecimento do controle social, no âmbito da consulta pública relativa à minuta do “Guia de Transparência e Proteção de Dados Pessoais”, elaborada conjuntamente pela Controladoria-Geral da União (CGU) e pela Agência Nacional de Proteção de Dados (ANPD), datada de maio de 2026.

De início, registra-se o reconhecimento ao esforço institucional de harmonização entre a Lei nº 12.527/2011 (Lei de Acesso à Informação, LAI) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD). A minuta acerta em seus fundamentos declarados: afirma corretamente que a LGPD não cria hipóteses de sigilo nem autoriza negativas de acesso fundadas genericamente na proteção de dados; incorpora os Enunciados CGU nº 4/2022 e nº 12/2023, salvaguardas relevantes contra o uso abusivo da proteção de dados como escudo de opacidade; e introduz a noção de transparência por desenho, cuja adoção estruturada tem potencial para reduzir negativas reativas e casuísticas.

O problema central da minuta não está, portanto, nas premissas que enuncia, mas nas bases estruturais adotadas e na engenharia operacional que constrói. Examinados em conjunto, o roteiro decisório proposto (Capítulo 4) e os entendimentos consolidados (Capítulo 5) apresentam uma **assimetria sistemática em desfavor do acesso**. O resultado previsível, na capilaridade dos milhares de Serviços de Informação ao Cidadão (SICs) que aplicarão o documento, é o incremento de negativas indevidas, com **inversão silenciosa da regra constitucional da publicidade**.

1.1 Objetivo da contribuição

Os problemas da minuta não são pontuais nem podem ser corrigidos por alterações localizadas. Eles resultam de premissas conceituais equivocadas, metodologias falhas, ausência de coerência jurídica e técnica e uma arquitetura desorganizada.

Reconhecemos a complexidade de produzir um texto coerente a partir da participação de diferentes órgãos, áreas técnicas e equipes. No entanto, a falta de unidade conceitual e referencial identificável, de encadeamento lógico e de consistência entre as partes evidencia que não houve tempo suficiente para consolidar as diversas contribuições em um documento maduro. As dificuldades inerentes ao processo de elaboração não podem justificar a publicação de um documento ainda imaturo, que orientará decisões de milhares de agentes públicos e afetarão diretamente o exercício de um direito fundamental.

É especialmente preocupante a **ausência de referências a notas técnicas, precedentes administrativos e judiciais, estudos especializados e diagnósticos concretos sobre os problemas enfrentados na aplicação da LAI e da LGPD nos últimos anos.**

O resultado previsível, na capilaridade dos milhares de Serviços de Informação ao Cidadão (SICs) que aplicarão o documento, é o incremento de negativas indevidas, com inversão silenciosa da regra constitucional da publicidade.

Esta contribuição, portanto, não se limita a propor ajustes de redação, mas defende a reformulação integral do documento e da metodologia proposta, a partir de uma arquitetura que reafirme a publicidade como regra, sistematize os entendimentos já consolidados e estabeleça um roteiro decisório coerente apenas para os casos em que exista dúvida real sobre a divulgação.

2. Premissas constitucionais e convencionais necessárias à discussão

2.1 A máxima divulgação como decisão do constituinte e do legislador

O direito de acesso à informação pública tem assento constitucional múltiplo: art. 5º, XXXIII (direito de receber dos órgãos públicos informações de interesse particular, coletivo ou geral), art. 5º, XIV (garantia de acesso à informação), art. 37, caput (princípio da publicidade administrativa), art. 70, parágrafo único (dever de prestação de contas) e art. 216, § 2º (dever de gestão da documentação governamental e de franquear sua consulta). A Lei nº 12.527/2011 densificou essa arquitetura ao estabelecer, como diretriz primeira de todos os procedimentos que disciplina, a “observância da publicidade como preceito geral e do sigilo como exceção” (art. 3º, I).

Essa estrutura normativa não é neutra nem meramente programática. Ela veicula uma **relação de precedência estabelecida pelo próprio legislador**, em cumprimento de mandamento constitucional: **no domínio da informação produzida ou custodiada pelo Estado, a publicidade é a posição jurídica de partida, e toda restrição é uma intervenção que demanda justificação específica, legal e motivada**. Qualquer metodologia decisória que coloque acesso e restrição em posição de partida equivalente contraria essa opção legislativa, e é exatamente isso, como se demonstrará na Seção 3, que a minuta faz no ponto mais sensível do seu roteiro.

2.2 Ônus argumentativo e *in dubio pro accesso*

A consequência dogmática da estrutura regra-exceção é a alocação do ônus argumentativo. Na teoria dos princípios, relações de precedência *prima facie* estabelecidas pelo ordenamento distribuem cargas de argumentação (Robert Alexy, Teoria dos Direitos Fundamentais): quem pretende afastar a posição preferencial suporta integralmente o ônus de demonstrar, no caso concreto, as razões que a superam. Aplicado ao acesso à informação, isso significa que:

- (i) é a negativa, e não a divulgação, que precisa ser justificada;
- (ii) a insuficiência ou a dúvida na argumentação restritiva resolve-se em favor do acesso (*in dubio pro accesso*);
- (iii) a ausência de decisão motivada de restrição não pode produzir, por si só, efeitos restritivos.

A própria LAI reforça essa assimetria de deveres ao tipificar como conduta ilícita do agente público recusar-se a fornecer informação requerida, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa

(art. 32, I)¹. Não há tipificação equivalente para o excesso de transparência quanto a informações não sigilosas: **o legislador conhecia os dois riscos e escolheu sancionar prioritariamente a opacidade indevida**. Um guia orientativo dirigido a agentes públicos deve refletir essa escolha, e não diluí-la.

2.3 Autonomia do direito à proteção de dados não significa paridade de partida

A Emenda Constitucional nº 115/2022 inseriu a proteção de dados pessoais no rol dos direitos fundamentais (art. 5º, LXXIX), e o Supremo Tribunal Federal, na apreciação da ADI 6.649 e da ADPF 695 (rel. Min. Gilmar Mendes, 2023), reconheceu a autonomia desse direito e fixou parâmetros para o tratamento e o compartilhamento de dados pelo poder público. Essa evolução é positiva e não é contestada nesta contribuição; ao contrário, é celebrada.

O que se contesta é a inferência, implícita na minuta, de que a autonomia do direito implicaria **equivalência de partida** entre acesso e proteção de dados no domínio específico da informação estatal. São questões distintas. A fundamentalidade de ambos os direitos convive com a decisão constitucional e legal de que, quanto à informação pública, a publicidade é a regra. A ponderação casuística é o método adequado para resolver colisões concretas, mas ela opera dentro de uma moldura que já contém uma precedência prima facie, e não em terreno axiologicamente plano.

2.4 O parâmetro interamericano, ausente da minuta

O Brasil está vinculado ao art. 13 da Convenção Americana sobre Direitos Humanos que, conforme interpretação firmada pela Corte Interamericana de Direitos Humanos no caso *Claude Reyes e outros vs. Chile*² (sentença de 19 de setembro de 2006), **protege o direito de acesso à informação sob controle do Estado como dimensão da liberdade de pensamento e de expressão**. Daquele julgado decorrem parâmetros que integram o bloco de convencionalidade aplicável a todos os órgãos brasileiros: o princípio da máxima

¹ Nesse sentido, o relatório do GT 6 do Conselho Nacional de Proteção de Dados: “Vale mencionar que a diretriz da publicidade como regra e sigilo como exceção, prevista no art. 3º, I, da LAI impõe forte ônus argumentativo para quaisquer iniciativas que visem restringir o acesso à informação, mesmo quando esta envolve dados pessoais. O STF tem entendido que as exceções, previstas pela Constituição de 1988, à regra geral da publicidade, devem ser interpretadas de forma restritiva e conforme o princípio da publicidade (p. 73)”. Em: < <https://www.gov.br/anpd/pt-br/cnpd/relatorios-gts-2a-formacao/relatorio-final-gt6-do-cnpd.pdf/@@display-file/file> >. Acesso em: 22/07/2026.

² Corte I.D.H., Caso Claude Reyes e outros Vs. Chile. Sentença de 19 de setembro de 2006. Série C, Nº 151, § 89-91. Corte I.D.H., Caso Gomes Lund e outros (Guerrilha do Araguaia) Vs. Brasil. Sentença de 24 de novembro de 2010. Série C, Nº 219, § 229. Corte I.D.H., Caso Palamara Iribarne Vs. Chile. Sentença de 22 de novembro de 2005. Série C, Nº 135, § 85; Corte I.D.H., Caso Ricardo Canese Vs. Paraguai. Sentença de 31 de agosto de 2004. Série C, Nº 111, § 96; Corte I.D.H., Caso Herrera Ulloa Vs. Costa Rica. Sentença de 2 de julho de 2004. Série C, Nº 107, § 121 e 123.

divulgação como diretriz interpretativa geral; a exigência de que as restrições estejam previamente fixadas em lei em sentido formal, persigam finalidade legítima à luz do art. 13.2 da Convenção e sejam necessárias em uma sociedade democrática (teste tripartite); e **a atribuição ao Estado do ônus de demonstrar a compatibilidade de cada negativa com esses requisitos.**

A Lei Modelo Interamericana sobre Acesso à Informação Pública (OEA, 2010, atualizada em 2020 pela Lei Modelo 2.0)³ consolida o mesmo desenho, incluindo a regra da divulgação parcial obrigatória e a prevalência do acesso em caso de dúvida. **É uma lacuna relevante que um guia elaborado por duas autoridades federais, destinado a orientar toda a Administração, não contenha uma única referência ao marco interamericano.** A omissão não é apenas formal: o teste tripartite convencional é mais protetivo do que o roteiro proposto na minuta e deve informá-lo, sob pena de o documento orientar práticas passíveis de censura em sede de controle de convencionalidade.

2.5 A jurisprudência do Supremo Tribunal Federal, ausente da minuta

A jurisprudência do STF sobre publicidade administrativa e liberdade de informação não sustenta a paridade de partida adotada pela minuta. Ao contrário, forma repertório consistente de precedência da publicidade no domínio da coisa pública.

Na Suspensão de Segurança nº 3.902 AgR (rel. Min. Ayres Britto, Plenário, 2011), precedente que a própria minuta invoca, **a Corte assentou que a divulgação de remuneração, cargo e lotação de servidores não viola a intimidade ou a vida privada**, por se tratar de informação vinculada ao exercício de função pública, prevalecendo o princípio republicano da publicidade. O entendimento foi reiterado na SL 623 (rel. Min. Ayres Britto, 2012) e consolidado em repercussão geral no RE 652.777 (Tema 483, rel. Min. Teori Zavascki, 2015), com tese pela legitimidade da divulgação nominal dos vencimentos de servidores em sítios oficiais. No mesmo sentido, o MS 28178 (rel. Min. Roberto Barroso, 2015).

Na ADPF 130 (rel. Min. Ayres Britto, 2009) e na ADI 4.815 (rel. Min. Cármen Lúcia, 2015), o Tribunal **reconheceu posição de precedência das liberdades de informação e de expressão em face dos direitos da personalidade, exigindo justificação reforçada para restrições e rechaçando regimes de autorização prévia.** Na ADI 5.371 (rel. Min. Roberto Barroso, 2021), o Tribunal assentou que o sigilo só pode ser

³ Em: < https://www.oas.org/en/sla/dil/docs/Publicacao_Lei_Modelo_Interamericana_2_o_Acesso_Informacao_Publica.pdf >. Acesso em: 21/07/2026.

decretado em situações específicas, com forte ônus argumentativo a quem deu origem à restrição ao direito fundamental à informação, observado o princípio da proporcionalidade.

No RE 1.010.606 (Tema 786, rel. Min. Dias Toffoli, 2021), o STF declarou incompatível com a Constituição a ideia de um direito ao esquecimento apto a impedir, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos lícitamente obtidos. O precedente é diretamente relevante contra presunções temporais de restrição: **o decurso do tempo ou o desconforto do titular não criam, por si, título jurídico de ocultação de informação lícita.**

Nas ADPFs 690, 691 e 692 (rel. Min. Alexandre de Moraes, 2020), a Corte reafirmou, em contexto de emergência sanitária, **o dever estatal de transparência máxima e a excepcionalidade de qualquer restrição, que exige justificação concreta.** No mesmo sentido, a ADPF 872 (rel. Min. Carmen Lucia, 2023). E no MS 33.340 (rel. Min. Luiz Fux, Primeira Turma, 2015), assentou-se que sigilos legais, como o bancário, não são oponíveis de forma genérica às instâncias de controle da coisa pública, prevalecendo o interesse público na fiscalização de operações que envolvam recursos estatais.

Em síntese: a jurisprudência constitucional admite e pratica a ponderação, mas o faz a partir de uma **posição preferencial da publicidade** quanto a informações vinculadas à função pública e ao emprego de recursos públicos, **com ônus argumentativo integral sobre quem restringe.** É esse o desenho que o guia deve refletir.

3. Problemas estruturais da minuta

3.1 A afirmação de que “não há hierarquia prévia entre os direitos”

“É fundamental destacar que não há hierarquia prévia entre o direito de acesso à informação e a proteção de dados pessoais. A decisão deve ser sempre casuística, contextualizada e devidamente motivada [...]” (minuta, item 4.2, etapa 4).

O enunciado mistura duas proposições distintas. É correto afirmar que não há hierarquia abstrata entre normas constitucionais e que a solução de colisões exige análise contextualizada. É incorreto extrair daí que acesso e restrição partem de posição equivalente. Como demonstrado na Seção 2, **a Constituição e a LAI fixaram relação de precedência prima facie em favor da publicidade no domínio da informação estatal** (art. 3º, I, da LAI), com a consequente alocação do ônus argumentativo sobre a restrição. **Ao apagar essa precedência, a minuta neutraliza, no ponto decisivo do roteiro, a diretriz da máxima divulgação que declara acolher**, e o faz precisamente na etapa em que o agente público formará sua convicção.

O risco prático é mensurável. Em milhares de SICs, servidores sem formação constitucional aprofundada aplicarão o teste diante de casos duvidosos. **Se o guia lhes diz que os direitos partem empatados e que a decisão é qualitativa e casuística, a tendência conhecida da burocracia, avessa ao risco pessoal de divulgar, resolverá os empates pela negativa.** A doutrina brasileira adverte, há mais de uma década, contra esse uso do sopesamento: ponderação sem parâmetros e sem cargas de argumentação degenera em justificação retórica de decisões tomadas por outras razões (Marcelo Neves, Entre Hidra e Hércules, 2013). O antídoto não é abandonar a ponderação, mas ancorá-la: precedência prima facie da publicidade, ônus sobre a restrição, prevalência do acesso na dúvida.

Proposta de redação:

“Não há hierarquia abstrata entre os direitos fundamentais envolvidos, e a decisão deve ser sempre contextualizada e motivada. No domínio da informação produzida ou custodiada pelo poder público, contudo, a Constituição e a LAI estabelecem a publicidade como preceito geral e o sigilo como exceção (art. 3º, I, da Lei nº 12.527/2011). Disso decorrem três diretrizes operacionais: (i) o ônus argumentativo recai integralmente sobre a restrição, cabendo ao órgão demonstrar, de forma

concreta e motivada, as razões que a justificam; (ii) a divulgação não depende de demonstração prévia de benefício, por ser a posição jurídica de partida; e (iii) permanecendo dúvida razoável ao final da análise, prevalece o acesso (*in dubio pro accesso*).”

3.2 A aplicação de normas e entendimentos já estabelecidos deve preceder a análise casuística

O documento trata a divulgação de dados pessoais como matéria a ser sempre reconstruída pelo agente público a partir do roteiro decisório, quando parte relevante dessas hipóteses já foi resolvida, em caráter geral, por instância superior e competente para tanto.

O agente responsável pelo atendimento à LAI não detém autoridade para, no exame de um caso concreto, reabrir questão já deliberada por órgão com atribuição constitucional ou legal específica para fazê-lo, seja o Congresso Nacional ao legislar, o Supremo Tribunal Federal em sede de jurisdição constitucional, seja o Tribunal de Contas da União no exercício do controle externo ou órgãos e agências no exercício de sua competência normativa e fiscalizatória. Trata-se de aplicação, ao contexto específico da divulgação de dados pessoais, do dever de atuação administrativa orientada à segurança jurídica e à uniformidade decisória, hoje positivado no art. 30 da Lei de Introdução às Normas do Direito Brasileiro (Decreto-Lei nº 4.657/1942, com a redação dada pela Lei nº 13.655/2018). A adequada gestão de um sistema de precedentes e entendimentos aplicáveis ao tema também vai ao encontro do disposto na legislação processual civil (art. 489, c/c art. 15, Lei nº 13.105/2015).

A consulta às normas e aos entendimentos aplicáveis deve, portanto, anteceder qualquer ponderação casuística, e não apenas orientá-la: **encontrado o caso já decidido por órgão competente, dispensa-se a análise casuística, e é dessa verificação, não da identificação do dado pessoal ou da ponderação entre benefícios e riscos, que o roteiro decisório (Capítulo 4) deve partir.**

O Guia não apenas deixa de partir dessa premissa, como acentua a confusão ao usar exemplos cuja publicidade já foi definida por normas ou entendimentos consolidados. Para citar apenas um exemplo, na “Tabela de exemplos concretos de aplicação do teste de interesse público”, são incluídos casos como “nome completo e remuneração de servidor público”, “matrícula funcional de servidor” e “compromissos oficiais de ministro de Estado”, embora essas matérias já tenham sido disciplinadas por precedentes mencionados na Seção 2.5 ou por normas específicas. Ao apresentar como objeto de nova ponderação

questões já resolvidas pelas instâncias competentes, **o documento reabre indevidamente controvérsias superadas.**

É imprescindível, portanto, que um documento orientativo reúna, em seção própria, o rol de deveres de divulgação já previstos em centenas de normas, como a Lei de Governo Digital (a exemplo do art. 29, § 3º, da Lei nº 14.129/2021), Lei de Responsabilidade Fiscal (LC 101/2000), a Lei de Licitações e Contratos Administrativos (Lei nº 14.133/2021), a Lei nº 15.017/2024 (divulgação dos microdados dos censos da educação), a Lei nº 10.650/2003 (transparência ambiental), Código Tributário Nacional (art. 198 da Lei nº 5.172/1966) e a Lei de Conflito de Interesses (Lei nº 12.813/2013), bem como os entendimentos já consolidados pelas instâncias superiores sobre categorias recorrentes de informação pessoal, como o Acórdão 1841/2022 do Tribunal de Contas da União, o RE 652.777 (Tema 483) do Supremo Tribunal Federal e a Nota Técnica nº 92/2022/CGF/ANPD. A ausência desse repositório único obriga cada órgão, e cada agente dentro de cada órgão, a reconstruir isoladamente um mapeamento que já deveria estar pronto, com risco de decisões mais restritivas do que as já assentadas para o mesmo tipo de caso.

3.3. A confusão do ponto de partida: a categoria do dado no lugar do contexto

O Guia tenta definir previamente quais categorias de dados devem ser divulgadas ou protegidas, como se uma informação tivesse sempre a mesma natureza. **Nenhum dado é público ou privado de forma isolada.**

O problema não está numa tabela específica, mas num pressuposto que atravessa o documento inteiro: o Guia analisa o dado pessoal como se ele existisse somente em si mesmo, com natureza fixa e destacável, quando o que efetivamente se decide, em qualquer pedido de acesso, é o destino de um documento ou de um conjunto de dados no qual o dado pessoal é um elemento entre outros. **A mesma informação muda de natureza jurídica conforme o papel do titular, a finalidade do registro e o restante do conteúdo documental.**

Um roteiro que examina o dado isoladamente não capta essa variação, porque a pergunta que faz (“este tipo de dado é protegido?”) não é uma pergunta juridicamente relevante. A pergunta correta é: “esta informação, neste conjunto documental, neste contexto, com esta função, deve ser divulgada ou restrita?”.

Para citar apenas alguns exemplos tratados ao longo do Guia:

- (a)** Um dado de filiação partidária, por exemplo, é público quando se refere a uma pessoa candidata a um cargo eletivo. A filiação de um cidadão comum a uma associação, sindicato, igreja ou outra entidade é de foro privado do cidadão. A categoria é a mesma, mas a avaliação sobre a divulgação é diferente.
- (b)** O endereço de um imóvel privado usado como moradia deve, em regra, ser protegido. Já o endereço de um imóvel pertencente ao poder público precisa ser conhecido pela sociedade, ainda que dados que permitam identificar desnecessariamente o residente possam ser retirados. O endereço pessoal de cidadãos, em regra, é privado, mas, se, por exemplo, a organização sem fins lucrativos que recebe recursos públicos tem como sede a residência do gestor, este deve ser público. A natureza do dado “endereço”, sozinha, não determina sua publicização ou não. É o *contexto* que define o que deve ser divulgado e o que precisa ser protegido.
- (c)** Entre os exemplos de informação protegida, em tese, na tabela do item 3.1, estão “dados sobre dependentes e familiares”, “informações sobre rotina, deslocamentos ou hábitos pessoais” e “filmagens de câmeras de segurança”. Nenhuma dessas categorias admite juízo abstrato, porque todas dependem de quem é o titular, em que contexto o dado aparece e qual a finalidade do registro. Dados sobre dependentes e familiares de agentes públicos, no contexto da divulgação de pagamentos de pensão por morte e de aposentadoria, são públicos, por força da transparência ativa da folha de pagamento a que se refere o art. 7º, § 3º, VI, do Decreto nº 7.724/2012 e são fundamentais para detecção de nepotismo e conflitos de interesses. Informações sobre deslocamentos de autoridades públicas no exercício da função são, como regra, públicas, por decorrência do princípio da publicidade administrativa (art. 37, caput, CF). Filmagens de câmeras de segurança de forças policiais, por exemplo, dependem de exame caso a caso, considerado o interesse no controle da atuação estatal.

O texto tenta remediar sua fragilidade conceitual com atalhos simplistas, como o grau de “proximidade com o Estado”, que, isoladamente, torna-se também um critério equivocado. Transparência pública não depende necessariamente de uma pessoa ser próxima ou distante do governo, mas da relação entre a informação e uma ação estatal que precisa ser fiscalizada. Uma pessoa autuada pelo Estado ou devedora de impostos, por exemplo, não é “próxima” da administração pública. Ainda assim, o registro nominal da autuação e da dívida são essenciais para controlar tanto como o governo fiscaliza quanto quem está prejudicando a sociedade como um todo. O que está em questão não é a proximidade da

pessoa com o Estado. É se a informação documenta o exercício do poder público, o uso de recursos públicos ou uma decisão com impacto coletivo.

Essa falha lógico-conceitual aparece em toda a arquitetura do documento. **Ao começar pela categoria do dado, o Guia torna-se inteiramente falho.** A ordem correta deveria ser outra. Primeiro, o Guia precisaria coadunar tudo o que já conta com publicidade garantida por leis, decisões judiciais e normas específicas já existentes. Apenas depois, deveria apresentar um roteiro para os casos em que existe uma dúvida real. Por fim, os exemplos deveriam mostrar como o mesmo tipo de dado recebe tratamentos diferentes conforme o contexto concreto, tornando-se assim um guia útil aos servidores em sua prática profissional cotidiana.

3.4 A salada teórica entre LAI e LGPD e a ampliação do arbítrio estatal

O Guia afirma adotar uma premissa clara sobre o regime jurídico aplicável. O Enunciado nº 4, de 10 de março de 2022⁴, da Controladoria-Geral da União, estabelece que as decisões sobre a publicidade de dados de pessoas naturais em pedidos de acesso e respectivos recursos devem ser fundamentadas nos arts. 3º e 31 da LAI. O próprio documento reproduz esse entendimento, afirma que a LGPD não criou novas hipóteses de sigilo e reconhece a LAI como norma específica para decidir sobre o acesso a informações pessoais sob custódia estatal.

Essa definição, contudo, não orienta a construção conceitual e metodológica do Guia. Em vez de aplicar consistentemente o regime da LAI e utilizar a LGPD como instrumento complementar de interpretação, o documento seleciona conceitos isolados de ambas as leis, altera a função que desempenham em seus respectivos sistemas e os recombina em uma arquitetura jurídica incoerente e inexistente.

O resultado é um regime híbrido que não corresponde integralmente a nenhuma das duas leis. Da LAI, o Guia preserva as categorias abertas de intimidade, vida privada, honra e imagem, classificações mais amplas e ultrapassadas do que as da própria LGPD. Por outro lado, da LGPD, pinça sobretudo os princípios da finalidade, da necessidade e da minimização e os distorce na aplicação. Para piorar, não incorpora, com o mesmo rigor, os limites de

⁴ Em: < <https://basedeconhecimento.cgu.gov.br/handle/1/14073> >. Acesso em: 22/07/2026.

incidência, as definições e as orientações da própria Agência Nacional de Proteção de Dados que poderiam afastar ou reduzir a restrição. Soma-se ainda imprecisões jurídicas e técnicas examinadas na Seção 3.6 desta contribuição.

Combinados seletivamente, esses elementos ampliam as possibilidades de restrição: um universo extenso de informações pode ser inicialmente enquadrado como restrito e, mesmo quando se reconhece a possibilidade de acesso, a divulgação é reduzida ao menor conjunto que o agente estatal considere suficiente.

Essa seleção não é neutra. Ela opera sistematicamente em uma única direção: amplia a margem de decisão do Estado, fragiliza as salvaguardas favoráveis ao acesso e reduz o conteúdo disponibilizado ao cidadão.

3.4.1 O Guia desloca a finalidade do tratamento realizado pelo Estado para a finalidade pretendida pelo cidadão dentro da transparência pública

O princípio da finalidade previsto no art. 6º, I, da LGPD exige que cada operação de tratamento tenha propósito legítimo, específico, explícito e informado. A finalidade é um atributo do tratamento realizado pelo controlador. Em uma relação privada, por exemplo, uma empresa pode tratar determinados dados com a finalidade de prestar o serviço contratado. No poder público, o art. 23 da LGPD determina que o tratamento atenda a uma finalidade pública e esteja vinculado ao exercício de competências ou atribuições legais.

No atendimento a um pedido formulado com base na LAI, a operação realizada pelo órgão consiste em localizar, analisar e divulgar informações para cumprir o dever legal de transparência, garantir o direito de acesso e viabilizar o controle social. Essa é a finalidade juridicamente relevante para a aplicação da LGPD: a finalidade da divulgação realizada pelo Estado em cumprimento aos seus deveres de transparência pública.

O Guia desloca indevidamente essa análise para o requerente. Em vez de verificar se a divulgação atende à finalidade pública estabelecida pela LAI, **pergunta qual interesse coletivo o cidadão pretende promover, por que o cidadão necessita da informação e que uso específico fará dos dados.**

São perguntas juridicamente distintas. Uma coisa é indagar por que o Estado trata e divulga a informação. A resposta é o cumprimento de sua obrigação legal de transparência. Outra é perguntar para que o cidadão utilizará a informação depois de recebê-la. Essa segunda questão não integra o princípio da finalidade da LGPD e não pode condicionar o acesso.

O Guia transforma, portanto, a finalidade em um segundo filtro dentro da própria transparência pública. O cidadão deixa de precisar apenas solicitar uma informação e passa a ter de demonstrar qual uso pretende fazer dela dentro da finalidade geral de transparência ou controle social. A LGPD, contudo, não autoriza o Estado a selecionar quais usos da informação pelo cidadão seriam suficientemente legítimos. Ela exige que o próprio Estado demonstre que sua operação de tratamento possui fundamento e finalidade públicos.

A correção necessária não é afastar o princípio da finalidade, mas aplicá-lo ao sujeito e à operação corretos. Cabe examinar se o tratamento realizado pelo órgão atende ao dever legal de transparência. Não cabe transformar esse princípio em investigação sobre o uso pretendido pelo requerente.

3.4.2 O Guia descola os conceitos de "necessidade" e "minimização" para ampliar a discricionariedade do Estado

O mesmo deslocamento aparece quando o Guia orienta que sejam divulgados apenas os dados "estritamente necessários", na hipótese de defesa de direitos humanos, "indispensáveis e proporcionais", na hipótese de interesse público e geral preponderante, ou o "minimamente necessários", no roteiro decisório.

O princípio da necessidade previsto no art. 6º, III, da LGPD limita o tratamento realizado pelo controlador aos dados pertinentes, proporcionais e não excessivos para alcançar sua finalidade. Aplicado corretamente à transparência pública, pode orientar a retirada pontual de informações efetivamente protegidas, preservando o acesso ao restante.

No Guia, entretanto, necessidade e minimização passam a definir o quanto o agente considera suficiente entregar ao requerente. Para aferir o que seria necessário, indispensável ou suficiente, o servidor precisa primeiro presumir qual seria a

finalidade do cidadão. A análise da motivação reaparece, assim, como pressuposto informal da decisão sobre quanto divulgar.

Além disso, essas expressões atribuem ao agente ampla margem pessoal para definir a extensão do acesso, gerando insegurança jurídica e incentivo à divulgação mínima por cautela. A pergunta deixa de ser quais parcelas possuem fundamento legal para permanecer protegidas e passa a ser quanto da informação o Estado considera suficiente para atender à finalidade que atribuiu ao pedido.

A inversão é clara. Pela LAI, o órgão deve fornecer todo o conteúdo público e retirar apenas as parcelas inequivocamente abrangidas por uma hipótese legal de restrição. **Na lógica do Guia, a Administração seleciona o menor conjunto que considera adequado e retém o restante.** A minimização do tratamento transforma-se, assim, em minimização do direito de acesso.

A expressão “estritamente necessário” é particularmente problemática na hipótese de defesa de direitos humanos. Organizações e cidadãos dependem de informações públicas para documentar violações, identificar padrões, responsabilizar autoridades e proteger direitos fundamentais. Conferir ao próprio órgão fiscalizado o poder de definir qual seria o mínimo suficiente pode enfraquecer essas iniciativas e conferir aparência de legitimidade a decisões restritivas ou autoritárias.

Proposta de redação:

"Substituir, em todas as hipóteses de divulgação e no Teste de Interesse Público, os critérios de 'estritamente necessário', 'dados indispensáveis e proporcionais' e 'minimamente necessário' pelo seguinte parâmetro único: “A divulgação deve ser feita de forma a impedir a exposição de dados cujo acesso, em análise fundamentada, seja verificado como inequivocamente restrito após aferidos os riscos de danos concretos e prováveis ao titular, sendo os demais dados divulgáveis independentemente de demonstração adicional de indispensabilidade.”

3.4.3 O efeito combinado: a acentuação da assimetria de poder entre sociedade e Estado e a ampliação do espaço para arbitrariedade

Os deslocamentos promovidos pelo Guia operam de forma combinada. Primeiro, o agente público é induzido a identificar e avaliar a finalidade pretendida pelo cidadão. Em seguida, utiliza essa finalidade presumida para decidir qual seria o volume mínimo de informação necessário para atendê-la. **O agente estatal passa, assim, a controlar simultaneamente a legitimidade do uso pretendido e a suficiência do conteúdo que considera adequado entregar.**

A Lei de Acesso à Informação foi concebida⁵ para enfrentar uma relação estruturalmente assimétrica. O Estado concentra a produção, a guarda e o controle das informações necessárias para que a sociedade compreenda e fiscalize sua atuação. O cidadão, por sua vez, depende do próprio Estado para acessar os registros que permitem avaliar políticas públicas, proteger direitos, controlar gastos e exigir prestação de contas. Nesse contexto, **o exercício do direito de acesso não pode ficar condicionado a um juízo estatal arbitrário sobre a relevância, a conveniência ou a legitimidade da demanda apresentada.**⁶

A LAI responde a essa assimetria vedando ao Estado exatamente a margem de discricionariedade que lhe permitiria transformar esse poder em arbítrio: o art. 10, § 3º, dispõe que "são vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público".

O Parecer sobre Acesso à Informação elaborado pela CGU para atender ao Despacho Presidencial de 1º de janeiro de 2023⁷ (Brasília, fevereiro de 2023) consolida esse entendimento no item 6.3.2, sob o título "Princípio da desmotivação do pedido": o princípio "obriga os agentes públicos a desconsiderar quaisquer conjecturas a respeito de que usos o cidadão poderá vir a fazer ou não fazer da informação solicitada". **Um guia orientativo elaborado pela própria CGU não pode, portanto, conter dispositivos que induzam o agente público a avaliar, ainda que indiretamente, o motivo ou a finalidade do pedido.** Como se demonstra nas seções seguintes desta contribuição, a minuta o faz em diversos pontos, incluindo na distinção entre "interesse coletivo" e "curiosidade geral", na hipótese de defesa de direitos humanos e nas perguntas norteadoras do próprio roteiro decisório do Capítulo 4.

⁵ Nesse sentido, vide Mensagem 316/2009, da Presidência da República ao Congresso Nacional e a Exposição de Motivos 07/2009. Em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=656533&filename=M-SC+316/2009+%3D%3E+PL+5228/2009> <<https://www.gov.br/memoriasreveladas/pt-br/acesso-a-informacao/institucional/PL5228.pdf/@@display-file/file>>. Acesso em: 21/07/2026.

⁶ De acordo com o Right to Information Index (RTI - Index), em 2026 mais de 109 países implementaram essa garantia. Em: <<https://www.rti-rating.org/country-data/by-indicator/13/>>. Acesso em: 21/07/2026.

⁷ Em: <<https://basedeconhecimento.cgu.gov.br/handle/1/16744>>. Acesso em: 21/07/2026.

A mesma vedação é violada por via indireta, quando o Guia exige que a divulgação se limite ao "estritamente necessário" para atender ao pedido. Esse tipo de exigência força o agente a reconstruir, ainda que informalmente, qual seria a finalidade do requerente, único parâmetro contra o qual a suficiência do "necessário" poderia ser aferida. **Estabelecer que apenas o mínimo será fornecido equivale, além disso, a afirmar que o sigilo é a regra e o acesso, a exceção, invertendo diretamente a lógica do texto e o espírito da LAI** e a posição preferencial do direito de acesso à informação.

A transparência como regra e a proibição de indagar a motivação foram dois dos principais avanços trazidos pela lei, responsáveis por superar a cultura do sigilo arbitrário e as negativas fundadas em "ausência de interesse público" na demanda. **Um guia que reintroduz esse tipo de exigência retrocede exatamente ao ponto que a LAI foi redigida para superar.**

Essa vedação tem um corolário que a minuta ainda não enfrenta: **não cabe ao agente estatal determinar o que é ou não de interesse público.** A avaliação do interesse público é geral preponderante, tal como estruturada no roteiro decisório, converte o agente público em árbitro do que merece ou não ser conhecido pela sociedade, papel que nenhuma norma lhe atribui e que a própria arquitetura da LAI rejeita ao consagrar a publicidade como regra geral. O objeto da análise deveria ser sempre a informação, os riscos concretos e identificáveis, bem como a sua probabilidade de acontecer frente aos benefícios coletivos avistados.

3.5 Responsabilidade pessoal do agente público: a assimetria entre a sanção à opacidade e a ausência de proteção à boa-fé

A alocação do ônus sobre a restrição, tratada nas seções anteriores, só produz efeito prático se acompanhada de dois mecanismos que precisam ser simétricos: proteção expressa a quem divulga de boa-fé, e responsabilização explícita de quem restringe indevidamente. Sem o primeiro, o agente tende à negativa por cautela pessoal⁸, ainda que a lei favoreça o acesso; sem o segundo, a restrição indevida segue sem custo, o que reforça o mesmo desvio.

O fundamento para a proteção já existe no direito brasileiro: o art. 28 do Decreto-Lei nº 4.657/1942 (Lei de Introdução às Normas do Direito Brasileiro) estabelece que o agente público responde pessoalmente por suas decisões apenas em caso de dolo ou erro grosseiro. O Guia deve tornar esse mecanismo explícito para o cenário de divulgação de dados

⁸ Nesse sentido: MENDEL, Toby. *The Public's Right to Know. Principles on Freedom of Information Legislation*. London: ARTICLE 19, 1999. p. 16. Em: < https://www.access-info.org/wp-content/uploads/Article_19_principles_on_the_public_right_to_know.pdf >. Acesso em: 21/07/2026.

peçoais, afastando sanção pessoal ao agente que aplicar razoavelmente seus critérios e procedimentos.

A contrapartida já vem sendo construída pela própria CGU: o Enunciado nº 2/2024 estabelece que "o reiterado descumprimento das orientações do órgão central sobre o uso do fundamento 'informações pessoais' para negar pedidos de acesso à informação sujeitará o agente público à apuração de responsabilidade, conforme o disposto no art. 32 da Lei nº 12.527". No mesmo sentido, o Tribunal de Contas da União recomendou que a CGU "identifique, oriente e, se necessário, responsabilize, por meio de sua função correcional, os órgãos públicos e servidores que indevidamente removem ou não mantêm atualizadas informações essenciais para a transparência ativa" (Voto do Ministro-Relator, TC 002.249/2023-5, Acórdão 506/2025 - Plenário TCU, item 10). O Guia deve incorporar essa diretriz como regra operacional padrão, não como recomendação isolada.

É este par de mecanismos, e não apenas um deles, que constitui a virada de tom que esta contribuição propõe: **uma lógica em que o custo pessoal recai sobre quem restringe indevidamente, não sobre quem divulga de boa-fé.**

Proposta de redação:

Inserir, no Capítulo 3 do Guia: "Desde que observado o devido processo administrativo, o agente público responsável por fornecer informações pessoais, por transparência ativa ou passiva, em atendimento à Lei nº 12.527/2011 apenas poderá ser responsabilizado em caso de comprovação de dolo ou erro grosseiro, nos termos do art. 28 do Decreto-Lei nº 4.657/1942 (Lei de Introdução às Normas do Direito Brasileiro)."

3.6 Imprecisões jurídicas e técnicas presentes ao longo da minuta

A incorporação da LGPD, que, como já apontado anteriormente é fragmentada em sua estrutura, contém ainda imprecisões até mesmo em suas categorias básicas. Os exemplos abaixo não são exaustivos.

3.6.1 Anonimização

O Guia trata a anonimização, em diversas passagens (pesquisa, transparência por desenho, mitigação de risco), como técnica de proteção aplicada ao dado pessoal, mas em nenhum momento esclarece que, uma vez efetivamente anonimizado, o dado deixa de ser dado pessoal para todos os efeitos legais (art. 12, *caput*, da LGPD). O Estudo Técnico sobre a

Anonimização de Dados na LGPD, publicado pela ANPD⁹, trata a anonimização precisamente como processo apto a afastar a caracterização do dado como pessoal e a reduzir riscos, distinção que a minuta não incorpora com a devida clareza. O risco é que agentes públicos entendam que informação anonimizada segue sujeita ao mesmo roteiro decisório do Capítulo 4, quando, tecnicamente, ela já saiu do escopo de proteção da LGPD e deveria ser divulgável sem as etapas do teste.

A tabela do Guia ainda descreve o tarjamento como forma de pseudonimização, embora sejam técnicas distintas, reforçando a falta de rigor no emprego do vocabulário da LGPD.

Proposta de redação:

"Incluir no Capítulo 4, no trecho introdutório sobre técnicas de mitigação, esclarecimento de que o dado efetivamente anonimizado, nos termos do art. 12, caput, da Lei nº 13.709/2018, e do Estudo Técnico sobre a Anonimização de Dados na LGPD (ANPD), não é considerado dado pessoal, não estando sujeito às demais etapas do roteiro decisório deste Guia."

3.6.2 Tratamento de dados pessoais de pessoas mortas e pessoas ausentes

O Guia tampouco delimita que a LGPD não incide sobre dados relativos exclusivamente a pessoas falecidas. A Nota Técnica nº 3/2023/CGF/ANPD¹⁰, de março de 2023, concluiu que a existência da pessoa natural termina com a morte, conforme o art. 6º do Código Civil, e que os dados de pessoas falecidas não constituem dados pessoais para fins da LGPD. A ANPD esclareceu que eventuais interesses pós-morte podem ser protegidos por outros instrumentos, como os direitos ao nome e à imagem, mas não pelo regime de proteção de dados pessoais. Nesse sentido, inclusive, o art. 6º e parágrafo único da Resolução nº 54/2023 do Conselho Nacional de Arquivos (CONArq)¹¹:

⁹ Em: <
https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd_analise_juridica.pdf/@@display-file/file >.
Acesso em: 22/07/2026.

¹⁰ Em: <
<https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-3-2023-cgf-anpd.pdf/@@display-file/file> >. Acesso em: 22/07/2026.

¹¹ Em: <
<https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-54-de-8-de-dezembro-de-2023> >. Acesso em: 22/06/2026.

Art. 6º Os dados de pessoas falecidas, existentes em arquivos permanentes, não estão sujeitos aos dispositivos da Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo único. Os dados de pessoas ausentes, existentes em arquivos permanentes, não estão sujeitos aos dispositivos da LGPD, nos casos em que a lei autoriza a abertura de sucessão definitiva.

A omissão permite que o agente aplique indistintamente princípios, riscos e procedimentos da LGPD a informações que estão fora de seu âmbito de incidência. Isso não significa que toda informação sobre pessoa falecida seja automaticamente pública, mas que eventual restrição deve encontrar fundamento em outra norma, e não ser presumida com base na LGPD.

3.6.3 Gênero como dado pessoal sensível

A tabela do procedimento inclui gênero entre os “dados pessoais sensíveis, nos termos da LGPD”. Gênero, contudo, não aparece no rol do art. 5º, II, que abrange origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou a organizações religiosas, filosóficas ou políticas, dados referentes à saúde ou à vida sexual, além de dados genéticos e biométricos.

Isso não impede que informações sobre gênero demandem proteção em contextos específicos, mas essa conclusão depende do conteúdo e dos riscos concretos envolvidos, e não de uma classificação legal inexistente.

3.6.4 Raça, idade e sexo

Em outro trecho, o Guia apresenta raça, idade e sexo como exemplos de dados cuja divulgação seria excessiva e deveria ser restringida, salvo quando constituíssem requisito para o recebimento de benefícios públicos. Essa formulação mistura três categorias diferentes. Raça integra o rol de dados sensíveis da LGPD. Idade e sexo não. Nenhuma delas, porém, está automaticamente submetida a sigilo perante a LAI.

A divulgação desses atributos pode ser indispensável para conhecer o perfil de servidores e usuários de serviços públicos, avaliar cobertura e desigualdades e fiscalizar políticas de equidade. O próprio Guia trata informações de heteroidentificação como excessivas na

tabela de minimização, mas reconhece, na seção sobre bolsas e ações afirmativas, sua relevância para o controle de fraudes, revelando uma contradição interna.

As Notas Técnicas nº 46/2022/CGF/ANPD¹² e nº 12/2023/CGF/ANPD¹³, relativas aos microdados do Censo Escolar e do Enem, também não estabeleceram proibição geral à divulgação de dados sensíveis. A ANPD determinou a avaliação dos riscos, inclusive por relatório de impacto, e admitiu diferentes níveis de divulgação, com medidas adequadas de mitigação.

Essas inconsistências mostram que o Guia não apenas seleciona conceitos da LGPD de forma fragmentada, mas também os utiliza sem a precisão exigida de um documento destinado a orientar decisões sobre direitos fundamentais.

Proposta de redação:

"Suprimir idade, raça e sexo do rol exemplificativo de dados cuja divulgação deve ser restringida. Inserir, em seu lugar, observação de que a restrição a esses atributos não é automática nem inflexível, devendo a divulgação ser avaliada caso a caso, com atenção a hipóteses em que ela é relevante ao controle social, como a aferição do perfil de servidores públicos, de usuários de serviços e políticas públicas, e da efetividade de políticas de redução de desigualdades.

3.7 Consequência dos problemas estruturais: o roteiro decisório deve ser reconstruído

Os problemas demonstrados nesta seção atingem os próprios fundamentos do roteiro decisório do Capítulo 4. A metodologia parte de uma equivalência indevida entre publicidade e restrição, reabre matérias já resolvidas, analisa categorias de dados fora de seu contexto, distorce conceitos da LGPD e amplia a discricionariedade estatal. Não se trata, portanto, de falhas isoladas em perguntas ou etapas específicas, mas de uma arquitetura incompatível com as premissas constitucionais, convencionais e jurisprudenciais apresentadas na Seção 2.

¹² Em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/sei_00261-000730_2022_53-nt-46.pdf/@@display-file/file>. Acesso em: 22/07/2026.

¹³ Em: <<https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-12-2023-cgf-anpd-inep.pdf>>. Acesso em: 22/07/2026.

Propõe-se substituir a denominação “Teste de Interesse Público” por **Procedimento de Ponderação para Restrição de Acesso à Informação Pessoal**, pois é a restrição, e não o interesse do requerente, que deve ser submetida a justificação. A mudança de nome, contudo, não é o centro da questão: manter a estrutura atual sob outra denominação apenas preservaria os mesmos problemas.

Por essa razão, esta contribuição deliberadamente não apresenta alterações pontuais ao roteiro decisório. **Sugerir a substituição de perguntas, a inversão de etapas ou ajustes localizados poderia conferir aparência de correção a uma metodologia que precisa ser repensada desde sua origem.** Antes de se formular um novo fluxo, é necessário enfrentar e solucionar, de maneira integrada, todos os problemas estruturais identificados nesta seção.

Somente a partir dessa revisão será possível construir um procedimento que parta da publicidade como regra, verifique previamente as normas e os entendimentos aplicáveis, analise a informação em seu contexto documental, concentre no Estado o ônus de justificar a restrição e reserve a ponderação aos casos em que persista dúvida jurídica real. O roteiro atual não deve ser remendado, mas substituído por uma nova metodologia construída desde o início sobre bases juridicamente corretas.

4. Necessidade de centralização da governança em capítulo próprio e ajustes teóricos

A minuta já reúne elementos relevantes de governança, como transparência por desenho e registro das decisões. Esses pontos, porém, aparecem dispersos ao longo do texto, sem constituir um sistema facilmente aplicável. Somados às propostas apresentadas nesta seção, devem ser reorganizados em capítulo próprio, com estrutura objetiva e intuitiva, capaz de orientar o agente público no uso cotidiano do Guia.

4.1 O Termo de Responsabilidade como condição geral de acesso

“As pessoas que acessarão os dados pessoais devem assinar Termo de Responsabilidade, que indique que as informações serão de uso restrito à pesquisa, sob pena de responsabilização”; “Orientações gerais para fornecer informações pessoais para defesa de direitos humanos: [...] Exigir assinatura de Termo de Responsabilidade para restringir o uso à finalidade específica”. (p. 15).

A minuta condiciona o acesso de terceiros a informações pessoais, como regra, à assinatura de Termo de Responsabilidade com vinculação de finalidade, dispensando-o apenas em hipóteses enumeradas (item 3.4 da minuta). Duas objeções se impõem. A primeira é sistemática: o art. 10, § 3º, da LAI veda quaisquer exigências relativas aos motivos determinantes da solicitação. A vinculação do uso da informação a uma finalidade declarada pressupõe, logicamente, a declaração dessa finalidade, reintroduzindo pela via do instrumento aquilo que a lei baniou pela via do procedimento. A segunda é conceitual: quando o acesso é deferido por preponderância do interesse público (art. 31, § 3º, V, da LAI), a informação torna-se pública para todos, como a própria minuta reconhece ao dispensar o termo nessa hipótese. No caso da proteção de direitos humanos (art. 31, § 3º, IV, da LAI), além da informação também se tornar pública para todos, exigir termo de responsabilidade como condicionante configura retrocesso avassalador no cenário jurídico brasileiro e contradiz inúmeras políticas federais. O instrumento somente faz sentido nas hipóteses de acesso subjetivamente qualificado (pesquisa com acesso à íntegra de dados pessoais considerados restritos e à prevenção e diagnóstico médico), nas quais a informação é entregue a destinatário determinado sem adquirir publicidade geral.

Proposta de redação:

Suprimir as diversas menções a Termo de Responsabilidade espalhadas pelo guia e criar uma seção única explicitando que o Termo de Responsabilidade é instrumento excepcional, cabível exclusivamente nas hipóteses de pesquisa com acesso à íntegra de dados pessoais considerados restritos ou à prevenção e diagnóstico médico, casos em que a informação é fornecida a destinatário determinado e sem aquisição

de publicidade geral, vedada sua exigência como condição de acesso a informações públicas ou como sucedâneo de declaração de motivos, nos termos do art. 10, § 3º, da LAI.

4.2. Registro da ponderação na decisão

“O registro da decisão é essencial para que a sociedade possa conhecer os critérios utilizados pela Administração Pública na ponderação entre o direito de acesso à informação e a proteção dos dados pessoais, bem como para possibilitar o eventual questionamento das decisões adotadas. A motivação deve demonstrar, de forma clara e objetiva, qual interesse coletivo está sendo considerado, quais são os benefícios concretos esperados para a coletividade com a divulgação do dado pessoal, quais os riscos de dano ao titular, as razões que justificam a divulgação integral, parcial ou a restrição de acesso”

A minuta acerta ao determinar que uma decisão de ponderação bem fundamentada deve registrar, no mínimo, estes quatro elementos. Mas, por incorporar conceitos equivocados na sequência (necessidade) e por relativizar com a frase “sempre que possível”, o texto precisa ser reajustado.

Proposta de redação:

“O registro da decisão final deverá conter, no mínimo: (i) descrição e demonstração do prejuízo identificável e específico ao titular decorrente do fornecimento ou divulgação; (ii) descrição do benefício coletivo e da probabilidade de sua concretização; (iii) demonstração da prevalência do risco sobre o benefício, ou vice-versa; (iv) descrição das medidas de mitigação de risco avaliadas e, em caso de negativa integral, a demonstração da inviabilidade do acesso parcial; e (v), em caso de acesso parcial, indicação específica do que não foi entregue e do fundamento da restrição. O registro da decisão deve ser realizado na resposta ao pedido de acesso à informação formulado.”

4.3 Publicidade centralizada das decisões de negativa

O Guia não prevê mecanismo adequado de consolidação ou publicidade das decisões tomadas com base em seu próprio roteiro decisório, o que impede o controle social sobre a aplicação do documento na prática, exatamente o risco de assimetria sistemática identificado nesta contribuição. O próprio TCU já recomendou, no âmbito do Acórdão nº

1841/2022 - TCU - Plenário (TC 014.307/2021-9, sessão de 10/8/2022), que órgãos classifiquem e publiquem informações vinculadas a processos de seleção e adotem meios de estimular o controle social sobre dados custodiados pela Administração. O mecanismo é diretamente aplicável ao Guia e complementa a proposta da Seção 4.6 desta contribuição sobre a verificação periódica da autoridade de monitoramento: aquela trata da revisão de segregações; esta, da publicidade agregada das negativas.

Proposta de redação:

Incluir orientação de que as decisões de negativa de acesso a informação pessoal, fundamentadas no roteiro decisório deste Guia, sejam periodicamente consolidadas e publicadas na seção “Acesso à Informação”¹⁴ do site do órgão público e, posteriormente, enviadas à Controladoria-Geral da União, à qual caberá dar publicidade ao conjunto de decisões, com seus fundamentos, em local de fácil acesso em seu sítio eletrônico, permitindo o controle social sobre a aplicação do Guia pelos órgãos e entidades da Administração Pública federal.

4.4 Consulta pública para retirada de bases e documentos de transparência ativa

De acordo com o art. 3º, IV e V da LAI a implementação da política de acesso à informação não apenas visa o fortalecimento do controle social, como também permitir e fortalecer a participação social. Justamente por isso, o Regulamento da Política de Dados Abertos (Decreto nº 8.777/2016) assegura em seu art. 5º, §2º, V a utilização obrigatória de processos de participação da sociedade civil na escolha e priorização de dados para abertura. Por outro lado, embora o princípio da transparência faça parte da política de proteção de dados, constata-se na prática que órgãos e entidades têm adotado decisões unilaterais, sem aviso prévio ou divulgação prévia da motivação para modificação ou remoção de bases de dados e informações até então disponibilizadas ao público.

Em homenagem ao princípio da transparência, segurança pública e coerência administrativa, processos de implementação de políticas de proteção de dados e, em especial, decisões que afetem bases de dados disponibilizadas ao público, precisam também ser submetidos à consulta pública prévia, fundamentada e informada. Igualmente, o resultado da consulta, a análise das contribuições apresentadas e a decisão final do órgão também precisam ser objeto de divulgação, tanto em seção específica quanto no próprio local onde antes os dados eram então localizados. O texto do Guia, ao não fazer menção alguma ao assunto, perde a oportunidade de reduzir incertezas jurídicas e o atrito decorrente de situações como esta.

¹⁴ Observação: a seção “Acesso à Informação” é obrigatória em todos os sites sob o domínio “[gov.br](https://www.gov.br)” Em: < <https://www.gov.br/ds/assets/downloads/GovbrManualdeDiretrizes.pdf> >. Acesso em: 21/07/2026.

Proposta de redação:

Incluir, em capítulo ou seção específica do guia: “A retirada completa ou a redução de escopo de bases de dados ou documentos já disponibilizados em transparência ativa ou mesmo cuja divulgação por transparência passiva esteja consolidada deverá ser obrigatoriamente precedida de consulta pública. No ato de convocação, o qual deverá ser objeto de ampla divulgação, inclusive no site do órgão ou entidade e redes sociais disponíveis, deverá ser divulgada a fundamentação da decisão submetida a consulta e os documentos técnicos sobre ela produzidos. A consulta pública deverá ter prazo razoável de duração que, na ausência de fundamentação específica, será de quarenta e cinco dias (art. 4º e art. 29 do Decreto-Lei nº 4.657/1942 c/c art. 9º, §2º, Lei nº 13.848/2019). O resultado da consulta, a análise das contribuições apresentadas e a decisão final precisam ser divulgadas, por transparência ativa, em seção específica do sítio eletrônico do órgão ou entidade.”

4.5. Gestão do acervo de informações pessoais

“[...] é importante destacar que o pleno exercício do direito de acesso à informação depende do constante aprimoramento da gestão documental, com sistemas e processos que viabilizem a adequada produção, organização, preservação e disponibilização das informações públicas, conforme determinam a Constituição Federal e a LAI.” (p.3)

Embora reconheça a necessidade de investimentos na gestão do acervo documental, o Guia também perde a oportunidade de orientar e exigir procedimentos contínuos de gestão do acervo já existente de documentos e informações pessoais. Essa desmobilização e desinvestimento da capacidade de gestão arquivística tende apenas a piorar com o passar dos anos e o progressivo acúmulo de informações. Não raramente, mesmo pedidos de acesso a informações pessoais pelo próprio titular são negados em razão da desorganização arquivística. Tal como recomendado no Regulamento da Política Federal de Dados Abertos, a interação do cidadão via pedidos de informação precisa ser utilizada como subsídio para planos de trabalho voltados a levantar, identificar, catalogar, organizar, armazenar e disponibilizar, tanto nos termos da LAI quanto da LGPD, as informações pessoais custodiadas.

Proposta de redação:

Incluir, no Capítulo 4 do Guia, seção que oriente órgãos a estabelecer e publicar planos de trabalho, atualizados periodicamente, nos quais constem medidas adotadas e a serem adotadas para organização e gestão do acervo de documentos e informações pessoais. Necessariamente, esses planos de trabalho precisam ser desenvolvidos mediante atuação conjunta de comissões de gestão de arquivos, autoridades de monitoramento da LAI e encarregados de proteção de dados.

4.6 Transparência por desenho: o risco da segregação sem revisão

“Sempre que possível, devem ser adotadas técnicas de transparência por desenho, com o objetivo de promover a transparência de forma compatível com a proteção de dados pessoais. A transparência por desenho consiste na incorporação, desde a fase de concepção de políticas públicas, sistemas de informação, bases de dados, processos administrativos e rotinas institucionais, de critérios voltados à futura divulgação de informações públicas. Essa abordagem busca organizar fluxos de trabalho, processos e sistemas já considerando a necessidade de promover a transparência, ao mesmo tempo em que permite identificar e separar, de forma antecipada, as informações que devem permanecer protegidas, como as informações sigilosas e as informações pessoais submetidas a regime de proteção”. (p. 29)

A recomendação de segregação prévia de informações (processos SEI relacionados, com o processo acessório categorizado como restrito) é boa prática e merece apoio. Sem mecanismo de revisão, contudo, o repositório restrito tende a expandir-se indefinidamente: a classificação é feita no momento de menor accountability, a autuação, e raramente é revisitada. Para que a transparência por desenho não degenere para **sigilo por desenho**, o guia deve prever contrapesos estruturais, aproveitando a figura da autoridade de monitoramento já existente na LAI.

Proposta de redação:

Acrescentar ao item 4.3 da minuta: “A segregação prévia de informações deve ser acompanhada de: (i) revisão periódica, ao menos anual, do acervo segregado como restrito, com desclassificação do que não mais se justifique; (ii) registro estatístico, em transparência ativa, do volume de documentos segregados como restritos, por unidade administrativa; e (iii) verificação periódica, pela autoridade de monitoramento de que trata o art. 40 da Lei nº 12.527/2011, da adequação das segregações realizadas.”

5. Problemas específicos da minuta

Nesta seção, cada ponto crítico é apresentado em quatro tempos: transcrição ou descrição do trecho da minuta, identificação do problema, fundamentação jurídica e proposta objetiva de alteração.

5.1 A negativa por “pedido desproporcional” fundada no custo de triagem de dados pessoais

Ao exemplificar o pedido desproporcional (“Quero cópia de todos os documentos registrados no SEI em 2023”), a minuta justifica: “Nesse caso, seria necessário analisar todos os documentos para verificar a existência de dados pessoais protegidos ou outras informações sigilosas.” (item 1.2).

O exemplo expõe e reforça um mecanismo circular perigoso: o custo de conformidade com a proteção de dados torna-se, ele próprio, fundamento de negativa de acesso. Quanto pior a gestão documental do órgão e quanto menos implementada a transparência por desenho que o próprio Guia preconiza, mais “desproporcional” será qualquer pedido abrangente, e mais legítima parecerá a recusa. **Premia-se, portanto, a desorganização e a opacidade.** A minuta chega a registrar, corretamente, que o órgão não pode se eximir indefinidamente por dificuldades operacionais, mas não dá limitações concretas para o uso desta justificativa. O exemplo escolhido estimula o caminho inverso e será, previsivelmente, o trecho citado nas negativas.

Proposta:

Reformular o item para prever que a negativa fundada em desproporcionalidade: (i) é excepcional e exige demonstração concreta e quantificada do comprometimento do funcionamento regular do órgão; (ii) não pode fundar-se exclusivamente no custo de triagem de dados pessoais, cabendo ao órgão, nesse caso, indicar as medidas de transparência por desenho em implementação para superar a limitação; e (iii) deve vir acompanhada, sempre, de oferta alternativa concreta (entrega parcelada, redução consensual de escopo, fornecimento de dados agregados ou indicação de base já publicada), com registro da alternativa oferecida na resposta ao requerente.”

5.2 A hipótese de pesquisa: restrição subjetiva sem base na LAI e o problema da identificação

“A demanda deve ser apresentada por representante de órgão de pesquisa. Segundo a LGPD, trata-se de órgão ou entidade da administração pública direta ou indireta, ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (definição trazida pelo art. 5º, inciso XVIII da LGPD).

- A demanda deve apresentar os dados pessoais requeridos, além de informações mínimas necessárias à avaliação do interesse público ou geral da pesquisa ou estudo. Não cabe avaliação da metodologia, mérito técnico ou científico da pesquisa.*
- As pessoas que acessarão os dados pessoais devem assinar Termo de Responsabilidade, que indique que as informações serão de uso restrito à pesquisa, sob pena de responsabilização.*
- Para pesquisas em saúde pública, os dados fornecidos serão tratados exclusivamente dentro do órgão, mantidos em ambiente controlado e seguro, que incluam, sempre que possível, a sua anonimização ou pseudonimização, e que considerem os devidos padrões éticos relacionados a estudos e pesquisas. Nesses casos, a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa poderá revelar dados pessoais.*
- Quando as informações forem fornecidas de forma anonimizada ou pseudonimizada, sem possibilidade de reidentificação, a assinatura de termo de responsabilidade é dispensada” (p. 15).*

A minuta exige que a demanda fundada na hipótese de estatísticas e pesquisas “seja apresentada por representante de órgão de pesquisa”, na definição do art. 5º, XVIII, da LGPD e, com apoio em entendimento da ANPD, admite a entrega de dados identificados quando a identificação for imprescindível aos objetivos da pesquisa (item 3.3, “d”).

Há dupla desconformidade, em sentidos opostos. De um lado, a LAI não contém restrição subjetiva: o art. 31, § 3º, II, autoriza o acesso para a realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, sem reservar a via a instituições. A importação da definição da LGPD (concebida para finalidade diversa, a de qualificar hipótese de tratamento) exclui pesquisadores independentes, jornalistas de dados, pós-graduandos sem vínculo formal e cidadãos no geral de uma hipótese legal que não os exclui, criando restrição infralegal ao direito de acesso. De outro lado, o mesmo dispositivo

da LAI é expresso ao vedar a identificação da pessoa a que as informações se referem quando o acesso se funda nessa hipótese. A orientação da ANPD sobre a desnecessidade de anonimização é defensável para tratamentos fundados na LGPD; transposta para o acesso fundado no art. 31, § 3º, II, da LAI, é *contra legem*. A minuta mistura as duas bases normativas e produz um híbrido que restringe o que a lei não restringiu (quem pode pedir) e flexibiliza o que a lei expressamente vedou (a identificação dos titulares).

Proposta de redação:

(i) Suprimir a exigência de que o requerente seja representante de órgão de pesquisa, admitindo a via a qualquer pessoa que demonstre o evidente interesse público ou geral da pesquisa ou estatística; (ii) esclarecer que, quando o acesso se fundar no art. 31, § 3º, II, da LAI, os dados serão fornecidos sem identificação dos titulares, mediante anonimização ou pseudonimização; e (iii) esclarecer que a entrega de dados identificados para fins de pesquisa depende de fundamento diverso (consentimento, previsão legal específica ou interesse público e geral preponderante), com a correspondente motivação.

5.3 “Interesse coletivo é diferente de curiosidade geral”: o exame de motivação pela janela

*“Vale lembrar, ainda, que interesse coletivo é diferente de curiosidade geral.”
(item 4.2, etapa 2).*

A advertência, embora corrente, é porta de reintrodução do exame de motivos, vedado pelo art. 10, § 3º, da LAI. **Qualificar um pedido como “mera curiosidade” pressupõe avaliar por que o requerente quer a informação, juízo que a lei proíbe expressamente.** Além disso, a afirmação levanta resquícios de uma cultura de opacidade da administração pública, em contrariedade com o art. 3º, IV, LAI. O roteiro decisório deve ser objetivo e impessoal: pergunta-se se a informação, em si, é apta a servir ao controle social e à prestação de contas, e a resposta independe de quem pede e do que pretende fazer. A informação apta ao controle social deve ser entregue tanto ao curioso quanto ao pesquisador; a inapta, negada a ambos. Sem essa ressalva expressa, a frase operará como fundamento retórico de negativas dirigidas contra requerentes, e não contra pedidos.

Proposta de redação:

Substituir a frase por: “A aferição do interesse público e geral é objetiva e recai sobre a informação, não sobre o requerente¹⁵: avalia-se a aptidão do dado, em si, para servir ao controle social, à prestação de contas e à proteção de direitos, sendo vedado ao órgão perquirir ou presumir os motivos da solicitação (art. 10, § 3º, da LAI).”

5.4 As tabelas do Capítulo 5 como regras categóricas: necessidade de cláusula geral de presunção relativa

O Capítulo 5 formula seus entendimentos em enunciados binários (“pode ser divulgado” / “não deve ser divulgado”). A experiência acumulada dos SICs demonstra que tabelas nesse formato são aplicadas como regras fechadas, dispensando a análise concreta, o que esvazia, por via transversa, o próprio roteiro decisório construído no Capítulo 4 do Guia. Algumas presunções restritivas são razoáveis como ponto de partida; nenhuma pode ser absoluta. Exemplo ilustrativo: os dados de veículos em listas de acesso a prédios públicos são rotulados como “desnecessários para a finalidade de controle social”, quando registros dessa natureza já se mostraram relevantes, em casos concretos, para a identificação de padrões de visitas e de tráfico de influência, admitindo divulgação com descaracterização parcial. O mesmo raciocínio vale, em direção inversa, para presunções de publicidade: circunstâncias concretas (servidor sob medida protetiva, por exemplo, como a própria minuta reconhece quanto à lotação) podem justificar restrição pontual e motivada.

Proposta de redação:

Inserir, na abertura do Capítulo 5, a cláusula geral: “As orientações constantes das tabelas deste capítulo veiculam presunções relativas, que estabelecem o ponto de partida da análise, mas não dispensam a aplicação do roteiro decisório do Capítulo 4 ao caso concreto e podem ser afastadas, em qualquer direção, mediante decisão motivada.” Rever, em coerência, as formulações “não deve ser divulgado” para “em regra, não se divulga, salvo demonstração de interesse público e geral preponderante no caso concreto”.

¹⁵ Inclusive, o foco no requerente opera como elemento dissuasório para eventuais demandantes de informações públicas. Nesse sentido: Michener G, Velasco RB, Contreras E, Rodrigues KF. Googling the requester: Identity-questing and discrimination in public service provision. *Governance*. 2020; 33: 249–267. <https://doi.org/10.1111/gove.12416>. Acesso em: 22/07/2026.

5.5 Terminologia das tabelas: substituir "pode" por "deve" nas hipóteses de transparência obrigatória

Verificação no texto do Guia mostra que a inconsistência entre "pode" e "deve" não se limita ao caso de Processos Administrativos Disciplinares (PADs) sobre assédio (Seção 5.11 desta contribuição): a tabela sobre PAD concluído usa "pode ser divulgado" para o nome do servidor sancionado, o cargo, a descrição da infração e o tipo de sanção, apesar de o próprio Guia citar, linhas depois, o art. 29, § 2º, IX, da Lei nº 14.129/2021 como fundamento. O mesmo padrão se repete na tabela de licitações e contratos, em que itens como contratos e termos aditivos, e notas fiscais e pagamentos, aparecem como "pode ser divulgado", quando sua publicidade decorre de obrigação de transparência decorrente da de legislação expressa (Lei nº 14.133/2021, Lei nº 14.129/2021, Lei nº 12.527/2011, Lei Complementar nº 101/2000, etc), não de faculdade do órgão.

Proposta de redação:

Revisar todas as tabelas do Capítulo 5 para substituir 'pode ser divulgado' por 'deve ser divulgado' sempre que a informação estiver sujeita a obrigação legal ou entendimentos já consolidados. Reservar a expressão 'pode ser divulgado' para os casos de divulgação efetivamente discricionária, sujeita à ponderação caso a caso."

5.6. Ausente das tabelas: casos complexos já decididos

As tabelas do Capítulo 5 e os exemplos do roteiro decisório tratam majoritariamente de casos de baixa complexidade (remuneração, PAD, licitação) e notórios e historicamente já pacificados. O Guia não incorpora precedentes de casos mais complexos, em que foi necessário real esforço de ponderação. Um exemplo relevante e recente é o Cadastro Ambiental Rural (CAR): o cadastro contém dados pessoais de proprietários e possuidores rurais (nome, CPF parcialmente ofuscado, delimitação da propriedade), e sua divulgação já foi objeto de pedidos de acesso à informação decididos favoravelmente por esta Controladoria-Geral da União, com reconhecimento do interesse público preponderante no monitoramento ambiental e fundiário sobre o interesse individual dos titulares na reserva desses dados. A inclusão desse tipo de precedente qualifica o Guia como referência prática para casos difíceis, e não apenas para os óbvios.

Proposta de redação:

Incluir, entre os exemplos da minuta, casos e precedentes de maior complexidade já analisados pelos órgãos competentes.

5.7 Redução da transparência da remuneração de agentes públicos

Na primeira tabela constante no item 5, p. 26, coluna “dado a ser divulgado (indispensável)”, consta genericamente apenas menção à divulgação da “remuneração bruta/líquida”. Essa referência genérica abre margem à redução do detalhamento hoje praticado na transparência de informações sobre despesas de pessoal. Além do texto não mencionar nem refletir a integralidade das informações exigidas pelo art. 7º, § 3º, VI, do Decreto nº 7.724/2012, é necessário recordar que o Guia é também referência para entes públicos subnacionais e não apenas para a União, cujas normas possuem densidade normativa mais detalhada. A coluna seguinte, sobre “dado que não pode ser divulgado (excessivo)”, traz dois equívocos conceituais importantes: **a)** embora o CPF seja o “padrão ouro” para fins de desambiguação e prevenção de homonímia, muitas bases de dados, em particular aquelas mais antigas, não possuem ou utilizam este dado em seus contextos; **b)** diversos entes públicos divulgam as informações sobre descontos em folha de pagamento apenas segregando e consolidando descontos de natureza pessoal numa só categoria, de forma a evitar identificação da natureza, por meio da rubrica “descontos de natureza pessoal”.

Proposta de redação:

No quadro relativo à remuneração, substituir a referência genérica à “remuneração bruta/líquida” por “relação completa das informações exigidas pelo art. 7º, § 3º, VI, do Decreto nº 7.724/2012”.

5.8. Agentes privados que gerenciam recursos públicos, prestam serviços ou possuem relação de interesse público com a administração pública: presunção de publicidade pouco ampla

O Guia trata a publicidade de informações de terceiros privados apenas no contexto pontual de licitações e contratos (tabela do Capítulo 5, restrita a “empresa contratada” e seu

representante legal), perdendo a oportunidade de aprofundar a questão e trazer parâmetros e subsídios para interpretação em casos que envolvam ao menos uma dessas situações, dentre outras: **a)** o agente privado arrecade, guarde, gerencie ou administre dinheiros, bens e valores públicos ou pelos quais a administração responda, ou que, em nome desta, assuma obrigações de natureza pecuniária; **b)** o agente privado exerça serviço público mediante qualquer modalidade de delegação estatal (autorização, permissão, concessão, etc); **c)** o agente privado presta serviços ou vende bens para a administração pública; **d)** o agente privado interage com a administração pública com a finalidade de influenciar a tomada de decisão ou política pública. Os itens “**b**” e “**c**”, em especial, são cada vez mais relevantes no atual cenário econômico de ampliação da prestação de serviços públicos por agentes privados.

Nessas modalidades de interação do agente privado com a administração pública, não há qualquer expectativa de privacidade que fundamente eventual restrição de informações pessoais¹⁶, ainda que possam existir outras razões, previstas em lei, para fundamentar eventual negativa. Ademais, além das bases constitucionais e convencionais já listadas na Seção 2 deste documento, a divulgação das informações também se baseia no princípio constitucional da isonomia.

Proposta de redação:

Incluir regra geral de que se presume pública a informação pessoal referente a agente privado que: **a)** arrecade, guarde, gerencie ou administre dinheiros, bens e valores públicos ou pelos quais a administração responda, ou que, em nome desta, assuma obrigações de natureza pecuniária; **b)** exerça serviço público mediante qualquer modalidade de delegação estatal (autorização, permissão, concessão, etc); **c)** presta serviços ou vende bens para a administração pública; **d)** interage com a administração pública com a finalidade de influenciar a tomada de decisão ou política pública.

5.9. Documentos preparatórios: a “regra simples” que simplifica demais

“A regra é simples: antes da decisão => acesso pode ser restringido; após a decisão => acesso deve ser garantido (exceto se houver outras hipóteses de sigilo).” (item 1.2).

¹⁶ Nesse sentido, por exemplo, o art. 2 da Lei Modelo Interamericana sobre Acesso à Informação Pública. Em: <https://www.oas.org/en/sla/dil/docs/Publicacao_Lei_Modelo_Interamericana_2_o_Acesso_Informacao_Publica.pdf>. Acesso em: 21/07/2026

O quadro sugere que a pendência do ato decisório autoriza, por si, a restrição de tudo o que o precede. Não é o que dispõe o art. 7º, § 3º, da LAI, que condiciona a restrição à existência de nexo entre o documento e ato ou decisão específica em elaboração e à sua necessidade, vale dizer, à demonstração de que a divulgação antecipada causaria prejuízo concreto ao processo decisório. Sem essas qualificações, notas técnicas, pareceres e estudos que instruem atos normativos permanecerão indefinidamente restritos sob o rótulo genérico de “preparatórios”, especialmente em processos regulatórios de longa maturação, com dano direto à participação social exatamente na fase em que ela é mais útil: a de formação da decisão.

Para além disso, tendo em vista que um “governo aberto” pressupõe a capacidade de participação efetiva da sociedade nos processos de formação, execução, acompanhamento e controle de políticas públicas, a “regra simples”, tal como escrita, permite a eliminação do direito de participação efetivo assegurado pelo art. 2º do Decreto nº 10.160/2019, tornando o restrição regra e não a exceção. Sendo o Brasil membro-fundador e atual co-presidente da Parceria para Governo Aberto¹⁷, a orientação viola o princípio básico dessa iniciativa.

Por fim, viola precedentes do STF nas ADPFs 690, 691 e 692 (rel. Min. Alexandre de Moraes, 2020) e a ADPF 872 (rel. Min. Carmen Lucia, 2023)¹⁸ que firmam entendimento claro segundo o qual qualquer modalidade de restrição exige justificação concreta. Ilustrativo do entendimento do STF sobre o ponto é o seguinte trecho do voto do Min. Roberto Barroso na ADI 5371: “[...] 9. A presunção constitucional de inocência dos concessionários nunca poderia, por si só, afastar a publicidade dos processos administrativos sancionadores. Se assim o fosse, todos os processos judiciais e administrativos que envolvessem direta ou indiretamente a imposição de penas ou outras sanções seriam sigilosos. A Constituição de 1988 caminhou em sentido diametralmente oposto: assegurou a publicidade dos julgamentos pelo Poder Judiciário como diretriz (art. 93, IX, CF/1988) e possibilitou a restrição da publicidade dos atos processuais somente em casos específicos, desde que não haja prejuízo ao interesse público à informação (art. 5º, LX, CF/1988). O Supremo Tribunal Federal já teve oportunidade de apreciar a constitucionalidade de regras relativas a julgamentos públicos. Nessa perspectiva, destaque-se trecho do voto do Min. Marco Aurélio na ADI 4.638 MC, no qual a Corte referendou, cautelarmente, a constitucionalidade de previsão regulamentar de publicidade dos processos disciplinares abertos pelo CNJ contra magistrados: [...] 10. Sendo assim, a ordem constitucional brasileira não adota o sigilo como regra sequer em processos

¹⁷ Em: < <https://www.gov.br/cgu/pt-br/governo-aberto/a-ogp> >. Acesso em: 21/07/2026.

¹⁸ Vide a tese estabelecida na ADPF 872: “O ato de qualquer dos poderes públicos restritivo de publicidade deve ser motivado objetiva, específica e formalmente, sendo nulos os atos públicos que imponham, genericamente e sem fundamentação válida e específica, impeditivo do direito fundamental à informação.”.

administrativos disciplinares ou em processos judiciais criminais, nos quais a tensão com o princípio da presunção de inocência é bem mais aguda. [...]”.

Proposta de redação:

Reformular para: “A restrição de documentos preparatórios exige, cumulativamente: (i) a indicação do ato ou decisão específica em elaboração a que o documento se vincula; (ii) a demonstração motivada do prejuízo concreto que a divulgação antecipada causaria ao processo decisório; e (iii) a reavaliação periódica da restrição, que não se prorroga pela mera pendência do ato. Editado o ato final, ou arquivado o processo, o acesso deve ser garantido.”

5.9.1. Informações sobre processos administrativos disciplinares

Documentos dos processos administrativos disciplinares (PADs): antes da conclusão do processo ficam restritos, evitando prejuízo e garantindo a eficácia da apuração.

Embora apenas ilustre, sem fazer menção expressa, o entendimento fixado no Enunciado CGU 14/2016¹⁹, o Guia orienta como absoluta uma regra inexistente na LAI. Evidentemente, algumas informações, de forma fundamentada, podem ter seu acesso restrito no âmbito de um processo disciplinar não concluído (tais como a portaria instauradora, as oitivas, os despachos, decisões, etc). Entretanto, há ressalvas a este entendimento: **a)** há informações que circunscrevem o PAD, mas que não afetam sua tramitação (tais como o número do processo administrativo, a autoridade administrativa responsável por sua instauração, a autoridade ou órgão competente por seu julgamento, etc)²⁰; **b)** há precedentes de aplicação da proibição absoluta de restrição no caso de

¹⁹ Literalmente: “RESTRIÇÃO DE ACESSO DOS PROCEDIMENTOS DISCIPLINARES “Os procedimentos disciplinares têm acesso restrito para terceiros até o julgamento, nos termos do art. 7º, parágrafo 3º, da Lei nº 12.527/2011, regulamentado pelo art. 20, caput, do Decreto nº 7.724/2012, sem prejuízo das demais hipóteses legais sobre informações sigilosas.”. Em: < <https://basedeconhecimento.cgu.gov.br/handle/1/2476> >. Acesso em: 21/07/2026.

²⁰ Nesse sentido, importa citar o texto da Súmula 08/2018 da CMRI/RS : “**8** – Em se tratando de pedido de acesso a informações que estejam a integrar alguma espécie de procedimento administrativo disciplinar ainda não concluído, há de se diferenciar as informações sobre o processo em si (p.ex., a portaria instauradora, as oitivas, os despachos e decisões, etc.) das eventuais informações que apenas circunstancialmente o instruem, as quais não necessariamente estão acobertadas por algum sigilo, a não ser que se enquadrem, por si só, em alguma das hipóteses de que trata o art. 10, incisos I a III, do Decreto nº 49.111/2012.”. Em: < <https://ouvidoriageral.rs.gov.br/upload/arquivos/201805/14091658-sumulas-cmri-rs.pdf> >. Acesso em: 21/06/2026.

informações que tratem sobre condutas violadoras de direitos humanos. Além disso, a orientação viola precedentes vinculantes do STF, conforme já ilustrado no item anterior. A própria ANPD, que assina o Guia como coautora, ao decidir sobre o acesso a seus próprios processos sancionadores, já adota um modelo de divulgação parcial obrigatória e rejeita, na prática de sua própria Coordenação-Geral de Fiscalização, o modelo de vedação categórica que o Capítulo 5 do Guia propõe para os PADs sobre assédio e discriminação. Nesse sentido, o item 3.9 da Nota Técnica nº 22/2024/FIS/CGF/ANPD²¹:

“[...] considerando os ditames da LAI, as orientações da CGU e o interesse público sobre procedimentos fiscalizatórios e sancionatórios, a restrição de acesso a informações contidas em documentos produzidos ou custodiados pela Coordenação-Geral de Fiscalização deve ocorrer de maneira pontual apenas sobre informações que efetivamente sejam protegidas nos termos da Lei de Acesso à Informação.”

Proposta de redação:

Reformular o texto para: “O acesso a informações sobre processos administrativos em curso não é vedado automaticamente pela legislação, sendo necessário que o órgão avalie, fundamentadamente: **a)** os eventuais riscos que o acesso a cada documento antes do término do processo possa acarretar ao resultado do próprio processo; ou **b)** os riscos que o acesso a cada documento possa acarretar a informações protegidas pela legislação vigente”.

5.9.2 A vedação categórica de acesso a PADs sobre assédio e discriminação

Tabela do Capítulo 5: “PAD sobre assédio moral, sexual ou sobre discriminação: Não devem ser divulgados”, ao fundamento de evitar “condenação social, revitimização, retaliação das testemunhas e exposição indevida de servidor que não foi sancionado”.

Este ponto é grave por três razões cumulativas. **Primeiro, a contradição interna.** O próprio guia afirma que o PAD concluído é, em regra, público; recomenda, como boa prática, a preparação de “versão pública do PAD”; e arrola, entre as técnicas menos invasivas, justamente “certidões de processos administrativos disciplinares sobre assédio sexual ou moral com as principais informações”. A tabela, contudo, veda tudo, em regra

²¹

Em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/sei_012_5695_nota_tecnica_22.pdf/@@display-file/file > Acesso em: 22/06/2026.

fechada, sem distinção de fase, de resultado ou de técnica de divulgação parcial. **Segundo, a contradição com a lei.** O art. 29, § 2º, IX, da Lei nº 14.129/2021 impõe a divulgação, em transparência ativa, das sanções administrativas aplicadas a servidores públicos, sem exceção de categorias de infração. Um guia orientativo não pode subtrair do regime legal de publicidade exatamente uma classe de sanções. **Terceiro, e decisivo:** a justificativa declarada é a proteção de vítimas e testemunhas, mas o efeito da regra categórica é o anonimato do agressor sancionado. Proteção de vítima não se confunde com blindagem de infrator, e a técnica para dissociá-las já consta do repertório do próprio guia: tarjamento das identidades de vítimas, testemunhas, denunciante e servidores não sancionados, com publicidade do nome do sancionado, da descrição objetiva da infração e da sanção aplicada. Nesse sentido, o art. 17-A e parágrafo único da Lei nº 11.340/2006 (Lei Maria da Penha):

Art. 17-A. O nome da ofendida ficará sob sigilo nos processos em que se apuram crimes praticados no contexto de violência doméstica e familiar contra a mulher.

Parágrafo único. **O sigilo referido no caput deste artigo não abrange o nome do autor do fato, tampouco os demais dados do processo.** (grifou-se)

A regra, como redigida, produz consequência sistêmica perversa: institucionaliza a opacidade precisamente na categoria de ilícito funcional em que o controle social da responsabilização é mais sensível e em que a assimetria de poder entre infrator e vítima é mais acentuada: o assédio praticado por superiores hierárquicos²². O sigilo integral do processo concluído desprotege as vítimas que desejam que a resposta institucional seja conhecida, desinforma a sociedade sobre a efetividade dos mecanismos de responsabilização e cria incentivo à reincidência protegida, permitindo que agentes sancionados circulem entre unidades e órgãos sem que o histórico disciplinar seja socialmente verificável. O argumento da “condenação social” do sancionado inverte a lógica do regime republicano: a sanção disciplinar transitada é ato de poder estatal, e sua publicidade é garantia para a sociedade, não pena acessória evitável.

Proposta de redação:

Substituir a linha da tabela por: **“PAD sobre assédio moral, sexual ou discriminação (concluído): Divulgação parcial obrigatória.** Devem ser protegidos, mediante tarjamento, certidão ou versão pública, todos os dados que

²² Nesse sentido, estudos indicam que, no Brasil, mulheres tendem a utilizar menos os canais de denúncia por conta da maior percepção de possibilidade de represálias. Em: Tavares, G.M., Lima, F.V. and Michener, G. (2024), To blow the whistle in Brazil: The impact of gender and public service motivation. Regulation & Governance, 18: 226-244. <https://doi.org/10.1111/rego.12418>. Acesso em: 22/07/2026.

permitam identificar, direta ou indiretamente, vítimas, testemunhas, denunciante e servidores que não tenham sido sancionados. Permanecem públicos o nome do servidor sancionado, seu cargo, a descrição objetiva da infração e a sanção aplicada, nos termos do art. 29, § 2º, IX, da Lei nº 14.129/2021 e art. 17-A, parágrafo único da Lei nº 11.340/2006. A proteção de vítimas e testemunhas não autoriza o anonimato do agente sancionado.”

5.10 Registros de entrada em residências oficiais: o critério deve ser a natureza do encontro, não o local

“Enunciado CGU nº 2/2023 - Registros de entrada e saída de residências oficiais.

Os registros de entrada e saída de pessoas em residências oficiais do Presidente e do Vice-presidente da República são informações que devem ser protegidas por revelarem aspectos da intimidade e vida privada das autoridades públicas e de seus familiares, salvo se tais registros disserem respeito a agendas oficiais, as quais têm como regra a publicidade, ou se referirem a agentes privados que estejam representando interesses junto à Administração Pública”. (p. 36)

O Enunciado CGU nº 2/2023, incorporado à minuta, parte da proteção como regra para os registros de entrada e saída de residências oficiais, ressaltando as agendas oficiais e os agentes privados que representem interesses junto à Administração. A presunção está invertida. **O critério constitucionalmente adequado é a natureza do encontro:** reunião de caráter público ou institucional não se converte em ato da vida privada pela escolha do endereço em que se realiza. **A presunção de privacidade, tal como formulada, cria incentivo conhecido (deslocar para a residência oficial os encontros que não se deseja ver registrados no gabinete),** e a experiência recente da Administração Federal demonstra a relevância desses registros para o controle social e para a apuração de irregularidades²³.

Proposta de redação:

²³ Cite-se, por exemplo: < <https://www1.folha.uol.com.br/poder/2017/06/1889182-apos-controversia-temer-registra-em-agenda-ate-reuniao-de-2-minutos.shtml> >. Acesso em: 22/06/2026

Reformular a orientação para: “Nos registros de entrada e saída de residências oficiais, presume-se pública a informação relativa a encontros de natureza institucional, oficial ou de representação de interesses, independentemente do local em que realizados; presume-se protegida apenas a informação relativa a visitas de natureza estritamente pessoal ou familiar. A qualificação da natureza do encontro deve ser registrada pelo órgão e é passível de controle.”

5.11 A hipótese de defesa dos direitos humanos: o exame de motivação pela porta dos fundos

Ao tratar da hipótese de defesa dos direitos humanos (art. 31, § 3º, IV, da LAI, e art. 60, IV, do Decreto nº 7.724/2012), a minuta orienta "avaliar se a informação é necessária para defesa do direito humano ameaçado ou violado, considerando a necessidade indicada na demanda", e "considerar que a entrega da informação deve ser feita ao solicitante que possa atuar na defesa pretendida".

Embora compatível com a literalidade do art. 60, IV, do Decreto nº 7.724/2012 (cujo texto, por si só, extrapola a disposição da LAI), a redação induz o agente a indagar o motivo do pedido, o que é vedado pelo art. 10, § 3º, da LAI e constitui o mesmo vício identificado na Seção 5.3 desta contribuição quanto à distinção entre interesse coletivo e curiosidade geral. **A exigência de que o solicitante "possa atuar na defesa pretendida" restringe indevidamente o alcance da transparência:** nada impede que uma pessoa sem vínculo direto com a causa obtenha a informação e a repasse a quem efetivamente atua na defesa do direito ameaçado, ou que a disponibilização ao público mais amplo produza, por si, efeito protetivo. Além disso, levando novamente em conta o delicado ecossistema de proteção de direitos humanos no Brasil²⁴, o Guia dá subsídios adicionais para conferir “verniz de legitimidade” a decisões administrativas arbitrárias que, na prática, buscam justamente escudar violações de direitos humanos de serem objeto de escrutínio.

Proposta de redação:

"A decisão sobre o fornecimento de informação com fundamento na defesa de direitos humanos deve avaliar a correlação objetiva entre a informação solicitada e a proteção

²⁴ De acordo com o Relatório “Na Linha de Frente”, entre 2023 a 2024 mais de 486 casos de violência contra defensores de direitos humanos foram registrados, incluindo 55 homicídios. Em: < <https://comiteddh.org.br/wp-content/uploads/2017/10/Resumo-executivo-dossi%C3%AAA-portugu%C3%AAs.pdf> >. Acesso em: 21/07/2026.

ou defesa do direito humano em questão, e não os motivos ou a intenção declarada pelo requerente. A solicitação não precisa indicar por que a informação é necessária, bastando a demonstração, pelo órgão, de como a divulgação contribui para a defesa do direito humano ameaçado ou violado. É dispensável que o requerente atue diretamente na defesa do direito humano em causa, sendo suficiente a aptidão da informação para essa finalidade, inclusive por reuso posterior por terceiros."

5.12 Dado tornado manifestamente público pelo titular: hipótese ausente no texto do Guia

O Guia não contempla, em nenhuma de suas hipóteses de divulgação ou mesmo como critério para avaliação, o caso em que o próprio titular tornou a informação manifestamente pública, a despeito do anunciado propósito do documento de harmonizar a aplicação da LAI e LGPD . A LGPD prevê essa hipótese de forma autônoma no art. 7º, § 4º, diversas entidades já defenderam sua aplicação no contexto do acesso à informação e a própria CGU reconhece a aplicabilidade do fundamento em seus precedentes²⁵.

A ausência é uma lacuna real: hoje, um agente público que divulgou voluntariamente um dado (por exemplo, em rede social ou currículo público) pode ter esse mesmo dado tratado como protegido pelo Guia, exigindo todo o Teste de Interesse Público para uma informação que o titular já expôs por conta própria.

Proposta de redação:

Incluir, entre as hipóteses que autorizam a divulgação de dados pessoais, a seguinte: existindo evidências de que o dado tenha sido tornado manifestamente público pelo titular, nos termos do art. 7º, § 4º, da Lei nº 13.709/2018, é dispensada, nessa hipótese, a aplicação do Teste de Interesse Público, sem prejuízo da avaliação sobre eventual descontextualização ou uso indevido da informação.

²⁵ Por exemplo, o PARECER Nº 397/2023/CGRAI/DRAI/SNAI/CGU e PARECER Nº 189/2023/CGRAI/DRAI/SNAI/CGU, acerca inclusive da divulgação de informações pessoais sensíveis, referentes à saúde do agente público.

6. Conclusão

A minuta submetida à consulta pública parte de fundamentos corretos e contém salvaguardas relevantes, mas sua arquitetura conceitual e operacional, tal como redigida, tende a produzir efeito contrário ao declarado. Em vez de oferecer segurança para a aplicação conjunta da LAI e da LGPD, o documento fornece aos órgãos públicos um repertório de fórmulas abertas, critérios subjetivos e atalhos classificatórios capazes de sustentar negativas indevidas com aparência de conformidade técnica.

Os problemas identificados nesta contribuição não são isolados. **Em conjunto, eles promovem um deslocamento silencioso do centro de gravidade do regime da LAI, afastando a publicidade como posição jurídica de partida e ampliando a discricionariedade dos agentes responsáveis pela decisão.** Deslocamento este que nenhuma das duas autoridades signatárias declara pretender, mas que a aplicação capilar do documento consumará.

Por essa razão, as alterações específicas apresentadas na Seção 5 e as propostas de redação distribuídas ao longo desta contribuição, embora necessárias, **não são suficientes.** A correção de exemplos, tabelas ou trechos isolados não resolverá os problemas produzidos pela organização geral do documento, por suas premissas conceituais e pelo encadeamento do roteiro decisório. Os pontos estruturais desenvolvidos nas seções anteriores precisam **orientar uma reformulação transversal do Guia**, com impacto sobre sua introdução, seus conceitos, sua metodologia, seus exemplos, suas tabelas e seus entendimentos temáticos.

A versão final deve partir de uma nova arquitetura, que:

1. reafirme a publicidade como regra e atribua ao Estado o ônus de justificar qualquer restrição;
2. sistematize, antes da análise casuística, as normas, os precedentes e os entendimentos que já definem a publicidade de determinadas informações;
3. delimite com precisão o papel da LAI e o papel complementar da LGPD, sem combinar seletivamente os elementos mais restritivos de cada regime;
4. reformule o roteiro decisório para priorizar o acesso em relação à restrição e limitar a discricionariedade do agente estatal;
5. revise os exemplos e entendimentos específicos à luz dessas premissas, e não como ajustes autônomos ou desconectados.

As correções propostas não enfraquecem a proteção de dados pessoais. Ao contrário, tornam essa proteção mais precisa, proporcional e juridicamente defensável, direcionando-a a situações em que existe risco efetivo aos titulares, especialmente pessoas em condição de vulnerabilidade, vítimas, testemunhas e denunciante. Ao mesmo tempo, impedem que a proteção de dados seja apropriada indevidamente por agentes sancionados, estruturas administrativas resistentes ao escrutínio ou órgãos que prefiram a comodidade da negativa ao trabalho da divulgação responsável. Transparência e proteção de dados não são adversárias. A opacidade seletiva prejudica ambas.

Requer-se, portanto, que a CGU e a ANPD não se limitem a responder às propostas pontuais de alteração do texto, mas enfrentem expressamente todos os problemas conceituais, jurídicos, metodológicos e institucionais apresentados nesta contribuição. **A resposta à consulta deve indicar, de forma individualizada e fundamentada, o acolhimento ou a rejeição de cada ponto, inclusive daqueles que demandam a reformulação da arquitetura geral do Guia.**

Também se requer que a versão final demonstre como as questões estruturais foram incorporadas ao conjunto do documento, evitando que sejam tratadas apenas por ajustes localizados na Seção 5, em exemplos específicos ou em redações isoladas. Sem essa revisão transversal, permanecerá o risco de que correções pontuais convivam com uma lógica geral ainda orientada para a restrição.

As entidades e especialistas signatários permanecem à disposição para o diálogo técnico e para contribuir com a construção de uma nova versão. Essa disponibilidade, contudo, não dispensa o registro formal e fundamentado do tratamento conferido a cada contribuição, condição indispensável para a transparência, a integridade e a efetividade do processo de participação social.

Brasília, 24 de julho de 2026.

1. Pessoas jurídicas signatárias

- 1.1. Associação Fiquem Sabendo
- 1.2. ABCPública
- 1.3. Aláfia Lab
- 1.4. Artigo 19

- 1.5. Associação Brasileira de Jornalistas Investigativos (ABRAJI)
- 1.6. Associação Matinal de Jornalismo e Cultura
- 1.7. Agência Livre.jor
- 1.8. Agência Tatu
- 1.9. Amazônia Real
- 1.10. Base dos Dados
- 1.11. Centro de Liderança Pública (CLP)
- 1.12. Honório - Grupo de Pesquisas em Políticas Públicas Arquivísticas
- 1.13. Instituto Fogo Cruzado
- 1.14. Instituto de Direito Coletivo (IDC)
- 1.15. Instituto de Estudos Socioeconômicos (INESC)
- 1.16. Instituto Mais Progresso.Org
- 1.17. Instituto Não Aceito Corrupção (INAC)
- 1.18. Instituto Novos Paradigmas
- 1.19. Instituto Operação Política Supervisionada (OPS)
- 1.20. Instituto Questão de Ciência (IQC)
- 1.21. Instituto República.Org
- 1.22. Inteligov
- 1.23. Grupo de Pesquisa e Intervenção em Direitos Humanos Mapinguari da Universidade Federal de Rondônia
- 1.24. Grupo de Pesquisa Jornalismo, Direito e Liberdade (JDL)
- 1.25. Grupo de Pesquisa Politeia
- 1.26. Movimento do Ministério Público Democrático (MPD)
- 1.27. Observatório da Ética Jornalística (objETHOS)
- 1.28. Observatório do Marajó
- 1.29. Observatório Social de Mato Grosso
- 1.30. Open Knowledge Brasil
- 1.31. Plataforma JUSTA
- 1.32. Sigalei
- 1.33. Sindicato dos Jornalistas Profissionais de Santa Catarina
- 1.34. Sindicato dos Jornalistas de Mato Grosso (Sindjor/MT)
- 1.35. Transparência Brasil
- 1.36. Transparência Eleitoral
- 1.37. Transparência Internacional - Brasil

2. Pessoas físicas signatárias

- 2.1. André Rosa de Oliveira, Professor dos cursos de Comunicação da Universidade São Judas Tadeu (São Paulo - SP)
- 2.2. André Luiz de Carvalho Matheus, advogado, mestre em direito pela UERJ
- 2.3. Andréa Sales, Professora da Faculdade de Ciências Humanas do Cabo de Santo Agostinho

- 2.4. Adriano Belisário, Jornalista e Pesquisador da UFRJ
- 2.5. Antonio Roque Citadini, ex-presidente do TCE/SP
- 2.6. Beatriz Rey, Cientista Política e Pesquisadora na Universidade de Lisboa
- 2.7. Bianca da Costa Maia Lopes, doutora em Ciência da Informação e professora da UFF
- 2.8. Cassuça Benevides, Produtora Executiva da Quartzô Comunicação
- 2.9. Cecília Nunes do Lago Oliveira, jornalista
- 2.10. Cristião Fernando Rosas, médico, Doctors for Choice/Brasil
- 2.11. Daniel Ferreira, Doutorando em História na Universidade de Chicago
- 2.12. Diego Werneck Arguelhes Professor Associado, Insper
- 2.13. Eloísa Machado, professora FGV Direito SP
- 2.14. Fabiano Angélico, Pesquisador e professor na Universidade de Lugano, na Suíça, Doutor em Administração Pública, com dupla titulação, Brasil e Suíça
- 2.15. Fábio Bispo, repórter em Sumaúma
- 2.16. Felipe Rodrigues Grandin, diretor da Agência Eixos
- 2.17. Fernando Augusto Martins Canhadas - Doutor em Direito do Estado - PUC/SP
- 2.18. Gabriel Leite Carvalho, advogado, Advocacia Ruy de Mello Miller
- 2.19. Giovane Caruso, jornalista
- 2.20. Haydée Svab, ativista pela transparência e acesso a informações públicas
- 2.21. Helton Lucinda Ribeiro, jornalista e pesquisador
- 2.22. Henrique Schiavo, co-fundador do Iluminando
- 2.23. Ivonei Souza Trindade, advogado brasileiro e professor de Direito Internacional na Ágora Universidad Hispanoamericana (México)
- 2.24. Jamile Santana, ativista pela transparência e acesso a informações públicas
- 2.25. Joice Melo Vieira, professora do Departamento de Demografia, Universidade Estadual de Campinas (Unicamp)
- 2.26. Katia Brembatti, jornalista, professora universitária, pesquisadora na área de transparência e acesso à informação, ex-presidente da ABRAJI e mestre em Comunicação Digital e Cultura de Dados pela FGV
- 2.27. Laila Bellix, Especialista em governo aberto e participação
- 2.28. Laís Martins, repórter Intercept Brasil
- 2.29. Laura Mendes Amando de Barros, procuradora do município de São Paulo, doutora em direito e professora do Insper
- 2.30. Lucas Maia, repórter e jornalista
- 2.31. Lucas Marchesini, repórter Folha de São Paulo
- 2.32. Luciana Menezes Carvalho (UFSM)
- 2.33. Luiz Felipe Monteiro Seixas, Professor da Universidade Federal de Pernambuco
- 2.34. Marcelo Crispim da Fontoura, professor de jornalismo
- 2.35. Marcelo Issa, Cientista político e advogado
- 2.36. Marcus Vinicius Brasil, bacharel em Economia

- 2.37. Maria Paula Almada, Diretora do Aláfia Lab e pesquisadora associada do INCT.DD
- 2.38. Marcelo Träsel, jornalista e professor na Faculdade de Biblioteconomia e Comunicação e no Programa de Pós-Graduação em Comunicação da Universidade Federal do Rio Grande do Sul. Ex-presidente da ABRAJI (2020-2021)
- 2.39. Marcelo Soares, diretor da Lagom Data
- 2.40. Marcio Leal Gonçalves, Diretor Financeiro, Instituto Tijuípe
- 2.41. Marcio Roberto de Oliveira Júnior, Contabilista, Especialista em Finanças
- 2.42. Margareth Arilha, pesquisadora do Núcleo de Estudos de População "Elza Berquó" (NEPO), Universidade Estadual de Campinas (Unicamp)
- 2.43. Marina Iemini Atoji, jornalista, especialista em transparência pública e controle social
- 2.44. Naira Hofmeister, jornalista investigativa
- 2.45. Nilzete Ferreira Gomes, discente de doutorado em Ciencia da Informação e bibliotecária
- 2.46. Ricardo Dahis, Senior Lecturer, Monash University
- 2.47. Rogério Florentino Pereira, advogado, vice-presidente do Sindijor/MT
- 2.48. Sandra Bitencourt (UFRGS/Obcomp)
- 2.49. Sérgio Praça, Cientista Político
- 2.50. Sílvia Lisboa, Editora investigativa do Matinal
- 2.51. Taís Seibt, professora Unisinos, doutora em Comunicação
- 2.52. Thiago Araújo, jornalista independente
- 2.53. Tiago Farina Matos, advogado sanitaria
- 2.54. Thiago Pinheiro Lima, procurador do Ministério Público de Contas de São Paulo
- 2.55. Vinicius Souza Sueiro, Designer de Informação
- 2.56. Yasodara Cordova, especialista e acadêmica



Guia CGU ANPD

De Bruna Armonas Colombo <bruna.colombo@anpd.gov.br>

Data Qui, 16/07/2026 16:30

Para Cibelle Cesar do Amaral Brasil <cibelle.brasil@cgu.gov.br>

Cc camila.alves@cgu.gov.br <camila.alves@cgu.gov.br>; tamara.bakuzis@cgu.gov.br <tamara.bakuzis@cgu.gov.br>

Cco Caroline Nazare dos Santos Chucre Kappel <caroline.kappel@anpd.gov.br>; Cristiane Miranda Araujo <cristiane.araujo@anpd.gov.br>

 1 anexo (179 KB)

ANPD - Oficio1_2026__Assip_Manifestacao_a_consulta_pub.pdf;

Olá Cibelle e demais em cópia,

Encaminho (anexa) a contribuição do Tribunal de Contas da União, protocolizada individualmente junto a ANPD, em razão da consulta pública ao "Guia de Transparência e Proteção de Dados."

Destacamos os itens abaixo por entendermos que a temática é de competência da CGU.

1) **2. Item do Guia: 4.2, tabela da página 22:** Complemento do rol exemplificativo de Interesse Público Preponderante com hipótese de Prevenção e Identificação de Conflitos de Interesses e Nepotismo (tabela pág. 22); e

2) **3. Item do Guia: Dados pessoais em processos administrativos disciplinares:**

- Concluídos (Guia dispõe "em tese")
- Em tramitação (para compartilhamento de informações e provas entre órgãos públicos)
- Casos de assédio moral, assédio sexual ou discriminação (sigilo seria para proteção ao denunciante/ fundamento da revitimização e proteção de testemunhas seria suficiente para afastar o controle social?)
- Divulgação da descrição da infração (íntegra ou extrato?)

Atenciosamente,



Bruna Armonas
Coordenadora de Regulação Setorial - CORS

Coordenação-Geral de Governança e Regulação Setorial - CGRS
Superintendência de Regulação - SRE
Agência Nacional de Proteção de Dados - ANPD

Ofício nº 01/2026 – Assip

Brasília, 23 de junho de 2026.

Assunto: Contribuição Técnica ao Guia de Transparência e Proteção de Dados Pessoais -
CGU/ANPD

À Autoridade Nacional de Proteção de Dados Pessoais

À Controladoria-Geral da União

1. Primeiramente gostaria de congratular a ANPD e a CGU pela divulgação do Guia de Transparência e Proteção de Dados Pessoais disponibilizado para consulta pública. Como Encarregada de Dados do Tribunal de Contas da União trago contribuições técnicas para o documento, em complemento àquelas levadas à Plataforma Brasil Participativo por este Tribunal, juntamente com outros onze Tribunais de Contas do Brasil. As contribuições são propostas em conjunto com a corregedoria e a área administra do TCU.

2. Solicito a consideração quanto à avaliação das contribuições aqui trazidas, a despeito da sua intempestividade. O período de 10 dias para as manifestações na audiência pública e a data final coincidente com dia não útil (domingo) dificultaram a coleta de contribuições junto às unidades do Tribunal.

3. Permanecemos à disposição para quaisquer esclarecimentos.

(assinado eletronicamente)

MÔNICA COTRIM CHAVES

Assessoria de Segurança da Informação e Proteção de Dados Pessoais

Proposta de Contribuição

1. Item do Guia: 3.3, alínea "e" (Cumprimento de ordem Judicial).

Texto Sugerido: a ser incluído como último parágrafo do item: "O fornecimento de dados pessoais a órgãos e unidades de auditoria, correição e controle (interno e externo) constitui tratamento de dados necessário para o cumprimento de obrigação legal ou regulatória, conforme o art. 7º, II, da LGPD."

Justificativa: O Guia esclarece que pedidos de órgãos de controle não são "ordens judiciais", mas não explicita qual é a base legal correta para esse atendimento. A inclusão proposta evita que a proteção de dados seja erroneamente utilizada como barreira ao exercício das competências institucionais de controle e auditoria.

2. Item do Guia: 4.2, tabela da página 22

Texto sugerido: inserção do item **em amarelo** abaixo

Interesse público	Exemplos de benefícios concretos à coletividade
Garantir o uso adequado do dinheiro público	• Verificar a compatibilidade dos valores gastos com preços de mercado • Prevenir sobrepreço e desperdício de recursos públicos
Fiscalizar a conduta dos agentes públicos	• Monitorar se um servidor está usando bens públicos, como veículos ou materiais, para fins pessoais ou se um gestor está tomando decisões enviesadas • Investigar se o patrimônio de um agente público cresceu de forma incompatível com a sua renda • Reforçar a moralidade administrativa
Prevenção e identificação de conflitos de interesses e nepotismo	• Identificar vínculos de parentesco ou afinidade que possam comprometer a impessoalidade e a moralidade administrativa em nomeações e contratações • Monitorar a atuação institucional e agendas de agentes públicos em cargos decisórios para prevenir o tráfico de influência e garantir a integridade do processo decisório
Combater a corrupção e ilícitos administrativos	• Identificar fraudes em licitações e contratos • Proteger o erário e inibir práticas ilícitas
Assegurar a integridade dos processos administrativos	• Verificar o cumprimento das regras em concursos e contratações • Garantir a legalidade e a isonomia em processos administrativos • Evitar favorecimento indevido

Interesse público	Exemplos de benefícios concretos à coletividade
Promover o controle social de políticas e serviços públicos	• Avaliar critérios de seleção de beneficiário de políticas públicas • Averiguar qualidade dos serviços públicos • Garantir adequação e conformidade das políticas e serviços • Aperfeiçoar políticas públicas específicas

Justificativa: a inclusão do item acima é um complemento ao rol exemplificativo de benefícios à coletividade e funciona como um instrumento de controle social e integridade, permitindo verificar se a conduta do agente público está pautada pelo interesse coletivo.

3. Item do Guia: Dados pessoais em processos administrativos disciplinares

3.1. PAD concluído: substituir “em tese” por “em regra”

A publicidade do PAD concluído é a regra jurídica que decorre diretamente do art. 37, caput, da CF/88 (princípio da publicidade) e do art. 5º, XXXIII, da CF/88 (direito de acesso à informação). O sigilo é a exceção. A locução “em tese” enfraquece a regra constitucional de publicidade e pode induzir à interpretação equivocada de que a divulgação seria apenas uma possibilidade abstrata.

Sugestão: Substituir a expressão “em tese” por “em regra”, deixando claro que a publicidade do PAD concluído constitui a regra jurídica aplicável, ressalvadas apenas as hipóteses de sigilo legal e proteção de dados pessoais.

3.2. Ausência de ressalva em relação ao compartilhamento de informações e provas do PAD em curso entre órgãos públicos

O sigilo do PAD em curso não impede o compartilhamento de informações e provas com autoridades competentes. A restrição prevista no art. 7º, § 3º, da LAI e no art. 150 da Lei nº 8.112/90 buscam preservar a investigação perante terceiros sem competência funcional sobre a matéria, não impedir a atuação coordenada de órgãos com competência legal sobre os mesmos fatos.

Sugestão - incluir o parágrafo: “O caráter restrito do PAD em curso não impede o compartilhamento de informações, provas e documentos com autoridades e órgãos públicos que detenham competência investigativa, disciplinar, fiscalizatória ou de controle sobre os mesmos fatos ou agentes envolvidos.

O compartilhamento deverá ser formalmente motivado e condicionado à manutenção do sigilo pelo órgão destinatário.”

3.3. PAD sobre assédio moral, assédio sexual ou discriminação: tratamento diferenciado injustificado

O Guia cria tratamento diferenciado sem fundamento legal expresso e reduz a transparência em casos de elevado interesse público, adotando como critério a natureza da prova utilizada durante a instrução (“majoritariamente testemunhal”).

Tal critério, no entanto, é assistemático, pois inúmeras infrações disciplinares são apuradas majoritária ou exclusivamente por prova testemunhal (insubordinação, conduta escandalosa, infração ao dever de urbanidade, entre outras), sem que o Guia reserve a qualquer delas tratamento restritivo equivalente. Aplicar o critério seletivamente, apenas ao assédio e à discriminação, que sequer encontram descrição autônoma na Lei nº 8.112/90, cria uma categoria privilegiada de sigilo, sem respaldo no ordenamento, violando o princípio da legalidade, da isonomia e da impessoalidade.

A LAI não veicula restrição de acesso com base na natureza do meio de prova utilizado na instrução. O art. 7º, § 3º, da LAI e o art. 150 da Lei 8.112/90 autorizam a restrição temporária durante a apuração, para preservar sua eficácia. Esse fundamento se exaure com a conclusão do processo, independentemente de como a prova foi produzida. Criar restrição permanente pós-julgamento com base em critério probatório é inovar contra legem.

O assédio moral, sexual e a discriminação praticados no ambiente do serviço público são desvios de conduta funcionais, cujas vítimas frequentemente são também servidores públicos ou colaboradores da instituição. O interesse coletivo no conhecimento da responsabilização de agentes públicos pelo cometimento dessas condutas é tão legítimo quanto em relação às demais infrações disciplinares, dado o impacto direto sobre o ambiente institucional e sobre a confiança da sociedade nas instituições.

A supressão desse controle social em nome da proteção da vítima é tanto ilegal, quanto desproporcional, porque o mesmo resultado protetivo pode ser alcançado por meio menos restritivo, como, por exemplo, a anonimização dos dados identificadores da vítima e das testemunhas na versão pública do PAD, após o julgamento. Em qualquer caso de oposição de sigilo (fiscal, bancário, saúde, dados sensíveis et) a proteção se dá em relação à informação ou peça processual específica e não ao processo que as contém.

Sugestão - Substituir a linha de tratamento diferenciado por orientação nos seguintes termos: “O PAD que apure assédio moral, assédio sexual ou discriminação, uma vez concluído, submete-se à regra geral de publicidade aplicável aos processos administrativos disciplinares.

A proteção das vítimas e testemunhas deve ser assegurada mediante anonimização dos dados identificadores constantes da versão pública do processo, observados os princípios da necessidade e da proporcionalidade.

A identidade do servidor sancionado, a descrição da conduta e a sanção aplicada devem ser divulgadas, por se referirem ao exercício da função pública e atenderem ao interesse coletivo no controle social da atividade disciplinar.”

3.4. Divulgação da descrição da infração

A descrição dos fatos é o elemento central para o controle da legalidade, da proporcionalidade da sanção e da regularidade do processo disciplinar.

A orientação de que a descrição deve ser objetiva e observar os “*princípios da finalidade, necessidade e proporcionalidade*” pode ser interpretada como autorização para resumir, modular ou omitir elementos relevantes da infração.

Sem a descrição integral dos fatos, torna-se impossível verificar: a) A correta subsunção da conduta às infrações disciplinares; b) a proporcionalidade da penalidade aplicada e; c) a congruência entre acusação e julgamento.

Qualquer redução ou modulação da descrição da infração na versão pública do PAD subtrai do controle social os elementos indispensáveis a esse juízo.

Sugestão - A descrição da infração constante de PAD concluído deve ser divulgada integralmente, por constituir elemento essencial ao controle de legalidade, de proporcionalidade da penalidade aplicada e de adequação da subsunção dos fatos às normas disciplinares pertinentes.

1. Item 2.1: Princípio da Responsabilização e Prestação de Contas (*Accountability*)

Problema: O Guia define o princípio de forma genérica ("demonstrar a adoção de medidas eficazes"). Para que a fiscalização ocorra, é necessário exigir registros técnicos que permitam a auditoria externa.

Sugestão de Nova Redação (em favor da fiscalização):

"O órgão público deve demonstrar a conformidade com a LGPD por meio da manutenção de um inventário de dados pessoais atualizado e da elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) sempre que o tratamento para fins de transparência puder gerar riscos às liberdades civis. Todas as operações de tratamento devem gerar trilhas de auditoria (logs) inalteráveis, permitindo que a ANPD e os órgãos de controle interno verifiquem a integridade do processo, conforme o Art. 37 da LGPD e o Art. 47 da Lei nº 14.129/2021."

2. Item 2.1: Inclusão do Princípio da Proteção Prioritária (Novo Subitem)

Problema: O capítulo define dados pessoais e sensíveis, mas não estabelece a proteção de crianças e adolescentes como um pilar central, ignorando o recente ECA Digital.

Sugestão de Inclusão de Nova Redação:

"Proteção de Crianças e Adolescentes: O tratamento de dados de menores de idade no âmbito da transparência deve observar o melhor interesse do menor (Art. 14 da LGPD) e garantir, por padrão, o nível mais elevado de proteção e privacidade (*High Level of Protection by Design*), conforme o Art. 7º da Lei nº 15.211/2025. É vedada a utilização desses dados para qualquer forma de perfilamento ou tratamento que não atenda estritamente à finalidade pública informada."

3. Item 2.2: Regime jurídico - Dever de Proporcionalidade

Problema: O texto afirma que o tratamento deve ser "proporcional", mas não vincula isso à obrigatoriedade de adotar a técnica menos invasiva disponível.

Sugestão de Nova Redação:

"O tratamento de dados pela Administração Pública deve ser realizado para o atendimento da finalidade pública, sendo obrigatória a adoção da medida menos invasiva à privacidade para atingir o objetivo pretendido. Sempre que o interesse público puder ser satisfeito por meio de dados anonimizados ou agregados, estes deverão ser priorizados em detrimento do uso de dados identificados, em observância ao princípio da necessidade (Art. 6º, III, LGPD)."

4. Item 2.3: LGPD e LAI - Decisão sobre Divulgação

Problema: O texto menciona que a decisão deve ser "motivada", mas não estabelece que essa motivação deve ser pública para permitir o controle social.

Sugestão de Nova Redação:

"A decisão administrativa que autoriza ou restringe a divulgação de dados pessoais deve ser formalmente motivada e registrada em repositório público, para consulta e fiscalização. A motivação deve explicitar o benefício coletivo esperado e as salvaguardas aplicadas para mitigar riscos ao titular. A ausência de motivação técnica e jurídica torna o ato de imposição de sigilo ou de divulgação nulo, sujeitando o agente às sanções cabíveis, nos termos do Art. 32 da LAI."

5. Item 2.1: Princípio da Transparência no Poder Público

Problema: O Guia menciona o "dever de publicidade", mas não o alinha totalmente ao conceito de Governo como Plataforma.

Sugestão de Nova Redação:

"O princípio da transparência impõe ao Poder Público o dever de disponibilizar, de forma ativa e em linguagem simples, informações claras sobre como, onde e por que os dados dos cidadãos estão sendo tratados. Os sistemas de transparência devem permitir que o titular consulte, via Selo Ouro ou Prata do Gov.br, o histórico de acessos aos seus dados pessoais realizados por terceiros ou outros órgãos, garantindo a autodeterminação informativa prevista no Art. 2º, II da LGPD."

1. Item 3.1: Prazo de Restrição e Transparência de Prazos

Problema: O Guia menciona o prazo de 100 anos como limite máximo. Embora cite o Enunciado CGU nº 1/2024 sobre a presunção de 15 anos, a redação não obriga o órgão a publicar o catálogo de informações protegidas com seus respectivos prazos, o que dificulta o controle social sobre o "estoque" de sigilo.

Sugestão de Nova Redação:

"A restrição de acesso a informações pessoais deve ser motivada por risco concreto, adotando-se a presunção de 15 (quinze) anos na ausência de prazo expresso. Os órgãos deverão manter e publicar anualmente um inventário de informações restritas, especificando o fundamento legal e a data prevista para a abertura, garantindo a auditabilidade do fluxo de transparência passiva, conforme o Art. 30 da LAI."

2. Item 3.2: Acesso pelo titular e Desburocratização

Problema: O texto condiciona o acesso do titular à comprovação de identidade via Gov.br Ouro/Prata ou presencial. No entanto, a Lei do Governo Digital veda exigências que inviabilizem o direito e promove o "autosserviço".

Sugestão de Nova Redação:

"O acesso do titular aos seus próprios dados deve ser garantido preferencialmente por meio de autosserviço em plataforma única. A exigência de comprovação de identidade não deve se tornar uma barreira burocrática indevida. A Administração deve priorizar meios digitais de autenticação que respeitem a presunção de boa-fé do cidadão, eliminando formalidades cujo custo social seja superior ao risco envolvido."

3. Item 3.3 (d): Estatísticas e Pesquisas

Problema: O Guia afirma que a identificação dos titulares pode ser imprescindível em pesquisas. Contudo, não exige um Relatório de Impacto (RIPD) quando dados identificados são compartilhados com órgãos de pesquisa, o que eleva o risco ao titular.

Sugestão de Nova Redação:

"O fornecimento de dados pessoais para fins de pesquisa deve priorizar a anonimização ou pseudonimização. Caso a identificação seja estritamente necessária, o órgão de pesquisa deverá apresentar Relatório de Impacto à Proteção de Dados Pessoais (RIPD), demonstrando as salvaguardas técnicas adotadas. A divulgação dos resultados de qualquer estudo em nenhuma hipótese poderá revelar dados pessoais dos titulares."

4. Item 3.3 (i): Interesse Público e Geral Preponderante

Problema: O Guia cita o Teste de Interesse Público, mas não estabelece que essa decisão de "flexibilizar" a privacidade deve ser registrada de forma que o titular possa contestá-la.

Sugestão de Nova Redação:

"A decisão que reconhece o interesse público preponderante para divulgar dados pessoais deve ser motivada, registrada e comunicada ao titular, sempre que possível, garantindo-lhe o direito de peticionar contra o tratamento indevido. O registro da decisão deve detalhar o benefício coletivo e o risco mitigado, permitindo que a ANPD fiscalize a proporcionalidade da medida."

5. Item 3.4: Responsabilidade e Auditabilidade Digital

Problema: O "Termo de Responsabilidade" para terceiros é citado de forma genérica. É necessário que este termo seja digital e auditável para evitar o uso desviado de dados.

Sugestão de Nova Redação:

"O acesso de terceiros a dados pessoais protegidos exige a assinatura de Termo de Responsabilidade em formato digital nativo, que deve ser incorporado a uma trilha de auditoria inalterável. O sistema deve registrar quem acessou, para qual finalidade legal e por quanto tempo, sob pena de responsabilidade administrativa e penal, assegurando que a fiscalização pelos órgãos de controle seja tempestiva e eficaz."

6. Inclusão Transversal: O Melhor Interesse da Criança (ECA Digital)

Problema: O capítulo 3 detalha as categorias de proteção (intimidade, vida privada, etc.), mas não inclui a Proteção Prioritária como uma categoria autônoma de restrição de acesso na LAI.

Sugestão de Inclusão de Item:

"Proteção de Menores: Independentemente de pedidos de acesso, os dados de crianças e adolescentes em sistemas de governo devem operar com o grau mais elevado de proteção por padrão. A restrição de acesso nominal de menores deve ser a regra, priorizando-se o acesso apenas ao responsável legal devidamente identificado, em observância ao princípio da proteção integral e do melhor interesse do menor."

1. Item 4.1: Roteiro para tomada de decisão (Passo 1 - Identificação)

Problema: O Guia inicia o roteiro verificando se a informação é de terceiros. No entanto, para garantir a ordem e a decência no atendimento digital, deve-se priorizar o canal de autosserviço para o próprio titular, reduzindo a carga de pedidos via LAI.

Sugestão de Nova Redação:

"O primeiro passo do roteiro decisório deve ser a verificação da identidade do solicitante. Caso a informação se refira ao próprio requerente, o acesso deve ser garantido de forma imediata via plataforma única de autosserviço (Selo Ouro/Prata do Gov.br), dispensando o trâmite de pedido de acesso à informação. Somente quando o sistema de autosserviço for inviável ou a informação for de terceiros, o gestor seguirá para as etapas de ponderação, conforme o Art. 14 da Lei nº 14.129/2021."

2. Item 4.2: Avaliação do risco de dano ao titular (Pilar 3 do Teste)

Problema: O Guia propõe uma análise qualitativa de risco (leve, médio, grave). Contudo, ele ignora o risco de reidentificação por cruzamento de bases e a proteção especial exigida para crianças e adolescentes pelo novo ECA Digital (Lei nº 15.211/2025).

Sugestão de Nova Redação:

"A avaliação de risco deve considerar não apenas o dano direto, mas o potencial de reidentificação do titular por meio do cruzamento com outras bases de dados públicas ou privadas. No caso de dados de crianças e adolescentes, a presunção de risco é absoluta e o nível de proteção deve ser, por padrão, o mais elevado (*High Level of Protection by Design*), sendo vedada a divulgação de qualquer dado que permita o perfilamento comportamental ou a localização do menor, nos termos do Art. 7º da Lei nº 15.211/2025."

3. Item 4.2: Registro da decisão final (Pilar 6 do Teste)

Problema: O Guia sugere que a decisão seja "motivada e registrada". Para que a fiscalização ocorra "com ordem", este registro deve ser estruturado e gerar trilhas de auditoria que não possam ser alteradas pelo gestor.

Sugestão de Nova Redação:

"A decisão final resultante do Teste de Interesse Público deve ser registrada em sistema eletrônico auditável, contendo a fundamentação técnica e jurídica. Este registro deve gerar uma trilha de auditoria (log) inalterável, que identifique o agente responsável pela ponderação. Tais registros deverão compor relatórios semestrais de transparência passiva, permitindo que a ANPD e a CGU fiscalizem, a qualquer tempo, a legalidade e a integridade das decisões de sigilo ou divulgação, conforme o Art. 47 da Lei nº 14.129/2021."

4. Item 4.3: Transparência por desenho (*Transparency by Design*)

Problema: O Guia apresenta a transparência por desenho como uma recomendação. No atual cenário de Governo Digital, ela deve ser uma obrigação técnica para garantir que os dados sejam abertos, mas seguros.

Sugestão de Nova Redação:

"A transparência por desenho é obrigatória na concepção de novos sistemas e políticas públicas. Os fluxos devem ser estruturados para que a segregação entre dados públicos e protegidos ocorra de forma automatizada na fonte. A saída de dados para transparência ativa deve seguir obrigatoriamente o formato aberto, estruturado e legível por máquina, incorporando técnicas de mascaramento automático e anonimização irreversível, conforme o Art. 29 da Lei nº 14.129/2021."

5. Inclusão de Novo Item: Auditabilidade da Minimização

Problema: O capítulo trata da minimização de dados, mas não explica como o cidadão ou o órgão de controle podem verificar se o "tarjamento" não está sendo usado para ocultar atos ilegais (como nomes de corruptos sob o pretexto de "intimidade").

Sugestão de Nova Redação:

"Auditabilidade da Minimização: Toda descaracterização (tarjamento) de documentos deve ser acompanhada de uma certidão ou extrato descritivo que justifique, para cada campo ocultado, o dispositivo legal específico que fundamenta a restrição. A utilização de proteção de dados pessoais para fins de ocultação de ato ilegal constitui conduta ilícita sujeita às sanções do Art. 32 da LAI e à apuração por improbidade administrativa."

1. Item: Dados pessoais de agentes públicos (CPF e Matrícula)

Problema: O Guia recomenda a descaracterização do CPF (****.999.999-**), mas não estabelece a necessidade de que essa máscara seja gerada por processos automatizados e auditáveis. Sem isso, há risco de erro humano ou ocultação deliberada de dados públicos.

Sugestão de Nova Redação:

"A descaracterização do CPF de agentes públicos deve ser realizada de forma automatizada pelos sistemas de RH e transparência, garantindo a desambiguação de homônimos sem expor o titular a fraudes. Todo o processo de mascaramento deve gerar trilhas de auditoria (logs) que permitam à CGU e à ANPD verificar se o algoritmo de proteção foi aplicado de forma íntegra a toda a base, conforme o Art. 47 da Lei nº 14.129/2021."

2. Item: Dados pessoais em processos administrativos disciplinares (PADs)

Problema: O Guia sugere como "Boa prática" instruir os PADs prevendo sua publicidade futura. No contexto da LGPD, a segregação de dados protegidos (vida privada/intimidade) deve ser um requisito técnico obrigatório desde a autuação, para evitar o retrabalho de "tarjamento" manual.

Sugestão de Nova Redação (Rigorismo Técnico):

"Os órgãos são obrigados a estruturar a instrução de PADs com segregação nativa entre documentos de interesse público e documentos contendo dados de intimidade ou vida privada. O sistema de gestão processual deve permitir a geração automática de uma versão pública indexada, garantindo que o tarjamento de dados sensíveis seja acompanhado de fundamentação legal específica para cada campo ocultado, assegurando a rastreabilidade das decisões de sigilo."

3. Item: Dados pessoais em listas de controle de acesso (Menores de idade)

Problema: O Guia menciona que o acesso pode ser negado para crianças e adolescentes mediante decisão motivada. No entanto, a Lei nº 15.211/2025 exige o nível mais elevado de proteção por padrão para menores, o que torna a proteção do nome do menor a regra absoluta, e não uma exceção motivada.

Sugestão de Nova Redação:

"Nos registros de controle de acesso a prédios públicos, os dados de crianças e adolescentes devem ser anonimizados por padrão em qualquer consulta de terceiros. A identificação nominal desses titulares é vedada em sistemas de transparência ativa ou passiva, devendo ser fornecido apenas o nome do responsável legal acompanhante, em observância ao melhor interesse do menor e ao Art. 7º da Lei nº 15.211/2025."

4. Item: Dados pessoais sobre beneficiários de programas sociais (Vulnerabilidade)

Problema: O texto afirma que o nome de beneficiários menores não deve ser divulgado a "terceiros não autorizados", mas permite a divulgação parcial do CPF. Para evitar o perfilamento de vulnerabilidade, vedações mais rígidas da Lei 15.211/2025 devem ser aplicadas.

Sugestão de Nova Redação (Proteção ao Vulnerável):

"A transparência sobre beneficiários de programas sociais deve garantir o controle social sem permitir o perfilamento comportamental ou socioeconômico de menores. É vedada a divulgação de qualquer dado (incluindo CPF parcial ou NIS) que permita a reidentificação de crianças e adolescentes. Tais dados devem ser substituídos pela identificação exclusiva do responsável legal, operando o sistema com o grau máximo de privacidade desde o projeto, conforme o Art. 26 da Lei nº 15.211/2025."

5. Item: Dados de estudantes beneficiários de bolsas (Ações Afirmativas)

Problema: O Guia admite que a demanda por informações de menores bolsistas seja avaliada "caso a caso" para identificar a preponderância do interesse público. Isso fragiliza a proteção do menor frente a pedidos de acesso abusivos.

Sugestão de Nova Redação (Garantia de Ordem Técnica):

"A divulgação de dados de estudantes menores beneficiários de bolsas ou cotas deve priorizar a anonimização irreversível dos dados sensíveis (raça, gênero, condição de saúde). O interesse público na fiscalização da política deve ser satisfeito via dados agregados ou extratos auditáveis, sendo a divulgação nominal do menor vedada, salvo se imprescindível para a defesa de direitos humanos, exigindo-se, neste caso, a assinatura de Termo de Responsabilidade Digital e registro na trilha de auditoria do órgão."

Embora a legislação reconheça que o direito à informação não é absoluto, na prática, as negativas de acesso à informação fundamentadas no Artigo 13 do Decreto 7.724/2012 não estão sendo levadas em consideração de forma apropriada pela CGU. Na situação atual, os órgãos continuam a ser obrigados a paralisar suas atividades rotineiras para consolidar dados que estão em sistemas diferentes ou extrair manualmente centenas de documentos que estão em sistemas que não geram automaticamente um único arquivo com todos os documentos (sem contar o tempo necessário para analisar os documentos quanto à necessidade de sigilo face à existência de dados pessoais). É necessário regulamentar de forma apropriada o artigo 13 para que realmente os órgãos não sejam obrigados a paralisar suas atividades e não sejam obrigados a atuar como assistentes de pesquisa aos cidadãos demandantes.

Adicionalmente, não há regulamentação apropriada sobre o tratamento que deva ser dado aos demandantes frequentes (ou demandantes costumazes), que utilizam de forma inapropriada o direito de acesso à informação para demandas que fogem ao interesse público e servem mais ao interesse particular. No CNPq isso fica muito claro em casos em que candidatos concorrem, mas não são contemplados com recursos em determinada Chamada Pública ou não têm seus pedidos atendidos (seja de complementação financeira ou de prorrogação).

Por fim, sugiro também que sejam alterados os artigos 23 e 24 da LAI para que seja incluído o sigilo de atividades de pesquisa e criação desenvolvidas por instituições científicas, tecnológicas e de inovação (ICTs), cfe. (Lei federal nº 10.973, de 2004). A pesquisa científica, embora tenha natureza colaborativa, precisa ser protegida até que alcance o momento em que os resultados já podem ser divulgados sem prejuízos ao autor, que precisa atender a critérios de originalidade e ineditismo para publicação em revistas científicas altamente qualificadas. Essa proteção é necessária mesmo quando a pesquisa não traz um componente de inovação e nem perspectivas de ganho econômico ou desenvolvimento tecnológico, ou seja, quando ela não seria naturalmente protegida pela legislação de propriedade intelectual.

Por fim, o tempo de sigilo dos documentos preparatórios não deve ser considerado como o tempo decorrido até a assinatura do documento. Por vezes, a assinatura que conclui o processo de tomada de decisão é também o momento inicial de execução de determinada atividade que precisa ser iniciada antes que a informação se torne pública. Por exemplo: A assinatura que dá autorização para o lançamento de uma chamada pública conclui o processo de tomada de decisão, mas a chamada pode ser publicada dias após essa assinatura. Se nesse intervalo, entre a assinatura e a publicação, o CNPq for obrigado a conceder cópia do

processo sob o escopo de um pedido feito pela LAI, o demandante terá acesso a uma informação privilegiada, ferindo a concorrência justa.

Sugere-se a inclusão de orientações específicas voltadas às entidades privadas responsáveis pela execução de serviços públicos ou políticas públicas por meio de contratos, convênios, termos de parceria ou instrumentos congêneres celebrados com órgãos e entidades da Administração Pública.

Embora essas entidades estejam sujeitas a obrigações de transparência relacionadas à execução dos recursos públicos recebidos, é importante reconhecer que, na maior parte dos casos, tais obrigações não são definidas autonomamente pela entidade executora. Ao contrário, os próprios órgãos e entidades da Administração Pública estabelecem, por meio de leis, regulamentos, contratos, manuais de transparência, orientações técnicas e instrumentos de monitoramento e fiscalização, quais documentos, informações e dados deverão ser divulgados, bem como a forma, a periodicidade e os ambientes em que essa divulgação deverá ocorrer.

Observa-se, contudo, que essas normas e orientações frequentemente adotam redações genéricas quanto ao conteúdo que deve ser disponibilizado e, em muitos casos, foram elaboradas em momento anterior à entrada em vigor da Lei Geral de Proteção de Dados Pessoais. Como consequência, embora tenham sido concebidas com o legítimo propósito de assegurar a transparência e o controle social, nem sempre incorporam critérios relacionados à necessidade, adequação, minimização de dados e proteção da privacidade dos titulares.

Nesse contexto, as entidades privadas contratadas ou parceiras da Administração Pública frequentemente possuem margem limitada para alterar o conteúdo, o formato ou a extensão das informações divulgadas, ainda que identifiquem potenciais riscos à privacidade e à proteção de dados pessoais. Como resultado, acabam reproduzindo integralmente exigências normativas e contratuais que podem levar à divulgação de dados pessoais em volume superior ao estritamente necessário para o atendimento das finalidades de transparência, controle social e fiscalização.

Diante desse cenário, sugere-se que o Guia ressalte a importância de que os órgãos e entidades da Administração Pública realizem avaliações fundamentadas acerca do interesse público envolvido na divulgação de dados pessoais, observando os princípios da necessidade, adequação, proporcionalidade e minimização previstos na LGPD e forneçam orientações claras, específicas e padronizadas às entidades privadas contratadas quanto aos documentos que efetivamente devem ser divulgados, aos dados pessoais cuja publicação é necessária para atendimento do interesse público e àqueles que podem ou devem ser objeto de anonimização, pseudonimização, ocultação ou outras medidas de mitigação.

Tal medida contribuirá para a harmonização entre os deveres de transparência e a proteção de dados pessoais, reduzirá a insegurança jurídica enfrentada pelas entidades executoras e permitirá que a divulgação de informações ocorra de forma proporcional, responsável e alinhada às finalidades que justificam sua publicidade.

Contribuição do Conselho Federal de Educação Física - CONFEF para a Consulta Pública do Guia de Transparência e Proteção de Dados Pessoais (CGU e ANPD), organizada conforme os três pontos de melhoria identificados.

Área de concentração das sugestões: Dados pessoais em processos administrativos disciplinares - páginas 34 e 35

Tipo de Sugestão: Alteração/Aprimoramento.

PONTO 1: AMPLIAÇÃO DA BASE LEGAL PARA AS AUTARQUIAS DE FISCALIZAÇÃO PROFISSIONAL

Campo 1: Identificação do Trecho do Guia

Capítulo/Seção: Processos Administrativos Disciplinares (PAD) em curso / Transparência Passiva.

Texto Original de Referência: *"No âmbito do Poder Executivo federal, a restrição de acesso ao PAD em curso também se fundamenta na Lei nº 8.112/1990..."*.

Campo 2: Justificativa Técnica

A redação atual fundamenta a restrição de acesso com base quase exclusiva na Lei nº 8.112/1990, que rege apenas servidores públicos estatutários da União. Todavia, os Conselhos de Fiscalização Profissional, como autarquias públicas federais, conduzem processos ético-disciplinares que envolvem agentes privados regulados (profissionais liberais), os quais não se submetem à referida lei. Para conferir segurança jurídica e harmonizar a LAI com a LGPD, é indispensável expandir o escopo para incluir o Artigo 46 da Lei nº 9.784/1999 (Lei do Processo Administrativo Federal), que restringe o acesso aos "interessados", e os princípios constitucionais de presunção de inocência e proteção à imagem (Art. 5º, X e LVII, CF/88).

Campo 3: Proposta de Nova Redação

"No âmbito da Administração Pública Federal, direta e indireta — incluindo as autarquias de fiscalização profissional —, a restrição de acesso ao PAD ou ao processo ético-disciplinar e de fiscalização em curso também se fundamenta na Lei nº 8.112/1990, bem como no art. 46 da Lei nº 9.784/1999. Estes diplomas legais, em harmonia com os princípios da presunção de inocência e de proteção aos dados pessoais (LGPD), asseguram o caráter reservado necessário

à elucidação dos fatos e garantem o acompanhamento do processo apenas às partes diretamente interessadas e a seus procuradores, evidenciando que terceiros estranhos à lide não possuem direito de acesso ou de certidão durante a fase de apuração."

PONTO 2: REFINAMENTO TERMINOLÓGICO (DA "RESTRIÇÃO DE ACESSO" EM VEZ DE "SIGILO")

Campo 1: Identificação do Trecho do Guia

Capítulo/Seção: Processos Administrativos Disciplinares (PAD) em curso / Transparência Passiva.

Texto Original de Referência: *"...o art. 150 assegura o sigilo necessário à elucidação dos fatos e o caráter reservado das atividades da comissão..."*.

Campo 2: Justificativa Técnica

A utilização do termo "sigilo", embora presente na Lei nº 8.112/1990, carece de atualização frente aos regimes jurídicos da LAI e da LGPD, onde o "sigilo" é reservado a hipóteses estritas de segurança do Estado ou segredo de justiça. O enquadramento técnico-jurídico mais adequado para processos em andamento é "Restrição de Acesso", fundamentada na proteção de dados pessoais e nos princípios da finalidade e necessidade (Art. 6º da LGPD). A divulgação de informações de um processo não finalizado viola a legítima expectativa de privacidade e gera risco de dano irreparável à reputação do investigado antes da comprovação de culpa.

Campo 3: Proposta de Nova Redação

Propõe-se que o Guia substitua ou complemente a menção ao "sigilo da comissão" pelo termo "Restrição de Acesso para salvaguarda de dados pessoais e eficácia da apuração", fixando que o fechamento temporário dos autos decorre do cumprimento dos princípios de segurança e proteção à imagem do investigado previstos na LGPD e na Constituição Federal.

PONTO 3: PROTEÇÃO CONTRA A CONFIRMAÇÃO DE EXISTÊNCIA DE PROCESSOS (METADADOS)

Campo 1: Identificação do Trecho do Guia

Capítulo/Seção: Processos Administrativos Disciplinares (PAD) em curso / Transparência Passiva.

Texto Original de Referência: *"...enquanto o art. 156 garante o acompanhamento do processo apenas ao servidor investigado e a seu procurador, evidenciando que terceiros não possuem direito de acesso durante a apuração."*

Campo 2: Justificativa Técnica

É comum a formulação de pedidos via LAI por terceiros que questionam apenas se "existe processo em andamento contra o profissional X". A simples confirmação da existência de uma apuração ética ou o fornecimento de metadados (número de protocolo, data) gera efeitos prejudiciais severos à imagem e à presunção de inocência do investigado. Sob a ótica da LGPD, a divulgação desses dados contextuais a terceiros carece de base legal e viola o princípio da segurança, podendo inclusive comprometer a eficácia das diligências em andamento.

Campo 3: Proposta de Nova Redação (Aditiva)

"...evidenciando que terceiros não possuem direito de acesso durante a apuração. Essa restrição estende-se, inclusive, à confirmação da existência do procedimento administrativo em curso ou ao fornecimento de seu respectivo número de protocolo e metadados a terceiros estranhos à lide, ressalvadas as hipóteses de requisição judicial, policial ou por órgãos de controle no exercício de suas competências legais."

Este documento foi assinado digitalmente por Mariana De Moraes Palmeira.
Para verificar as assinaturas vá ao site <https://oab.portaldeassinaturas.com.br> e utilize o código 686F-9D6A-1C55-4CE9.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal OAB. Para verificar as assinaturas clique no link: <https://oab.portaldeassinaturas.com.br/Verificar/686F-9D6A-1C55-4CE9> ou vá até o site <https://oab.portaldeassinaturas.com.br> e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 686F-9D6A-1C55-4CE9



Hash do Documento

5831E67D6415AB10DD893559BA7A8866BF807E6E1EC79E4AD199F0CFA1F53474

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 17/06/2026 é(são) :

☒ **Nome no certificado:** Mariana De Moraes Palmeira em 17/06/2026 20:48 UTC-03:00

Tipo: Certificado Digital

Evidências

Geolocation: Latitude: -23.006134957885987 Longitude: -43.32592100451898 Accuracy: 43

IP: 172.16.4.22

AC: AC OAB G3



CONTRIBUIÇÕES À CONSULTA PÚBLICA DA ANPD SOBRE O GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

Site: [Guia de Transparência e Proteção de Dados Pessoais - Brasil Participativo](#)

1 - Necessidade de reforço da distinção entre Poder Público e particulares:

O Guia trata da divulgação de dados como dever da Administração Pública, especialmente no Item 5 (publicidade de dados pessoais e de agentes públicos).

Recomendamos explicitar, de forma mais contundente, que os deveres de transparência previstos na Lei de Acesso à Informação - LAI são aplicáveis ao Poder Público, não sendo automaticamente transferíveis a particulares contratados, como instituições financeiras.

Na prática, há risco de interpretação de que terceiros contratados, mediante acionamento do próprio Poder Público, estariam obrigados a realizar divulgação de dados pessoais, o que pode conflitar com:

- LGPD
- sigilo bancário
- deveres contratuais de confidencialidade

2 - Limites para dados de terceiros sem vínculo com função pública:

4.2. Identificando o interesse público e geral preponderante.

O Guia diferencia agentes públicos de demais titulares, indicando menor expectativa de privacidade para os primeiros.

Sugerimos inclusão expressa de orientação sobre dados de terceiros sem relação direta com a função pública (ex: testemunhas, clientes, usuários de serviços financeiros) devem, em regra, ser protegidos, com restrição de divulgação ou aplicação de técnicas de anonimização/mascaramento.

Tal sugestão evitará a exposição indevida de terceiros que não são objeto de controle social direto.

3 - Reforço do sigilo bancário como limite à divulgação:

Item 1.2 – Sigilo legal.

O Guia reconhece o sigilo bancário como hipótese de restrição de acesso.

Entendemos como ponto reforçar expressamente que o sigilo bancário constitui limitação autônoma e prevalente à divulgação de dados, inclusive em contextos de transparência pública.

No contexto de instituições financeiras, o sigilo bancário possui regime legal próprio (LC 105) e não pode ser relativizado por demandas genéricas de transparência.

4 - Aplicabilidade a terceiros contratados:

Item 4.3 – Transparência por desenho

O Guia incentiva a adoção de transparência por desenho no setor público.

O guia deve esclarecer que eventuais obrigações de estruturação de dados para fins de transparência devem ser definidas pelo órgão público, não sendo automaticamente imputáveis aos contratados sem previsão legal ou contratual específica.

Tal ação evitará transferência indevida de ônus operacional e regulatório ao particular.

5 - Necessidade de base legal para solicitações a terceiros:

Itens 4.1 - Roteiro para tomada de decisão e 4.2- Identificando o interesse público e geral preponderante.

O Guia prevê análise de base legal para tratamento de dados no setor público.

Recomendamos incluir orientação expressa de que solicitações de dados a terceiros contratados devem estar acompanhadas de fundamentação legal específica, não bastando invocação genérica de interesse público ou transparência, a fim de garantir segurança jurídica e evitar compartilhamentos indevidos por parte de contratados.

6 Reforço do princípio da minimização

Itens 4.2 - Identificando o interesse público e geral preponderante e 4.3. – Transparência por desenho.

O Guia já prevê a necessidade de divulgar apenas o mínimo necessário.

Sugerimos reforçar, de forma prática, a recomendação de:

- mascaramento de identificadores (ex: CPF).
- anonimização sempre que possível.
- exclusão de dados excessivos.

Tal aplicação visa preservar a exposição integral de dados de testemunhas e CPF ou quaisquer outros dados de terceiros.

7 - Vedação à solicitação de dados bancários em contexto de folha de pagamento:

1.2. Exceções da transparência.

No contexto de contratos administrativos que envolvam processamento de folha de pagamento ou gestão de benefícios, não devem ser solicitados ou divulgados dados bancários individuais de titulares (tais como número de conta, agência ou chaves de pagamento), por não serem necessários ao controle social e envolverem elevado risco de fraude e uso indevido.

Assim, sugerimos explicitar que, em contratos firmados com terceiros, como por exemplo, mas não se limitando, a folha de pagamento, não devem ser solicitados ou divulgados dados bancários individuais dos beneficiários, por não serem necessários à transparência e estarem sujeitos a sigilo bancário e elevado risco de fraude.

Assim, para fins de fiscalização e controle social da folha de pagamento, mostra-se suficiente a divulgação de informações como identificação do beneficiário, vínculo com a Administração e valores pagos, não sendo justificável a ampliação do acesso a dados financeiros individualizados.

8 - Aplicação a dados de qualificação:

Item 5 - Entendimentos sobre a publicidade de dados pessoais.

Ainda, no contexto de contratos administrativos, especialmente aqueles relacionados ao processamento de folha de pagamento ou gestão de benefícios, entende-se igualmente pertinente reforçar a vedação à solicitação e divulgação de dados de qualificação dos titulares que não sejam necessários à finalidade de transparência.

Informações como endereço residencial, telefone, e-mail pessoal ou outros dados de contato inserem-se no âmbito da vida privada e não apresentam relação direta com o controle social da execução da despesa pública, razão pela qual não devem ser objeto de divulgação.

Assim, recomendamos o reforço expresso de que, para fins de fiscalização da folha de pagamento, devem ser limitadas às informações estritamente necessárias, afastando-se a solicitação de dados cadastrais adicionais que possam implicar exposição indevida dos titulares e violação aos princípios da necessidade e da minimização.

CONTRIBUIÇÕES À CONSULTA PÚBLICA DA ANPD SOBRE O GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

Site: [Guia de Transparência e Proteção de Dados Pessoais - Brasil Participativo](#)

1 - Necessidade de reforço da distinção entre Poder Público e particulares:

O Guia trata da divulgação de dados como dever da Administração Pública, especialmente no Item 5 (publicidade de dados pessoais e de agentes públicos).

Recomendamos explicitar, de forma mais contundente, que os deveres de transparência previstos na Lei de Acesso à Informação - LAI são aplicáveis ao Poder Público, não sendo automaticamente transferíveis a particulares contratados, como instituições financeiras.

Na prática, há risco de interpretação de que terceiros contratados, mediante acionamento do próprio Poder Público, estariam obrigados a realizar divulgação de dados pessoais, o que pode conflitar com:

- LGPD
- sigilo bancário
- deveres contratuais de confidencialidade

2 - Limites para dados de terceiros sem vínculo com função pública:

4.2. Identificando o interesse público e geral preponderante.

O Guia diferencia agentes públicos de demais titulares, indicando menor expectativa de privacidade para os primeiros.

Sugerimos inclusão expressa de orientação sobre dados de terceiros sem relação direta com a função pública (ex: testemunhas, clientes, usuários de serviços financeiros) devem, em regra, ser protegidos, com restrição de divulgação ou aplicação de técnicas de anonimização/mascaramento.

Tal sugestão evitará a exposição indevida de terceiros que não são objeto de controle social direto.

3 - Reforço do sigilo bancário como limite à divulgação:

Item 1.2 – Sigilo legal.

O Guia reconhece o sigilo bancário como hipótese de restrição de acesso.

Entendemos como ponto reforçar expressamente que o sigilo bancário constitui limitação autônoma e prevalente à divulgação de dados, inclusive em contextos de transparência pública.

No contexto de instituições financeiras, o sigilo bancário possui regime legal próprio (LC 105) e não pode ser relativizado por demandas genéricas de transparência.

4 - Aplicabilidade a terceiros contratados:

Item 4.3 – Transparência por desenho

O Guia incentiva a adoção de transparência por desenho no setor público.

O guia deve esclarecer que eventuais obrigações de estruturação de dados para fins de transparência devem ser definidas pelo órgão público, não sendo automaticamente imputáveis aos contratados sem previsão legal ou contratual específica.

Tal ação evitará transferência indevida de ônus operacional e regulatório ao particular.

5 - Necessidade de base legal para solicitações a terceiros:

Itens 4.1 - Roteiro para tomada de decisão e 4.2- Identificando o interesse público e geral preponderante.

O Guia prevê análise de base legal para tratamento de dados no setor público.

Recomendamos incluir orientação expressa de que solicitações de dados a terceiros contratados devem estar acompanhadas de fundamentação legal específica, não bastando invocação genérica de interesse público ou transparência, a fim de garantir segurança jurídica e evitar compartilhamentos indevidos por parte de contratados.

6 Reforço do princípio da minimização

Itens 4.2 - Identificando o interesse público e geral preponderante e 4.3. – Transparência por desenho.

O Guia já prevê a necessidade de divulgar apenas o mínimo necessário.

Sugerimos reforçar, de forma prática, a recomendação de:

- mascaramento de identificadores (ex: CPF).
- anonimização sempre que possível.
- exclusão de dados excessivos.

Tal aplicação visa preservar a exposição integral de dados de testemunhas e CPF ou quaisquer outros dados de terceiros.

7 - Vedação à solicitação de dados bancários em contexto de folha de pagamento:

1.2. Exceções da transparência.

No contexto de contratos administrativos que envolvam processamento de folha de pagamento ou gestão de benefícios, não devem ser solicitados ou divulgados dados bancários individuais de titulares (tais como número de conta, agência ou chaves de pagamento), por não serem necessários ao controle social e envolverem elevado risco de fraude e uso indevido.

Assim, sugerimos explicitar que, em contratos firmados com terceiros, como por exemplo, mas não se limitando, a folha de pagamento, não devem ser solicitados ou divulgados dados bancários individuais dos beneficiários, por não serem necessários à transparência e estarem sujeitos a sigilo bancário e elevado risco de fraude.

Assim, para fins de fiscalização e controle social da folha de pagamento, mostra-se suficiente a divulgação de informações como identificação do beneficiário, vínculo com a Administração e valores pagos, não sendo justificável a ampliação do acesso a dados financeiros individualizados.

8 - Aplicação a dados de qualificação:

Item 5 - Entendimentos sobre a publicidade de dados pessoais.

Ainda, no contexto de contratos administrativos, especialmente aqueles relacionados ao processamento de folha de pagamento ou gestão de benefícios, entende-se igualmente pertinente reforçar a vedação à solicitação e divulgação de dados de qualificação dos titulares que não sejam necessários à finalidade de transparência.

Informações como endereço residencial, telefone, e-mail pessoal ou outros dados de contato inserem-se no âmbito da vida privada e não apresentam relação direta com o controle social da execução da despesa pública, razão pela qual não devem ser objeto de divulgação.

Assim, recomendamos o reforço expresso de que, para fins de fiscalização da folha de pagamento, devem ser limitadas às informações estritamente necessárias, afastando-se a solicitação de dados cadastrais adicionais que possam implicar exposição indevida dos titulares e violação aos princípios da necessidade e da minimização.

ITEM: O texto utiliza predominantemente o termo "**Processos Administrativos Disciplinares (PADs)**" para tratar do acesso e da publicidade da atuação correcional, p.6,27,34

FUNDAMENTAÇÃO PARA ALTERAÇÃO: A **Portaria Normativa CGU nº 27/2022** divide o macrocosmo correcional em **Procedimentos Investigativos** (Investigação Preliminar Sumária - IPS, Sindicância Investigativa, etc. - que são preparatórios e inquisitoriais) e **Processos Correcionais Acusatórios** (PAD, Sindicância Acusatória, PAR). Os procedimentos investigativos também são de acesso restrito até a sua conclusão (decisão de arquivamento ou julgamento do PAD subsequente), conforme art. 115 da PN CGU 27/2022.

SUGESTÃO DE MELHORIA: O subtítulo do Guia "Dados pessoais em processos administrativos disciplinares" deveria ser alterado para "**Dados pessoais em processos e procedimentos correcionais**". É preciso esclarecer que o sigilo preparatório (§ 3º do art. 7º da LAI) se aplica desde a fase de admissibilidade e às investigações preliminares (IPS, SINVE, etc.), sendo estas consideradas concluídas apenas quando arquivadas ou com o julgamento final do rito punitivo que delas decorrer.

ITEM: "h) Processo de apuração de irregularidades", p.16

ONDE ESTÁ O PONTO PARA O QUAL SE SUGERE ALTERAÇÃO: propõe-se alterar a justificativa para o tratamento de dados: de "quando o titular for parte" para "quando for necessário ao exercício das competências legais de investigação".

FUNDAMENTAÇÃO PARA ALTERAÇÃO: A atividade correcional não se resume a um genérico "processo de apuração", dividindo-se entre procedimentos investigativos (preparatórios e sigilosos) e processos acusatórios (contraditórios), conforme a Portaria Normativa CGU nº 27/2022. Ademais, a alteração sugerida reflete o entendimento constante da **Nota Técnica nº 1263/2024/CGUNE/DICOR/CRG**, a qual determina que as Corregedorias não precisam do consentimento do titular (ou que este seja formalmente "parte") para tratar dados, pois atuam no **estrito cumprimento de obrigação legal** (art. 7º, II e art. 11, II, "a" da LGPD c/c art. 143 da Lei nº 8.112/90).

ITEM: "Dados pessoais em processos administrativos disciplinares", p.34

ONDE ESTÁ O PONTO PARA O QUAL SE SUGERE ALTERAÇÃO: Na tabela (p.35) o Guia afirma categoricamente que PADs concluídos sobre assédio moral, sexual ou discriminação **"Não devem ser divulgados"** para evitar condenação social, revitimização e exposição de servidor não sancionado.

FUNDAMENTAÇÃO PARA ALTERAÇÃO: O entendimento consolidado da CGU, expresso na **Nota Técnica nº 2993/2022/CGUNE/CRG** e reafirmado na **Nota Técnica nº 1869/2024/CGUNE/DICOR/CRG**, é diametralmente oposto naquilo que tange ao infrator. A CGU firmou que **processos correcionais concluídos que envolvam ilícitos de natureza sexual podem e devem ser divulgados** para fins de acesso à informação, **sem a necessidade de ocultação do nome do acusado/apenado**, pois atende ao interesse público e ao controle social. O que se preserva e se tarja obrigatoriamente são os dados pessoais das vítimas, dos denunciantes e testemunhas.

SUGESTÃO DE MELHORIA: O Guia deve ser corrigido para alinhar-se à jurisprudência da CGU. A regra não é a "não divulgação" do PAD como um todo, mas sim a **divulgação com tarjamento (pseudonimização) rigoroso dos dados da vítima, denunciantes e testemunhas**, mantendo-se a publicidade em relação ao servidor que sofreu a sanção.

ITEM: "Dados pessoais em processos administrativos disciplinares", p.34

ONDE ESTÁ O PONTO PARA O QUAL SE SUGERE ALTERAÇÃO: Ao tratar do "PAD em curso", o texto afirma que o art. 156 da Lei nº 8.112/1990 garante o acompanhamento apenas ao servidor e seu procurador, **"evidenciando que terceiros não possuem direito de acesso durante a apuração"**.

FUNDAMENTAÇÃO PARA ALTERAÇÃO: Embora a regra geral seja o sigilo instrumental para terceiros durante o curso do PAD (Enunciado CGU/CCC nº 14/2016), existem exceções. A recente **Nota Técnica nº 1869/2024/CGUNE/DICOR/CRG** afirma que o acesso a terceiros ao processo disciplinar em curso **poderá ser manejado a título de exceção**, quando o terceiro comprovar interesse particular legítimo ou houver necessidade de produzir provas para defesa em outro processo administrativo/judicial, desde que deferido pela autoridade competente e limitado ao estritamente necessário (sem dados fiscais, bancários, etc.).

SUGESTÃO DE MELHORIA: O Guia deve atenuar a afirmação absoluta de que terceiros "não possuem direito de acesso". É tecnicamente mais preciso indicar que o acesso de terceiros a processos correcionais em curso é **restrito, admitindo-se o acesso parcial a título de exceção, mediante decisão fundamentada da autoridade competente**, quando comprovado o legítimo interesse ou para a produção de provas em outros processos formais.

ITEM: “h) Processo de apuração de irregularidades”, p.16

FUNDAMENTAÇÃO PARA ALTERAÇÃO: A **Nota Técnica nº 1263/2024/CGUNE/DICOR/CRG** é o principal balizador atual sobre a relação entre LGPD e procedimentos investigativos correcionais. Segundo tal documento, fundamentos legais dispensam o consentimento do titular para que a Corregedoria obtenha dados sensíveis e pessoais: a atividade disciplinar é o cumprimento de uma obrigação legal (Art. 7º, II e Art. 11, II, "a" da LGPD, combinados com o dever de apuração imediata do art. 143 da Lei nº 8.112/1990).

SUGESTÃO DE MELHORIA: Para conferir maior segurança jurídica aos operadores que utilizarão este Guia da CGU/ANPD, sugere-se incluir expressamente que as Corregedorias **prescindem do consentimento do titular** para requisitar dados pessoais e sensíveis no curso de apurações (art. 7º, II, e 11, II, "a", da LGPD c/c art. 143 da Lei nº 8.112/90), cabendo à Corregedoria demandante justificar a finalidade, a necessidade e a adequação da medida.

ITEM: Regimes de Publicidade para PADs em Curso e Concluídos

FUNDAMENTAÇÃO PARA ALTERAÇÃO: A restrição de acesso a terceiros durante o curso do processo baseia-se no sigilo de documentos preparatórios até a tomada de decisão (Art. 7º, §3º da LAI) e no Enunciado CGU/CCC nº 14/2016. Quanto aos processos concluídos, a proposição é validada pela **Nota Técnica nº 2418/2023** e **Nota Técnica nº 547/2023** da CGU. Estas notas firmaram que processos concluídos com sanção são públicos (informação de interesse coletivo), mas que **decisões de arquivamento ou absolvição devem ser publicizadas sem a menção ao nome do servidor e sua matrícula**, citando-se apenas o número do PAD e os números centrais do CPF. Logo, a distinção entre PAD com e sem penalidade proposta é essencial e deve constar no Guia.

SUGESTÃO DE MELHORIA: Sugere-se reforçar o sigilo de atos instrutórios de PADs em curso e propõe uma **matriz específica para PADs** indicando que processos em curso são restritos; PADs concluídos com penalidade são públicos (com tarjamentos); e PADs concluídos sem penalidade (absolvição) são restritos como regra.

OMISSÃO: Publicidade e Dados no Termo de Ajustamento de Conduta (TAC). O documento não menciona o Termo de Ajustamento de Conduta (TAC).

FUNDAMENTAÇÃO PARA ALTERAÇÃO: O TAC (regulamentado pela Portaria Normativa CGU nº 27/2022) tornou-se a principal ferramenta de resolução consensual de infrações disciplinares de menor potencial ofensivo no Executivo Federal. A **Nota Técnica nº 2222/2024/CGUNE/DICOR/CRG** define regras claras sobre a publicidade e proteção de dados no TAC: *"Uma vez publicado o extrato do TAC, os autos do processo administrativo tornam-se públicos, salvo as informações especialmente protegidas"*. Além disso, o art. 69 da PN CGU 27/2022 determina a publicação do extrato com o nome do servidor, número do processo e descrição genérica do fato.

SUGESTÃO DE MELHORIA: Recomenda-se incluir uma seção ou tabela específica no Guia tratando do **Termo de Ajustamento de Conduta (TAC)**, informando que o processo é restrito até sua celebração, mas que os autos tornam-se públicos (resguardados dados protegidos como endereços e telefones) a partir da publicação do seu extrato no Diário Oficial ou Boletim de Pessoal, o qual obrigatoriamente veiculará o nome do servidor celebrante.

ITEM: Vedação ao Uso Abusivo da LGPD para Negativa de Acesso

FUNDAMENTAÇÃO PARA ALTERAÇÃO: A sugestão reflete o principal embate atual entre a Lei de Acesso à Informação e a proteção de dados. O **Enunciado CGU nº 12/2023** explicita a tese defendida: o fundamento "informações pessoais" não pode ser utilizado de forma geral e abstrata para negar pedidos de acesso; os dados devem ser tratados (tarjados, ocultados) para que o restante do documento seja fornecido à sociedade. O Enunciado CGU nº 4/2022 também reforça que a LAI e a LGPD são sistemicamente compatíveis e não há antinomia, não sendo a LGPD um escudo absoluto contra a transparência pública.

SUGESTÃO DE MELHORIA: Sugere-se a inclusão de vedação expressa ao uso abusivo da LGPD para negar integralmente o acesso a processos, priorizando-se o fornecimento parcial com anonimização, pseudonimização ou tarjamento.

OMISSÃO - PROPOSTA DE INCLUSÃO AO FINAL DO DOCUMENTO DA SEGUINTE SEÇÃO: "Canais de Atendimento, Governança de Dados e Fluxo Recursal"

PROPOSTA DE REDAÇÃO A SER INCLUÍDA:

O Encarregado pelo Tratamento de Dados Pessoais

Todo órgão ou entidade (Controlador) deve indicar um Encarregado pelo Tratamento de Dados Pessoais.

A identidade e as informações de contato do Encarregado devem ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do órgão.

Este profissional atua como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), tendo como funções aceitar reclamações e comunicações dos titulares, prestar esclarecimentos, adotar providências e orientar os funcionários a respeito das práticas de proteção de dados.

Serviço de Informações ao Cidadão (SIC) e Plataforma Fala.BR

Os órgãos devem manter um Serviço de Informações ao Cidadão (SIC), instalado em unidade física identificada, de fácil acesso e aberta ao público, com o objetivo de atender e orientar o público e receber e registrar pedidos de acesso à informação.

No âmbito do Poder Executivo federal, o registro e atendimento aos pedidos de acesso à informação ocorrem de forma integrada por meio de sistema eletrônico específico mantido pela Controladoria-Geral da União (Plataforma Fala.BR / e-SIC).

Autoridade de Monitoramento da LAI

Para assegurar o cumprimento eficiente das normas relativas ao acesso à informação, o dirigente máximo do órgão designará uma autoridade de monitoramento que lhe seja diretamente subordinada.

Esta autoridade é responsável por avaliar e monitorar a implementação da lei, orientar as unidades do órgão e manifestar-se sobre reclamações apresentadas contra omissão de resposta aos solicitantes.

Prazos e Instâncias Recursais

Caso a informação solicitada não esteja prontamente disponível, o órgão tem o prazo de até 20 dias para responder, sendo admitida a prorrogação por mais 10 dias mediante justificativa.

No caso de negativa total ou parcial de acesso à informação (inclusive sob alegação de proteção de dados pessoais), o órgão deve indicar as razões da recusa, a possibilidade e o prazo de recurso, bem como a autoridade que o apreciará.

No âmbito federal, desprovidos os recursos nas instâncias internas do órgão, cabe recurso à Controladoria-Geral da União (CGU) e, posteriormente, à Comissão Mista de Reavaliação de Informações (CMRI).

FUNDAMENTAÇÃO LEGAL PARA CADA ITEM PROPOSTO

Para o Item Encarregado/DPO: A base legal reside no inciso VIII do art. 5º e no art. 41, *caput* e §§ 1º e 2º, ambos da LGPD.

Para o Item SIC e Fala.BR: A fundamentação encontra-se no inciso I do art. 9º da LAI, regulamentado pelos arts. 9º e 10 do Decreto nº 7.724/2012. A obrigatoriedade do sistema eletrônico federal (Fala.BR) baseia-se no art. 11-A do mesmo Decreto.

Para o Item Autoridade de Monitoramento: Fundamenta-se no art. 40 da LAI e, detalhadamente, no art. 67 do Decreto nº 7.724/2012.

Para o Item Prazos e Recursos: Os prazos de 20 e 10 dias constam nos arts. 15 e 16 do Decreto nº 7.724/2012. A obrigatoriedade de informar as vias recursais repousa no art. 21 do referido Decreto. As instâncias externas de recurso encontram guarida no art. 35 do Decreto nº 7.724/2012.

EXPLICAÇÃO DO PORQUÊ SE ESTÁ SUGERINDO A INCLUSÃO DO REFERIDO TEXTO

A inclusão dessa seção é sugerida porque um **"Guia", por sua própria natureza, deve transcender a análise puramente teórica ou material do direito**. Enquanto o restante do documento explica *o que* deve ser protegido e *o que* deve ser publicizado, a ausência de uma instrução sobre *como* e *com quem* resolver os impasses práticos torna o documento incompleto para a governança diária das instituições.

Ao detalhar a estrutura de governança (Encarregado de Dados, SIC, e Autoridade de Monitoramento) e o fluxo procedimental (prazos e instâncias de recursos), **o Guia confere segurança jurídica e previsibilidade**. Ele orienta o cidadão sobre onde protocolar seu pedido ou reclamação e guia o próprio servidor público sobre a quem recorrer internamente em casos de dúvidas complexas que envolvam a intersecção entre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados. Isso atende ao objetivo das legislações de garantir que os direitos informacionais não sejam apenas uma previsão em papel, mas possuam canais ágeis e transparentes de efetivação.

CONSULTA PÚBLICA

GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS ANPD E CGU

Capítulo 5: Entendimentos sobre a publicidade de dados pessoais

A FIESP recomenda atenção especial aos trechos do Guia que tratam de licitações, contratos, fornecedores, registros de acesso a prédios públicos, processos fiscalizatórios, auditorias e atividades regulatórias. Esses temas afetam diretamente a relação entre Administração Pública e setor produtivo.

No caso de fornecedores e contratados, é legítima a divulgação de informações necessárias ao controle social, como razão social, CNPJ, objeto contratado, valores globais, vigência, órgão contratante, situação contratual e sanções administrativas aplicadas, quando houver. Contudo, não devem ser divulgados de forma irrestrita dados pessoais de representantes, empregados, responsáveis técnicos ou terceiros, nem informações empresariais protegidas por sigilo legal, segredo industrial, propriedade intelectual ou legítimo interesse concorrencial.

A divulgação de documentos empresariais deve observar análise concreta e proporcional, especialmente quando envolver metodologias proprietárias, projetos técnicos sensíveis, informações de segurança, dados de fornecedores, documentos de identificação, dados bancários, contatos pessoais, assinaturas manuscritas e informações comerciais que possam gerar risco de fraude, prejuízo concorrencial ou exposição indevida.

A FIESP sugere que o Guia estabeleça exemplos mais claros de divulgação parcial em contratos e processos empresariais, com indicação de quais dados tendem a ser públicos, quais devem ser avaliados para descaracterização e quais podem justificar restrição de acesso, conforme o caso concreto.

Sugestão de inclusão:

“Em processos de contratação pública, fiscalização, regulação e controle, a publicidade deve assegurar o controle social sobre o uso de recursos públicos e a atuação administrativa, sem acarretar exposição desnecessária de dados pessoais ou de informações empresariais protegidas. Como regra, podem ser divulgados razão social, CNPJ, objeto, valor global, vigência, órgão contratante, situação contratual e sanções administrativas. Devem ser avaliados para restrição, descaracterização ou divulgação parcial dados pessoais de representantes, empregados, responsáveis técnicos, procuradores e terceiros, bem como informações protegidas por segredo industrial, propriedade intelectual, sigilo comercial, segurança institucional ou risco concorrencial.”

Sugestão de novo item: Dados pessoais e informações empresariais em documentos de pessoas jurídicas privadas

A FIESP recomenda a inclusão de item específico no Guia dedicado a documentos empresariais custodiados pelo Poder Público. A ausência de tratamento próprio para esse tema pode gerar insegurança jurídica, especialmente porque empresas privadas são frequentemente obrigadas a fornecer informações detalhadas à Administração Pública em razão de contratos, fiscalizações, políticas públicas, programas de incentivo, regulação setorial ou exigências legais.

Esse novo item poderia consolidar orientações sobre publicidade, divulgação parcial, proteção de dados pessoais de representantes e empregados, preservação de segredo industrial, tratamento de informações concorrencialmente relevantes e aplicação de técnicas como tarja, extração de

certidões, elaboração de versões públicas de documentos, descaracterização de CPF, ocultação de assinaturas e supressão de dados excessivos.

Sugestão de redação para novo item:

“Documentos apresentados por pessoas jurídicas de direito privado à Administração Pública podem conter, simultaneamente, informações de interesse público, dados pessoais de indivíduos vinculados à empresa e informações empresariais protegidas por sigilo legal, segredo industrial, propriedade intelectual ou legítimo interesse concorrencial. Nesses casos, o órgão ou entidade deverá avaliar a possibilidade de divulgação parcial, preservando as informações necessárias ao controle social e restringindo, descaracterizando ou suprimindo dados pessoais excessivos, documentos de identificação, endereços residenciais, contatos pessoais, assinaturas manuscritas, dados bancários, informações técnicas proprietárias, estratégias comerciais, composições de custos cuja divulgação possa gerar prejuízo concorrencial, informações de segurança e demais elementos cuja divulgação possa gerar exposição indevida, risco de fraude, prejuízo concorrencial ou violação de direitos.”

CONSULTA PÚBLICA

GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS ANPD E CGU

Capítulo 1: Direito de acesso à informação e seus limites

A FIESP concorda com a premissa de que a transparência deve ser a regra e o sigilo a exceção. Contudo, recomenda-se que o Guia reforce, de maneira mais explícita, que as exceções à transparência não se limitam às hipóteses de classificação da informação, abrangendo também sigilos legais específicos, proteção de dados pessoais, documentos preparatórios, segredo industrial, sigilo comercial, sigilo fiscal, sigilo bancário, propriedade intelectual e informações cuja divulgação possa afetar a segurança institucional, econômica ou competitiva de agentes privados.

Sugere-se aprimorar o texto para evitar interpretações segundo as quais todo documento apresentado por empresa à Administração Pública, pelo simples fato de estar sob custódia estatal, passaria automaticamente a ser público em sua integralidade.

Em contratações públicas, processos regulatórios, fiscalizações, programas de fomento, certificações, habilitações técnicas, projetos de inovação e interações com órgãos públicos, empresas frequentemente compartilham informações que podem envolver estratégia comercial, metodologia produtiva, dados técnicos, estrutura de fornecedores, informações de segurança, dados de empregados, documentos de representantes e informações protegidas por propriedade intelectual.

Assim, recomenda-se que o Guia destaque a necessidade de análise concreta, motivada e proporcional antes da divulgação de documentos empresariais que contenham dados pessoais ou informações protegidas por sigilo legal, segredo industrial, sigilo comercial ou legítimo interesse concorrencial.

Sugestão de inclusão:

“Nos casos em que documentos custodiados pela Administração Pública contenham informações fornecidas por pessoas jurídicas de direito privado, especialmente em processos de contratação, fiscalização, regulação, fomento, inovação, certificação ou habilitação técnica, a análise de acesso deverá considerar, além do interesse público na divulgação, a eventual incidência de sigilos legais, segredo industrial, propriedade intelectual, informações concorrencialmente relevantes, dados pessoais de representantes, empregados ou terceiros, bem como riscos à segurança, à concorrência e à competitividade.”

Capítulo 2: Direito à proteção de dados pessoais e da privacidade nos termos da LGPD

A FIESP considera positiva a afirmação de que LAI e LGPD são normas compatíveis e complementares. No entanto, recomenda-se que o Guia esclareça com maior objetividade que a compatibilização entre transparência e proteção de dados deve observar, de forma cumulativa, os princípios da finalidade, adequação, necessidade, segurança, prevenção, transparência e responsabilização.

É importante que o Guia evite uma interpretação excessivamente centrada na divulgação, sem incorporar de forma equivalente a lógica de governança do tratamento de dados. A divulgação de dados pessoais pela Administração Pública é também uma operação de tratamento e, portanto, deve estar submetida a critérios mínimos de necessidade, proporcionalidade, segurança e prestação de contas.

A FIESP sugere que o Guia reforce que os órgãos públicos devem manter registros decisórios, critérios objetivos e mecanismos de controle interno para justificar a divulgação integral, a divulgação parcial ou a restrição de acesso. Isso é especialmente importante para reduzir decisões contraditórias entre órgãos públicos e evitar insegurança jurídica para cidadãos e empresas.

Sugestão de inclusão:

“A divulgação de dados pessoais pela Administração Pública, seja em transparência ativa ou em resposta a pedidos de acesso à informação, constitui operação de tratamento de dados pessoais e deve observar os princípios da LGPD, em especial finalidade, adequação, necessidade, segurança, prevenção e responsabilização. A decisão pela divulgação integral, divulgação parcial ou restrição de acesso deve ser motivada, registrada e compatível com a finalidade pública pretendida.”

Capítulo 3: Proteção de dados pessoais prevista na LAI

A FIESP concorda com a distinção entre dado pessoal em sentido amplo, nos termos da LGPD, e informação pessoal protegida pela LAI, relacionada à intimidade, vida privada, honra e imagem. Essa diferenciação é importante para evitar o uso indevido da LGPD como barreira automática à transparência.

Contudo, recomenda-se que o Guia explicita que dados pessoais de representantes, sócios, empregados, responsáveis técnicos, procuradores, consultores ou prepostos de empresas privadas não devem ser tratados, de forma automática, como dados de interesse público irrestrito. A existência de vínculo entre uma empresa e o Poder Público não elimina a necessidade de proteção dos dados pessoais de indivíduos vinculados à pessoa jurídica.

Em processos administrativos, contratações, convênios, termos de cooperação, procedimentos fiscalizatórios e interações regulatórias, é comum que documentos contenham assinaturas, documentos de identificação, endereços pessoais, telefones, e-mails pessoais, procurações, currículos, informações profissionais, dados bancários e outros elementos pessoais. A publicidade do ato administrativo pode ser preservada sem que haja exposição excessiva desses dados.

Sugestão de inclusão:

“A publicidade de atos administrativos envolvendo pessoas jurídicas de direito privado não implica, por si só, autorização para divulgação irrestrita de dados pessoais de sócios, administradores, empregados, representantes legais, responsáveis técnicos, procuradores ou terceiros vinculados à empresa. Sempre que possível, devem ser preservadas as informações necessárias ao controle social do ato, com supressão, descaracterização ou restrição de dados pessoais excessivos ou desvinculados da finalidade pública da divulgação.”

Capítulo 4: Teste de Interesse Público

A FIESP considera o Teste de Interesse Público um dos pontos mais relevantes do Guia, pois oferece metodologia prática para ponderar transparência, proteção de dados e riscos ao titular. Recomenda-se, entretanto, que o Guia detalhe melhor a aplicação do teste em situações que envolvam pessoas jurídicas e dados pessoais presentes em documentos empresariais.

A divulgação de informações deve considerar não apenas a existência de interesse público abstrato, mas o benefício coletivo concreto, a necessidade da informação para atingir esse benefício, a existência de meios menos invasivos e os riscos decorrentes da divulgação. O interesse público não deve ser confundido com curiosidade pública, conveniência genérica ou exposição ampla de documentos sem triagem prévia.

Também se recomenda incluir expressamente que o Teste de Interesse Público considere riscos de segurança institucional, fraudes, engenharia social, ataques cibernéticos, exposição de dados de empregados, fornecedores e representantes, bem como riscos concorrenciais e de violação de segredo industrial quando documentos empresariais estiverem envolvidos.

Sugestão de inclusão:

“Na aplicação do Teste de Interesse Público a documentos apresentados por pessoas jurídicas de direito privado à Administração Pública, a avaliação deverá considerar o benefício coletivo concreto da divulgação, a necessidade dos dados para a finalidade pretendida, a existência de meios menos invasivos, a possibilidade de divulgação parcial, anonimização, pseudonimização ou descaracterização, bem como riscos à privacidade de indivíduos, à segurança da informação, à prevenção de fraudes, à concorrência, ao segredo industrial e à proteção de informações estratégicas.”

Capítulo 4.3: Transparência por desenho

A FIESP considera positiva a inclusão do conceito de transparência por desenho. A adoção desse princípio pode reduzir retrabalho, diminuir riscos de exposição indevida de dados, padronizar procedimentos e permitir que informações públicas sejam disponibilizadas de forma segura desde a origem.

Sugere-se, contudo, que o Guia avance em recomendações práticas para os órgãos públicos. Em especial, recomenda-se prever que sistemas de protocolo, contratação, fiscalização, regulação, ouvidoria e gestão documental sejam estruturados com campos segregados para informações públicas, informações pessoais, informações sensíveis, documentos sigilosos e informações empresariais protegidas.

A ausência dessa segregação gera insegurança para a Administração e para o setor privado, pois documentos inteiros podem acabar sendo restringidos ou divulgados indevidamente por falta de classificação adequada dos campos de informação.

Sugestão de inclusão:

“Os órgãos e entidades públicas devem, sempre que possível, estruturar seus sistemas, formulários, processos eletrônicos e bases documentais com segregação entre campos de informação pública, dados pessoais, dados pessoais sensíveis, informações protegidas por sigilo legal e informações empresariais estratégicas. Essa organização favorece a transparência ativa, reduz o risco de exposição indevida e permite respostas mais céleres e proporcionais a pedidos de acesso à informação.”

Capítulo 5: Entendimentos sobre a publicidade de dados pessoais

A FIESP recomenda atenção especial aos trechos do Guia que tratam de licitações, contratos, fornecedores, registros de acesso a prédios públicos, processos fiscalizatórios, auditorias e atividades regulatórias. Esses temas afetam diretamente a relação entre Administração Pública e setor produtivo.

No caso de fornecedores e contratados, é legítima a divulgação de informações necessárias ao controle social, como razão social, CNPJ, objeto contratado, valores globais, vigência, órgão contratante, situação contratual e sanções administrativas aplicadas, quando houver. Contudo, não devem ser divulgados de forma irrestrita dados pessoais de representantes, empregados,

responsáveis técnicos ou terceiros, nem informações empresariais protegidas por sigilo legal, segredo industrial, propriedade intelectual ou legítimo interesse concorrencial.

A divulgação de documentos empresariais deve observar análise concreta e proporcional, especialmente quando envolver metodologias proprietárias, projetos técnicos sensíveis, informações de segurança, dados de fornecedores, documentos de identificação, dados bancários, contatos pessoais, assinaturas manuscritas e informações comerciais que possam gerar risco de fraude, prejuízo concorrencial ou exposição indevida.

A FIESP sugere que o Guia estabeleça exemplos mais claros de divulgação parcial em contratos e processos empresariais, com indicação de quais dados tendem a ser públicos, quais devem ser avaliados para descaracterização e quais podem justificar restrição de acesso, conforme o caso concreto.

Sugestão de inclusão:

“Em processos de contratação pública, fiscalização, regulação e controle, a publicidade deve assegurar o controle social sobre o uso de recursos públicos e a atuação administrativa, sem acarretar exposição desnecessária de dados pessoais ou de informações empresariais protegidas. Como regra, podem ser divulgados razão social, CNPJ, objeto, valor global, vigência, órgão contratante, situação contratual e sanções administrativas. Devem ser avaliados para restrição, descaracterização ou divulgação parcial dados pessoais de representantes, empregados, responsáveis técnicos, procuradores e terceiros, bem como informações protegidas por segredo industrial, propriedade intelectual, sigilo comercial, segurança institucional ou risco concorrencial.”

Sugestão de novo item: Dados pessoais e informações empresariais em documentos de pessoas jurídicas privadas

A FIESP recomenda a inclusão de item específico no Guia dedicado a documentos empresariais custodiados pelo Poder Público. A ausência de tratamento próprio para esse tema pode gerar insegurança jurídica, especialmente porque empresas privadas são frequentemente obrigadas a fornecer informações detalhadas à Administração Pública em razão de contratos, fiscalizações, políticas públicas, programas de incentivo, regulação setorial ou exigências legais.

Esse novo item poderia consolidar orientações sobre publicidade, divulgação parcial, proteção de dados pessoais de representantes e empregados, preservação de segredo industrial, tratamento de informações concorrencialmente relevantes e aplicação de técnicas como tarja, extração de certidões, elaboração de versões públicas de documentos, descaracterização de CPF, ocultação de assinaturas e supressão de dados excessivos.

Sugestão de redação para novo item:

“Documentos apresentados por pessoas jurídicas de direito privado à Administração Pública podem conter, simultaneamente, informações de interesse público, dados pessoais de indivíduos vinculados à empresa e informações empresariais protegidas por sigilo legal, segredo industrial, propriedade intelectual ou legítimo interesse concorrencial. Nesses casos, o órgão ou entidade deverá avaliar a possibilidade de divulgação parcial, preservando as informações necessárias ao controle social e restringindo, descaracterizando ou suprimindo dados pessoais excessivos, documentos de identificação, endereços residenciais, contatos pessoais, assinaturas manuscritas, dados bancários, informações técnicas proprietárias, estratégias comerciais, composições de custos cuja divulgação possa gerar prejuízo concorrencial, informações de segurança e demais elementos cuja divulgação possa gerar exposição indevida, risco de fraude, prejuízo concorrencial ou violação de direitos.”

Em atenção à comunicação acerca da abertura de consulta pública conjunta da CGU e da ANPD sobre o Guia de Transparência e Proteção de Dados Pessoais, informamos que realizamos análise técnica do documento.

De forma geral, o Guia apresenta importante avanço ao consolidar diretrizes para harmonização entre a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD), com destaque para o modelo de tomada de decisão baseado na ponderação entre transparência e proteção de dados.

Contudo, considerando as particularidades do nosso negócio, especialmente em razão do tratamento intensivo de dados financeiros e da sujeição ao regime de sigilo bancário (LC nº 105/2001), identificamos oportunidades de aprimoramento do Guia, dentre as quais destacamos:

1. Tratamento específico do sigilo bancário (Referência: item “Sigilo legal”, p. 5)

Sugere-se a inclusão de seção específica tratando da interação entre LAI, LGPD e sigilo bancário, com delimitação mais clara das hipóteses de restrição absoluta de acesso, especialmente quanto a dados individualizados de clientes e operações financeiras.

2. Classificação de dados financeiros como dados de alto risco (Referência: definição de dados pessoais e sensíveis – p. 8)

Sugere-se o reconhecimento expresso dos dados financeiros individualizados como categoria de elevado risco, diante do potencial de fraude, uso indevido e impactos à segurança dos titulares.

3. Transparência ativa no setor financeiro (Referência: Capítulo 4 – transparência ativa e minimização, p. 25–26)

Sugere-se a inclusão de orientações objetivas sobre a definição dos campos mínimos e dos campos vedados para divulgação em bases de transparência ativa, especialmente no Portal da Transparência e em sistemas de consulta pública.

Embora o Guia apresente diversos exemplos de dados que podem ou não ser divulgados em situações específicas, não há orientação consolidada que auxilie os órgãos na definição prática dos campos a serem disponibilizados em listas e bases de dados amplamente divulgadas. Essa lacuna pode resultar em tratamentos distintos para informações equivalentes entre órgãos públicos, aumentando o risco de exposição excessiva de dados pessoais.

Nesse contexto, seria interessante que o Guia apresentasse critérios objetivos para a construção de bases públicas, considerando: A finalidade de controle social pretendida; A demonstração da necessidade de cada campo divulgado; A adoção preferencial de identificadores parcialmente mascarados e a exclusão de campos que não agreguem valor à fiscalização da atuação estatal.

Adicionalmente, sugere-se que o Guia esclareça expressamente o tratamento aplicável às assinaturas constantes de contratos administrativos, convênios e instrumentos congêneres. Embora o documento afirme que assinaturas manuscritas não devem ser divulgadas por representarem risco de fraude e não serem necessárias ao controle social, seria importante deixar expresso que a comprovação da autenticidade dos documentos pode ocorrer por mecanismos de validação institucional, sem necessidade da exposição da imagem da assinatura dos servidores públicos ou representantes das partes contratantes.

4. Inclusão de exemplos práticos do setor financeiro (Referência: Capítulo 5 – entendimentos práticos, p. 32 em diante)

Sugere-se a inclusão de casos aplicados ao contexto bancário (ex.: crédito, contratos financeiros, beneficiários de programas operados por instituições financeiras públicas), de modo a facilitar a aplicação prática do Guia.

Diante da relevância do tema e do potencial impacto sobre as atividades do Banco, permanecemos à disposição para eventuais esclarecimentos ou aprofundamentos adicionais, caso necessário.

Ref.: Consulta Pública da ANPD e da CGU – Guia de Transparência e Proteção de Dados Pessoais

Apresentamos a seguir as nossas sugestões de contribuições à Consulta Pública sobre o Guia de Transparência e Proteção de Dados Pessoais ([aqui](#)), promovida pela Agência Nacional de Proteção de Dados (ANPD) e pela Controladoria-Geral da União (CGU).

Considerações Gerais

O Einstein Hospital Israelita (“Einstein”), entidade que atua em assistência, ensino, pesquisa, inovação e saúde digital, e que mantém colaboração com políticas públicas e com o Poder Público, apoia a iniciativa da CGU e da ANPD e reconhece a relevância do Guia para harmonizar a transparência pública e a proteção de dados pessoais. A contribuição busca aprimorar a clareza, a segurança jurídica e a aplicabilidade prática do documento, especialmente em contextos de saúde, pesquisa, inovação e tratamento de dados pessoais sensíveis. Parte-se das premissas de que a publicidade é a regra, de que a LGPD não cria sigilo e de que eventuais restrições se fundamentam na LAI.

Capítulo 1 — Direito de acesso à informação e seus limites

Sugerimos que o rol exemplificativo de sigilos legais (art. 22 da LAI) do capítulo 1.2 mencione expressamente o sigilo profissional, em especial o sigilo médico, por sua elevada relevância para a Administração Pública que custodia informações de saúde (redes públicas, perícias, programas e parcerias com instituições de saúde). Trata-se de sigilo legal típico, preservado pela LAI, que não se confunde com a (inexistente) criação de sigilo pela LGPD e que convive com o regime do art. 31. Sugere-se acrescentar:

“Sigilo profissional, inclusive o sigilo médico, protege informações confiadas em razão do exercício de profissão regulamentada, amparado, entre outros, no art. 154 do Código Penal, na Lei nº 12.842/2013 (exercício da medicina) e, quanto à guarda e confidencialidade de prontuários, na Lei nº 13.787/2018, constituindo exceção legítima ao acesso preservada pelo art. 22 da LAI.”

Capítulo 2 — Proteção de dados pessoais nos termos da LGPD

Apoiamos integralmente a afirmação de que a LGPD não cria hipóteses de sigilo, nem altera o rol de informações restritas. Sugerimos apenas reforçar, na parte final, que a complementaridade entre LAI e LGPD impõe, no tratamento para fins de transparência, a observância dos princípios da finalidade, necessidade, adequação, segurança e prestação de contas, o que é particularmente sensível quando há dados de saúde sob guarda pública ou compartilhados em parcerias.

Capítulo 3 — Proteção de dados pessoais prevista na LAI

Sugerimos a inclusão de um box específico sobre dados de saúde, reconhecendo que: (i) dados de saúde são dados sensíveis (art. 5º, II, e art. 11 da LGPD) e estão abarcados pela proteção da intimidade (art. 31 da LAI); (ii) prontuários e registros assistenciais sujeitam-se a sigilo profissional, que é sigilo legal preservado pelo art. 22 da LAI; e (iii) quando a identificação individual não for indispensável ao interesse público, deve-se preferir a divulgação agregada, anonimizada ou pseudonimizada. Quanto à pesquisa (item 3.3, alínea “d”), apoiamos o entendimento da ANPD de que a anonimização não é condição para o compartilhamento, mas sugerimos ressalva sobre o risco de reidentificação em bases clínicas, genômicas, biométricas, de doenças raras ou de alta granularidade, com remissão à governança ética da pesquisa (CEP/CONEP).

Box sugerido no Capítulo 3 ou no Capítulo 5:

“Dados de saúde são dados pessoais sensíveis (art. 5º, II, e art. 11 da LGPD) e estão abrangidos pela proteção da intimidade e da vida privada de que trata o art. 31 da LAI. Prontuários e registros assistenciais sujeitam-se, ainda, ao sigilo profissional, que constitui sigilo legal preservado pelo art. 22 da LAI. A presença de dados de saúde em documentos sob guarda pública ou em informações decorrentes de parcerias não impõe sigilo automático, mas exige análise reforçada de risco e a preferência, sempre que a identificação individual não for indispensável ao interesse público preponderante, pela divulgação agregada, anonimizada ou pseudonimizada. Indicadores agregados de produção, qualidade, cobertura e resultados assistenciais e de pesquisa devem ser divulgados; dados individuais de pacientes, acompanhantes, familiares e participantes de pesquisa, em regra, devem ser protegidos.”

Adicionalmente, sugerimos acrescentar, após o parágrafo que acolhe o entendimento da ANPD sobre anonimização:

“Em bases de alta granularidade, como dados clínicos detalhados, genômicos, biométricos, de imagens médicas, de doenças raras ou de coortes reduzidas, há risco concreto de reidentificação mesmo após pseudonimização. Nesses casos, recomenda-se análise reforçada de risco, a adoção de salvaguardas adicionais (controle de acesso, ambiente seguro, Termo de Responsabilidade e, quando cabível, dados sintéticos ou agregados) e a observância da governança ética da pesquisa, inclusive a aprovação pelo sistema CEP/CONEP, quando aplicável. A divulgação de resultados deve preferir formatos agregados que preservem o conteúdo científico sem expor titulares.”

Capítulo 4 — Garantindo a transparência com proteção dos dados pessoais

No Teste de Interesse Público (item 4.2, passo 3), sugerimos a inclusão de matriz orientativa de risco (probabilidade × impacto), com graduação em baixo, médio e alto, e de tipologia de danos a considerar: discriminação, estigmatização, fraude, constrangimento, reidentificação, dano reputacional, exposição indevida de condição de saúde e abalo da confiança no serviço público. A matriz é meramente orientativa e não substitui a análise qualitativa e casuística. Sugerimos, ainda, que o Guia trate expressamente dos pedidos de acesso relativos a sistemas de inteligência artificial, algoritmos e decisões automatizadas do Poder Público, privilegiando a transparência sobre finalidade, lógica geral, governança, métricas de desempenho, riscos e medidas de mitigação, sem expor dados pessoais, segredos legais, propriedade intelectual ou vulnerabilidades de segurança. Na transparência por desenho (item 4.3), sugerimos estender as boas práticas às entidades parceiras, mediante cláusulas de segregação prévia entre informação pública e protegida, metadados e trilhas de auditoria.

Sugerimos, adicionalmente, acrescentar à tabela de técnicas menos invasivas exemplos do setor de saúde:

- Agregação por faixa etária, sexo, município/região e período, para indicadores epidemiológicos e de produção assistencial, sem identificação dos titulares.
- Descaracterização de CPF (***.999.999-**) e tarjamento de identificadores diretos em documentos de parcerias e prestações de contas.
- Divulgação de quantitativos de atendimentos, procedimentos e beneficiários por unidade ou programa, em vez de listas nominais de pacientes.
- Uso de pseudonimização com chave controlada para acompanhamento de coortes em estudos, dispensando a identificação direta.

Capítulo 5 — Entendimentos sobre a publicidade de dados pessoais

Sugerimos a inclusão de subseção sobre dados de saúde em contratos, convênios e parcerias com o Poder Público, diferenciando claramente as informações públicas (objeto, valores, metas, entregas, execução financeira e indicadores agregados de produção, qualidade, ensino e pesquisa) dos dados individuais protegidos (pacientes, acompanhantes, familiares, participantes de pesquisa e, com ressalvas, profissionais). Sugerimos, também, consolidar diretriz geral sobre titulares vulneráveis — crianças, adolescentes, idosos, pessoas com deficiência, pacientes em vulnerabilidade clínica, vítimas de violência e portadores de doenças estigmatizantes — com presunção reforçada de proteção e análise caso a caso do melhor interesse, em especial de crianças e adolescentes (art. 227 da CF, ECA e art. 14 da LGPD). Sugestões abaixo:

“Nos instrumentos celebrados entre o Poder Público e instituições de saúde, a publicidade incide amplamente sobre objeto, valores, metas, entregas, prazos, execução financeira e resultados agregados. Tais informações não se confundem com os dados individuais de pacientes, acompanhantes, familiares e participantes de pesquisa, que, em regra, devem ser protegidos, salvo interesse público preponderante na identificação. Incluem-se nesse contexto, ainda, dados de natureza administrativa que possam permitir inferências sobre o estado de saúde dos titulares, como registros de controle de acesso a unidades assistenciais (por exemplo, listas de visitantes), os quais, em razão do contexto, demandam tratamento com salvaguardas equivalentes às aplicáveis a dados pessoais sensíveis. Sempre que a finalidade de controle social puder ser atendida por indicadores agregados, esta deve ser a forma preferencial de divulgação.

Adicionalmente, o tratamento e a eventual divulgação de dados de pessoas em situação de vulnerabilidade (crianças e adolescentes, idosos, pessoas com deficiência, pacientes em vulnerabilidade clínica, vítimas de violência e portadores de doenças estigmatizantes) exigem cautela reforçada. No caso de crianças e adolescentes, observa-se o melhor interesse (art. 227 da CF, ECA e art. 14 da LGPD), com presunção reforçada de proteção e divulgação preferencialmente agregada ou anonimizada. A identificação nominal só deve ocorrer quando indispensável e amparada em interesse público preponderante, devidamente motivado, e nunca quando puder gerar risco à vida, à segurança, à integridade ou à dignidade do titular.”

Ref.: Consulta Pública da ANPD e da CGU – Guia de Transparência e Proteção de Dados Pessoais

Apresentamos a seguir as nossas sugestões de contribuições à Consulta Pública sobre o Guia de Transparência e Proteção de Dados Pessoais ([aqui](#)), promovida pela Agência Nacional de Proteção de Dados (ANPD) e pela Controladoria-Geral da União (CGU).

Considerações Gerais

O Einstein Hospital Israelita (“Einstein”), entidade que atua em assistência, ensino, pesquisa, inovação e saúde digital, e que mantém colaboração com políticas públicas e com o Poder Público, apoia a iniciativa da CGU e da ANPD e reconhece a relevância do Guia para harmonizar a transparência pública e a proteção de dados pessoais. A contribuição busca aprimorar a clareza, a segurança jurídica e a aplicabilidade prática do documento, especialmente em contextos de saúde, pesquisa, inovação e tratamento de dados pessoais sensíveis. Parte-se das premissas de que a publicidade é a regra, de que a LGPD não cria sigilo e de que eventuais restrições se fundamentam na LAI.

Capítulo 1 — Direito de acesso à informação e seus limites

Sugerimos que o rol exemplificativo de sigilos legais (art. 22 da LAI) do capítulo 1.2 mencione expressamente o sigilo profissional, em especial o sigilo médico, por sua elevada relevância para a Administração Pública que custodia informações de saúde (redes públicas, perícias, programas e parcerias com instituições de saúde). Trata-se de sigilo legal típico, preservado pela LAI, que não se confunde com a (inexistente) criação de sigilo pela LGPD e que convive com o regime do art. 31. Sugere-se acrescentar:

“Sigilo profissional, inclusive o sigilo médico, protege informações confiadas em razão do exercício de profissão regulamentada, amparado, entre outros, no art. 154 do Código Penal, na Lei nº 12.842/2013 (exercício da medicina) e, quanto à guarda e confidencialidade de prontuários, na Lei nº 13.787/2018, constituindo exceção legítima ao acesso preservada pelo art. 22 da LAI.”

Capítulo 2 — Proteção de dados pessoais nos termos da LGPD

Apoiamos integralmente a afirmação de que a LGPD não cria hipóteses de sigilo, nem altera o rol de informações restritas. Sugerimos apenas reforçar, na parte final, que a complementaridade entre LAI e LGPD impõe, no tratamento para fins de transparência, a observância dos princípios da finalidade, necessidade, adequação, segurança e prestação de contas, o que é particularmente sensível quando há dados de saúde sob guarda pública ou compartilhados em parcerias.

Capítulo 3 — Proteção de dados pessoais prevista na LAI

Sugerimos a inclusão de um box específico sobre dados de saúde, reconhecendo que: (i) dados de saúde são dados sensíveis (art. 5º, II, e art. 11 da LGPD) e estão abarcados pela proteção da intimidade (art. 31 da LAI); (ii) prontuários e registros assistenciais sujeitam-se a sigilo profissional, que é sigilo legal preservado pelo art. 22 da LAI; e (iii) quando a identificação individual não for indispensável ao interesse público, deve-se preferir a divulgação agregada, anonimizada ou pseudonimizada. Quanto à pesquisa (item 3.3, alínea “d”), apoiamos o entendimento da ANPD de que a anonimização não é condição para o compartilhamento, mas sugerimos ressalva sobre o risco de reidentificação em bases clínicas, genômicas, biométricas, de doenças raras ou de alta granularidade, com remissão à governança ética da pesquisa (CEP/CONEP).

Box sugerido no Capítulo 3 ou no Capítulo 5:

“Dados de saúde são dados pessoais sensíveis (art. 5º, II, e art. 11 da LGPD) e estão abrangidos pela proteção da intimidade e da vida privada de que trata o art. 31 da LAI. Prontuários e registros assistenciais sujeitam-se, ainda, ao sigilo profissional, que constitui sigilo legal preservado pelo art. 22 da LAI. A presença de dados de saúde em documentos sob guarda pública ou em informações decorrentes de parcerias não impõe sigilo automático, mas exige análise reforçada de risco e a preferência, sempre que a identificação individual não for indispensável ao interesse público preponderante, pela divulgação agregada, anonimizada ou pseudonimizada. Indicadores agregados de produção, qualidade, cobertura e resultados assistenciais e de pesquisa devem ser divulgados; dados individuais de pacientes, acompanhantes, familiares e participantes de pesquisa, em regra, devem ser protegidos.”

Adicionalmente, sugerimos acrescentar, após o parágrafo que acolhe o entendimento da ANPD sobre anonimização:

“Em bases de alta granularidade, como dados clínicos detalhados, genômicos, biométricos, de imagens médicas, de doenças raras ou de coortes reduzidas, há risco concreto de reidentificação mesmo após pseudonimização. Nesses casos, recomenda-se análise reforçada de risco, a adoção de salvaguardas adicionais (controle de acesso, ambiente seguro, Termo de Responsabilidade e, quando cabível, dados sintéticos ou agregados) e a observância da governança ética da pesquisa, inclusive a aprovação pelo sistema CEP/CONEP, quando aplicável. A divulgação de resultados deve preferir formatos agregados que preservem o conteúdo científico sem expor titulares.”

Capítulo 4 — Garantindo a transparência com proteção dos dados pessoais

No Teste de Interesse Público (item 4.2, passo 3), sugerimos a inclusão de matriz orientativa de risco (probabilidade × impacto), com graduação em baixo, médio e alto, e de tipologia de danos a considerar: discriminação, estigmatização, fraude, constrangimento, reidentificação, dano reputacional, exposição indevida de condição de saúde e abalo da confiança no serviço público. A matriz é meramente orientativa e não substitui a análise qualitativa e casuística. Sugerimos, ainda, que o Guia trate expressamente dos pedidos de acesso relativos a sistemas de inteligência artificial, algoritmos e decisões automatizadas do Poder Público, privilegiando a transparência sobre finalidade, lógica geral, governança, métricas de desempenho, riscos e medidas de mitigação, sem expor dados pessoais, segredos legais, propriedade intelectual ou vulnerabilidades de segurança. Na transparência por desenho (item 4.3), sugerimos estender as boas práticas às entidades parceiras, mediante cláusulas de segregação prévia entre informação pública e protegida, metadados e trilhas de auditoria.

Sugerimos, adicionalmente, acrescentar à tabela de técnicas menos invasivas exemplos do setor de saúde:

- Agregação por faixa etária, sexo, município/região e período, para indicadores epidemiológicos e de produção assistencial, sem identificação dos titulares.
- Descaracterização de CPF (***.999.999-**) e tarjamento de identificadores diretos em documentos de parcerias e prestações de contas.
- Divulgação de quantitativos de atendimentos, procedimentos e beneficiários por unidade ou programa, em vez de listas nominais de pacientes.
- Uso de pseudonimização com chave controlada para acompanhamento de coortes em estudos, dispensando a identificação direta.

Capítulo 5 — Entendimentos sobre a publicidade de dados pessoais

Sugerimos a inclusão de subseção sobre dados de saúde em contratos, convênios e parcerias com o Poder Público, diferenciando claramente as informações públicas (objeto, valores, metas, entregas, execução financeira e indicadores agregados de produção, qualidade, ensino e pesquisa) dos dados individuais protegidos (pacientes, acompanhantes, familiares, participantes de pesquisa e, com ressalvas, profissionais). Sugerimos, também, consolidar diretriz geral sobre titulares vulneráveis — crianças, adolescentes, idosos, pessoas com deficiência, pacientes em vulnerabilidade clínica, vítimas de violência e portadores de doenças estigmatizantes — com presunção reforçada de proteção e análise caso a caso do melhor interesse, em especial de crianças e adolescentes (art. 227 da CF, ECA e art. 14 da LGPD). Sugestões abaixo:

“Nos instrumentos celebrados entre o Poder Público e instituições de saúde, a publicidade incide amplamente sobre objeto, valores, metas, entregas, prazos, execução financeira e resultados agregados. Tais informações não se confundem com os dados individuais de pacientes, acompanhantes, familiares e participantes de pesquisa, que, em regra, devem ser protegidos, salvo interesse público preponderante na identificação. Incluem-se nesse contexto, ainda, dados de natureza administrativa que possam permitir inferências sobre o estado de saúde dos titulares, como registros de controle de acesso a unidades assistenciais (por exemplo, listas de visitantes), os quais, em razão do contexto, demandam tratamento com salvaguardas equivalentes às aplicáveis a dados pessoais sensíveis. Sempre que a finalidade de controle social puder ser atendida por indicadores agregados, esta deve ser a forma preferencial de divulgação.

Adicionalmente, o tratamento e a eventual divulgação de dados de pessoas em situação de vulnerabilidade (crianças e adolescentes, idosos, pessoas com deficiência, pacientes em vulnerabilidade clínica, vítimas de violência e portadores de doenças estigmatizantes) exigem cautela reforçada. No caso de crianças e adolescentes, observa-se o melhor interesse (art. 227 da CF, ECA e art. 14 da LGPD), com presunção reforçada de proteção e divulgação preferencialmente agregada ou anonimizada. A identificação nominal só deve ocorrer quando indispensável e amparada em interesse público preponderante, devidamente motivado, e nunca quando puder gerar risco à vida, à segurança, à integridade ou à dignidade do titular.”

2. Direito à proteção de dados pessoais e da privacidade nos termos da Lei Geral de Proteção de Dados - LGPD

O item 2.1 precisa ser mais explicativo — e didático — no que tange à COLETA, que é o primeiríssimo passo para a existência e o funcionamento da LGPD. Embora o item anterior já esclareça que tratamento inclui coleta, o item 2.1 não parece capaz de destacar a importância desse tratamento inicial. Apenas por meio da lista em destaque do referido item (Finalidade, Adequação, Transparência, Segurança e Responsabilização/prestação de contas), não é possível notar que a coleta tem prioridade em relação a todas as demais formas de tratamento, as quais, no fim das contas, decorrem dela. O termo COLETA precisa ser mais destacado, sobretudo no tópico Necessidade.

O item 2.2, por sua vez, toca nessa ferida, mas apenas muito de leve. Ao reforçar que o regime jurídico especial da LGPD não permite ao poder público fugir de suas prerrogativas específicas (“[tratamento de] dados de forma proporcional, finalística e compatível com suas competências institucionais”), não se destaca aqui, novamente, que o tratamento inclui a COLETA.

Inúmeros órgãos e entidades públicos coletam dados que nenhuma relação possuem com suas naturezas públicas. Num mero formulário de “Fale conosco” ou numa ligação para alguma central de atendimento do governo, diversos são os dados demandados para que se preste o atendimento (incluindo dados sensíveis como raça e até mesmo orientação sexual!). Em se tratando do tópico Necessidade (item 2.1), órgãos e entidades públicos somente deveriam solicitar dados pessoais se estes fossem pertinentes à sua natureza pública — e isso deveria estar didaticamente mais claro no item 2.2.

Um caso real que ilustrará bem a questão: há alguns meses, tive de entrar em contato com o BCB. No formulário online, foi solicitada obrigatoriamente minha “data de nascimento” (incluindo DIA e MÊS). Ora, se a natureza pública do BCB é economia e finanças, por que se exige tal dado para um mero registro de “fale conosco”? Acaso seria para geração de estatísticas relacionadas a faixas etárias? Primeiro problema: não é de forma alguma pertinente à natureza do BCB gerar estatísticas de faixas etárias. Segundo problema: ainda que fosse para gerar estatísticas de faixas etárias, não se precisaria do dia, nem do mês de nascimento, senão apenas do ANO.

Embora este seja apenas um exemplo, inúmeros são os órgãos e entidades públicos que, num mero contato de atendimento ou em outras situações relacionadas, coletam dados pessoais que nenhuma relação possuem com as suas naturezas públicas. Ocorre, em consequência disso, que todos esses dados — desnecessariamente coletados — ficam em guarda do poder público, o qual, numa contradição inexplicável, passa a se anunciar muitíssimo sobrecarregado ante a responsabilidade de garantir a manutenção e proteção dos dados que ele próprio coletou de modo excessivo e, em diversos casos, abusivo.

O tratamento começa na COLETA. E é precisamente porque órgãos e entidades públicos insistem em coletar informações cuja qualidade não é pertinente às suas naturezas públicas que é preciso dar o máximo de destaque nos itens 2.1 e 2.2 a uma “didática da coleta”.

Diferença entre Pesquisa Processual e Publicação

Para adequada interpretação das disposições relativas à transparência administrativa e à proteção de dados pessoais, recomenda-se que a norma reconheça expressamente a diferença existente entre informações pessoais constantes de documentos acessíveis mediante consulta individualizada em processos administrativos e aquelas contidas em documentos submetidos à publicação oficial de ampla divulgação.

Embora ambas as situações possam envolver informações formalmente públicas, os impactos sobre a privacidade dos titulares não são equivalentes. A mera possibilidade jurídica de acesso não se confunde com a efetiva capacidade de localização, agregação, disseminação e reutilização da informação por qualquer pessoa. Por essa razão, a avaliação dos riscos associados ao tratamento de dados pessoais deve considerar não apenas o caráter público do documento, mas também as condições concretas de acesso à informação.

Nesse contexto, mostra-se particularmente relevante o conceito de **obscuridade prática** (*practical obscurity*), segundo o qual determinada informação pode ser considerada publicamente acessível sob o ponto de vista formal, mas permanecer, na prática, protegida contra exposição ampla em razão das limitações naturais, técnicas ou operacionais existentes para sua localização e obtenção. A proteção decorrente da obscuridade prática não resulta da restrição jurídica ao acesso, mas do fato de que a informação somente pode ser encontrada mediante busca específica, contextualizada e direcionada.

É o que ocorre com documentos inseridos em processos administrativos cuja consulta depende do conhecimento prévio de identificadores específicos, como número de processo ou de documento, associados, ainda, a mecanismos destinados a dificultar consultas automatizadas e extração massiva de dados. Nesses casos, o acesso exige iniciativa individual, está vinculado a um contexto administrativo determinado e não favorece, ordinariamente, a formação de grandes bases de dados pessoais nem a realização de atividades sistemáticas de mineração, cruzamento ou perfilhamento de informações.

A existência dessa obscuridade prática reduz significativamente o potencial de exposição dos titulares. Ainda que a informação possa ser consultada por terceiros, sua obtenção demanda esforço específico e conhecimento prévio de elementos de identificação, circunstância que limita naturalmente a escala de acesso e contribui para preservar o contexto original em que os dados foram produzidos e disponibilizados.

Situação substancialmente diversa ocorre quando informações pessoais são inseridas em documentos publicados em diários oficiais, boletins de serviço ou

outros meios destinados à divulgação ampla e geral dos atos administrativos. Nesses ambientes, a informação deixa de estar protegida pela obscuridade prática e passa a integrar um espaço de ampla visibilidade, caracterizado pela facilidade de acesso, pela indexação por mecanismos de busca, pela possibilidade de captura automatizada, pela replicação em múltiplas plataformas e pela permanência indefinida em repositórios digitais.

A transição de um ambiente de consulta contextualizada para um ambiente de divulgação ampla produz alteração qualitativa no nível de exposição dos dados pessoais. A informação que antes dependia de busca específica torna-se imediatamente disponível a um universo indeterminado de pessoas, podendo ser localizada por pesquisas simples, agregada a outras bases de dados e utilizada para finalidades diversas daquelas que justificaram originalmente sua disponibilização.

Por essa razão, não se mostra adequado atribuir tratamento regulatório idêntico a situações que apresentam riscos substancialmente distintos aos direitos dos titulares. A divulgação em meio de ampla publicidade potencializa riscos de reutilização indevida, monitoramento, perfilhamento, discriminação, fraude e descontextualização das informações, exigindo a adoção de salvaguardas mais rigorosas e de critérios mais restritivos para a exposição de dados pessoais.

Dessa forma, sugere-se que a regulamentação adote abordagem baseada no risco e reconheça expressamente que a forma de disponibilização da informação constitui elemento relevante para a definição das medidas de proteção aplicáveis. A análise não deve se limitar à classificação formal do documento como público, devendo considerar também fatores como grau de acessibilidade, potencial de indexação, possibilidade de coleta automatizada, alcance da divulgação e capacidade de circulação da informação fora de seu contexto original.

Tal entendimento permite conciliar, de maneira proporcional e equilibrada, os valores constitucionais da transparência administrativa e da proteção de dados pessoais. Além disso, evita a equiparação indevida entre acesso pontual e contextualizado a documentos administrativos e publicação oficial de ampla difusão, reconhecendo que a eliminação da obscuridade prática representa incremento significativo do risco à privacidade e, conseqüentemente, demanda maior cautela por parte da Administração Pública.

Procuração e Atos Constitutivos

Sugere-se que a norma estabeleça, como regra geral, a publicidade de procurações, atos constitutivos, documentos de representação, termos de designação e demais documentos apresentados para comprovação da qualificação das partes, representantes legais e procuradores nos processos administrativos, ressalvadas apenas as hipóteses excepcionais de restrição de acesso previstas em lei ou devidamente fundamentadas. Da mesma forma, recomenda-se que a norma esclareça expressamente que a anonimização ou o mascaramento de dados de qualificação constantes desses documentos não constitui medida necessária de forma geral quando mantidos nos autos administrativos.

A publicidade desses documentos encontra fundamento nos princípios da transparência, da publicidade administrativa e do controle social, uma vez que a identificação das partes e de seus representantes é elemento essencial para a verificação da legitimidade dos atos praticados perante a Administração, da regularidade da representação processual, da prevenção de fraudes, da identificação de eventuais conflitos de interesse e da adequada fiscalização da atuação estatal.

A avaliação da necessidade de restringir ou ocultar dados pessoais deve considerar não apenas a natureza da informação, mas também o contexto de sua disponibilização e os riscos efetivamente associados ao acesso. É importante distinguir os documentos mantidos em processos administrativos, normalmente acessados mediante consulta individualizada e relacionados a um contexto específico, daqueles disponibilizados em ambientes de ampla divulgação, como diários oficiais, portais de transparência ativa e bases abertas. Enquanto estes estão sujeitos à indexação por mecanismos de busca, coleta automatizada, agregação de bases de dados e reutilização em larga escala, os documentos inseridos em processos administrativos permanecem submetidos a barreiras naturais de acesso e localização, o que reduz significativamente os riscos à privacidade.

Nesse contexto, a mera presença de dados de qualificação, inclusive CPF, em documentos de representação ou habilitação processual não deve conduzir automaticamente à anonimização, ao mascaramento ou à restrição de acesso. A adoção indiscriminada dessas medidas desconsidera as diferenças de risco entre os diversos ambientes de disponibilização da informação, dificulta a rastreabilidade dos atos processuais, compromete a compreensão do histórico processual e cria obstáculos à verificação da regularidade da atuação dos agentes envolvidos.

Além disso, procurações, contratos sociais, atos constitutivos e demais documentos de representação são, em regra, produzidos e apresentados pelos próprios interessados, não pela Administração Pública. A exigência de anonimização sistemática desses documentos transfere à Administração o ônus permanente de editar documentos elaborados por terceiros, gerando custos operacionais relevantes, aumento da carga de trabalho administrativa e maior complexidade na gestão documental. Em muitos casos, essa exigência ainda impõe a manutenção simultânea de versões integrais e versões editadas dos mesmos documentos, ocasionando duplicação documental, riscos de inconsistência entre versões e ampliação desnecessária do volume de informações armazenadas.

Por essa razão, recomenda-se que a restrição de acesso, a anonimização ou o mascaramento sejam adotados apenas em situações excepcionais, quando houver fundamento legal específico ou demonstração concreta de risco decorrente da divulgação de determinada informação. Nesses casos, a proteção deve recair exclusivamente sobre os dados que efetivamente demandem tratamento diferenciado, mediante fornecimento de cópia parcial, extrato, certidão, tarja ou outro mecanismo de ocultação pontual, preservando-se a integridade do documento original constante dos autos.

Essa abordagem promove o adequado equilíbrio entre a proteção de dados pessoais e os princípios da publicidade, da transparência e do controle social, privilegiando uma análise baseada em risco e contexto. Ao mesmo tempo, assegura a legitimidade da representação processual, a segurança jurídica dos atos administrativos e o acesso às informações necessárias ao acompanhamento e à fiscalização da atuação da Administração Pública, sem impor restrições ou anonimizações generalizadas desnecessárias.

TRIBUNAIS DE CONTAS DO BRASIL

Encarregados de Dados e Estruturas de Governança em Proteção de Dados

CONTRIBUIÇÃO TÉCNICA CONJUNTA

Consulta Pública – Guia de Transparência e Proteção de Dados Pessoais

CGU/ANPD – Plataforma Brasil Participativo

Órgão	Tribunais de Contas do Brasil signatários desta contribuição
Responsáveis	Encarregados de Dados e estruturas de governança em proteção de dados dos respectivos Tribunais
Natureza do Documento	Contribuição técnica conjunta – Consulta Pública CGU/ANPD
Prazo da Consulta	21 de junho de 2026
Plataforma de Submissão	Brasil Participativo (participativo.brasil.gov.br)
Data	Junho de 2026

1. Identificação e Legitimidade

Os Tribunais de Contas brasileiros constituem instituições permanentes de controle externo da Administração Pública, com assento constitucional nos artigos 70 a 75 da Constituição Federal. Compete-lhes fiscalizar a aplicação de recursos públicos, julgar contas de administradores e responsáveis por dinheiros, bens e valores públicos, apreciar a legalidade dos atos de admissão de pessoal e de concessão de aposentadorias, reformas e pensões, aplicar sanções aos responsáveis, realizar inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial, e exercer demais atribuições essenciais à tutela do patrimônio público.

Os Encarregados de Dados e as estruturas de governança em proteção de dados das Cortes de Contas acompanham com atenção a elaboração do *Guia de Transparência e Proteção de Dados Pessoais* (CGU/ANPD, maio de 2026) e apresentam, por meio desta contribuição técnica conjunta, posição fundamentada sobre ponto específico da minuta que impacta diretamente a efetividade do controle externo: a diretriz de descaracterização do Número de Inscrição no Cadastro de Pessoas Físicas (CPF) nas publicações de órgãos públicos, sem ressalva para as decisões e acórdãos com eficácia jurídica específica proferidos pelas Cortes de Contas.

2. Síntese da Questão e do Conflito Normativo

2.1. A diretriz geral do Guia

O Guia, em suas tabelas exemplificativas (itens 4.2 e 5), recomenda sistematicamente que o CPF de agentes públicos, fornecedores e beneficiários seja publicado de forma descaracterizada (***.999.999-**), com o objetivo de minimizar o risco de fraudes ao titular e atender ao princípio da necessidade previsto no art. 6º da Lei Geral de Proteção de Dados Pessoais (LGPD). Trata-se de orientação tecnicamente justificável como regra geral para publicações de transparência ativa em portais governamentais que, todavia, traz aspectos discrepantes quando aplicada a atos e decisões proferidos pelos Tribunais de Contas.

2.2. O conflito com as publicações das Cortes de Contas

As publicações dos Tribunais de Contas não se confundem com as publicações de transparência ativa ordinária. As decisões e acórdãos proferidos no exercício das competências constitucionais possuem espécies com exigências de identificação especialmente rigorosas, em especial:

- Decisões de atos de pessoal (art. 71, III, CF/88): deliberações sobre legalidade de admissões, aposentadorias, reformas e pensões, cujo registro funcional e de identificação do responsável é pressuposto de validade e eficácia perante os órgãos destinatários — inclusive para fins de registro no SIAPE e nos sistemas previdenciários.
- Decisões condenatórias com eficácia de título executivo (art. 71, §3º, CF/88): acórdãos de imputação de débito ou multa e listas de responsáveis com contas julgadas irregulares, cujos destinatários não são apenas o cidadão-controlador social, mas também órgãos executores que dependem da identificação inequívoca e correta do responsável para produzir os efeitos legais das sanções — Procuradorias, Justiça Eleitoral e SERASAJUD.
- Acórdãos de julgamentos de contas (art. 71, CF/88): atos decisórios colegiados proferidos na apreciação e no julgamento de processos de prestação de contas em que são apreciados os atos dos responsáveis pela aplicação de recursos públicos, sujeitos à jurisdição dos Tribunais de Contas.

Diversas Cortes de Contas brasileiras já consolidaram normativos internos reconhecendo a necessidade do registro do CPF na sua integralidade, sem qualquer técnica de mascaramento ou de descaracterização, tendo em vista a exigência de identificação inequívoca dos responsáveis nessas categorias de decisão, em consonância com o entendimento firmado pelo Tribunal de Contas da União na Resolução nº 354/2023.

Para a identificação inequívoca de um responsável é necessário o nome completo em conjunto com o CPF integral, dada a existência de homônimos, que não são afastados somente com o CPF descaracterizado. A aparente individualização conseguida com a publicação do nome completo somado ao CPF mascarado, segundo a forma

***.999.999-**, não ocorre de fato. É possível encontrar homônimos em tal forma de descaracterização, ou seja, pessoas diferentes que têm o mesmo par nome completo mais CPF mascarado no formato ***.999.999-**. Ao fazermos teste computacional sobre bases de dados do Tribunal de Contas da União, ficou constatado que é possível encontrar a quantidade de 135.631 homônimos¹.

A ausência de ressalva expressa no Guia para essas hipóteses cria risco concreto de insegurança jurídica: gestores e jurisdicionados poderão invocar o documento da CGU/ANPD — com o peso institucional que lhe é inerente — para contestar a regularidade das publicações das Cortes de Contas, sobrepondo uma diretriz de transparência geral a competências expressamente atribuídas pela Constituição Federal.

3. Fundamentação Jurídica da Exceção Pleiteada

3.1. Fundamento constitucional e da LAI

A competência constitucional das Cortes de Contas decorre dos artigos 70 a 75 da Constituição Federal. Destacam-se, para os fins desta contribuição, dois incisos do art. 71: o inciso III, que atribui ao Tribunal de Contas competência para apreciar a legalidade dos atos de admissão de pessoal e de concessão de aposentadorias, reformas e pensões; e o §3º, que confere eficácia de título executivo extrajudicial às decisões das quais resulte imputação de débito ou multa.

A identificação inequívoca do responsável é pressuposto lógico e jurídico da eficácia de ambas as categorias de decisão. No caso das decisões condenatórias, não há como executar um título cujo devedor não esteja plenamente individualizado. No caso das decisões sobre atos de pessoal, a ausência do CPF integral compromete o registro nos sistemas de controle de pessoal e o cumprimento das determinações pelos órgãos destinatários.

A divulgação do CPF de responsável sujeito à jurisdição do TCU permite à sociedade identificar e conhecer exatamente quem gerenciou de determinada maneira os recursos públicos. Portanto, não pode o Estado, sobre o pretexto de proteger dado pessoal de responsável, restringir o controle social, próprio das democracias.

A identificação da pessoa que teve as contas julgadas é informação imprescindível para que o direito de acesso à informação do cidadão (art. 5º, XXXIII) seja plenamente atendido. A existência do CPF visa exatamente a este ponto, eis que o objetivo do Cadastro é justamente o de individualizar pessoas físicas, de forma que se tornem identificáveis.

Não apenas o direito constitucional do acesso à informação (art. 5º, XXXIII), mas também seu corolário da transparência na gestão da coisa pública, o princípio republicano, da prestação de contas (art. 70, parágrafo único), da participação do

¹ Da análise realizada em nossas bases de dados em 27/4/2021, foram identificadas as seguintes quantidades de repetições do par CPF mascarado + nome: 1 – 258.019.466; 2 – 129.660; 3 – 5.352; 4 – 564; e 5 – 55. Se a repetição é igual a 1, então o par CPF mascarado e nome é único.

usuário na administração pública (art. 37, §3º, II e III), e o princípio da publicidade (art. 37, caput) autorizam a divulgação de dados pessoais, como, vide decisões da Corte Suprema², prevalecem sobre o direito à vida privada, intimidade, quando se trata de agentes públicos.

Avançando no direito de acesso à informação pelo cidadão, a LAI reconhece expressamente o direito do cidadão de obter o resultado não só da prestação de contas, mas também de inspeções e auditorias (art. 7º, III, b). O resultado dessa prestação de contas não se limita ao julgamento pela regularidade, regularidade com ressalva ou irregularidade, mas também a quem deu causa ao resultado, dada a obrigação personalíssima da prestação de contas e do julgamento das contas, exigindo, inclusive, a identificação de quem tenha demonstrado a boa e regular aplicação dos recursos públicos.

A própria LAI permite a integral divulgação de dados pessoais, incluído o CPF, quando houver, entre outros casos, a necessidade de proteção do interesse público e geral preponderante, conforme inc. V, do §3º, do art. 31, dispensando a necessidade do consentimento expresso da pessoa a quem os dados se referem.

A ocultação parcial do número do CPF dos responsáveis sujeitos à jurisdição dos Tribunais de Contas caracteriza prejuízo aos princípios constitucionais da transparência, da prestação de contas e da accountability na administração pública, pois a sociedade não se mantém capaz de associar o resultado de determinado julgamento das Cortes de Contas à exata pessoa física que lhe deu causa e nem de conhecer o histórico de atuação do responsável no trato da coisa pública.

3.2. Fundamento na própria LGPD e no Guia

O art. 7º, II, da LGPD autoriza o tratamento de dados pessoais para cumprimento de obrigação legal ou regulatória pelo controlador. O art. 23 estabelece regime diferenciado para o Poder Público, admitindo o tratamento de dados pessoais para o atendimento de finalidade pública legítima.

Ao abordar o tratamento dos dados pessoais pelo poder público (Capítulo IV), a LGPD admitiu a necessidade de divulgação de dados pessoais quando, expressamente reconheceu o direito do acesso dos dados pelo público em geral: “art. 25 - Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral”. O próprio Guia, em seu item 3.3(b), reconhece que o acesso a dados pessoais pode ocorrer mediante previsão legal — hipótese que dispensa consentimento do titular. As normas constitucionais e legais que estruturam a competência das Cortes de Contas constituem precisamente essa previsão legal específica.

² BRASIL. Supremo Tribunal Federal. ARE 652.777/SP. Plenário. Relator Ministro Teori Zavascki. Julgado em 23 de abril de 2015 e Agr MS 3.3902 MC-REF/DF. Plenário. Relator Ministro Ayres Britto. Julgado em 3 de outubro de 2011.

Ademais, o Enunciado CGU nº 12/2023 — referenciado no próprio Guia — é explícito: a proteção de dados pessoais "*pode ser flexibilizada quando, no caso concreto, a proteção do interesse público geral e preponderante se impuser*". A identificação de responsáveis por irregularidades no erário e a eficácia das decisões de controle externo são paradigma de interesse público preponderante, enquadrado pelos próprios critérios do Teste de Interesse Público constantes do Guia: combate à corrupção, verificação de probidade administrativa e controle social do uso de recursos públicos.

Reforça esse entendimento o *Guia Ouvidoria e Transparência: como a LAI e a LGPD fortalecem o Controle Social* (TCE-MS, setembro de 2025), que reconhece expressamente a complementaridade entre transparência, proteção de dados e efetividade do controle social — inclusive no âmbito dos órgãos de controle externo. A presente contribuição está alinhada a esse espírito: não se busca afastar a LGPD, mas aplicá-la de forma constitucionalmente adequada.

3.3. Fundamento na Lei nº 14.534/2023 e nos precedentes das Cortes de Contas

A Lei Federal nº 14.534/2023 instituiu o CPF como número único de identificação do cidadão nos bancos de dados de serviços públicos, consolidando sua função como identificador inequívoco em relações jurídicas com o Estado. A descaracterização do CPF em acórdãos condenatórios e em decisões de atos de pessoal prejudicaria diretamente a comunicação entre as Cortes de Contas e os órgãos que dependem dessa identificação para produzir os efeitos práticos das decisões:

- A Procuradoria-Geral da União e a Procuradoria-Geral do Estado (e congêneres estaduais) na execução fiscal dos acórdãos de imputação de débito;
- a Justiça Eleitoral, na declaração de inelegibilidade de responsáveis condenados, nos termos do art. 1º, I, g, da Lei Complementar nº 64/1990;
- o SERASAJUD e demais sistemas de consulta de adimplência que utilizam o CPF como chave de identificação do devedor;
- os sistemas de controle de pessoal (SIAPE e equivalentes estaduais) nos quais as decisões sobre atos de pessoal precisam ser registradas com identificação integral do servidor.

Esse entendimento já está consolidado na prática de múltiplas Cortes de Contas brasileiras. O Tribunal de Contas da União firmou posição expressa na Resolução nº 354/2023, determinando a publicação do CPF integral nos acórdãos. Diversos Tribunais de Contas estaduais adotaram normativos internos no mesmo sentido. A publicação do Guia sem ressalva expressa criaria contradição entre a orientação nacional e a prática institucional normatizada e já sedimentada no Sistema de Controle Externo.

3.4. A distinção essencial: transparência geral × publicação com eficácia jurídica

O Guia não diferencia dois contextos que possuem naturezas jurídicas radicalmente distintas:

- Publicações de transparência ativa ordinária: divulgação de dados em portais governamentais para fins de controle social difuso, onde a minimização de dados — incluindo a descaracterização do CPF — é plenamente justificável e deve ser a regra.
- Publicações com eficácia jurídica específica: decisões sobre atos de pessoal e acórdãos condenatórios das Cortes de Contas, cujos efeitos jurídicos não se esgotam na transparência pública, mas produzem consequências executivas e registrais que exigem identificação integral do responsável.

A ausência de diferenciação entre esses dois contextos é a raiz do conflito. A ressalva pleiteada não excepciona a proteção de dados pessoais; ela aplica o próprio princípio da adequação (art. 6º, II, LGPD), segundo o qual o tratamento de dados deve ser compatível com a finalidade informada. A finalidade de um acórdão condenatório ou de uma decisão sobre ato de pessoal é juridicamente diversa da finalidade de um portal de transparência — e a adequação exige tratamentos também distintos.

4. Proposta Concreta de Contribuição ao Guia

Com base na fundamentação exposta, propõe-se a inclusão das seguintes modificações na versão final do Guia CGU/ANPD:

4.1. Inclusão de ressalva nas tabelas do Capítulo 5

Sugere-se que, nas tabelas exemplificativas em que o Guia indica que o CPF deve ser descaracterizado (agentes públicos, representantes legais de fornecedores e congêneres), seja acrescentada a seguinte nota de exceção:

EXCEÇÃO — Tribunais de Contas e órgãos com poder sancionador: A presente diretriz de descaracterização não se aplica às publicações de atos, decisões e acórdãos proferidos no exercício de suas competências constitucionais (art. 71, CF/88). A publicação do CPF em sua integralidade é condição para o amplo exercício do controle social e para a eficácia de decisões sobre atos de pessoal, acórdãos condenatórios e listas de responsáveis com contas julgadas irregulares proferidas pelos Tribunais de Contas, bem como quaisquer atos administrativos com natureza de título executivo ou com destinação específica a órgãos de execução extrajudicial (Procuradorias, Justiça Eleitoral, SERASAJUD e sistemas de controle de pessoal), com fundamento no art. 71, III e §3º, da CF/88, nos arts. 7º, II, e 23 da LGPD e na Lei Federal nº 14.534/2023.

4.2. Inclusão de subtópico específico no Capítulo 5

Sugere-se a criação de subtópico no Capítulo 5 do Guia, intitulado "Dados pessoais em decisões dos Tribunais de Contas e órgãos com poder sancionador", com o seguinte conteúdo mínimo:

Tipo de informação	Regra de divulgação	Observações
CPF em acórdãos ou lista de responsáveis inabilitados ou	Publicação integral	Necessário para o controle social e para a eficácia de títulos executivos.

com contas julgadas irregulares		Fundamento: art. 71, §3º, CF/88 e Lei nº 14.534/2023.
CPF em decisão sobre ato de pessoal (admissão, aposentadoria, reforma, pensão)	Publicação integral	Condição de eficácia processual e de registro nos sistemas de controle de pessoal. Fundamento: art. 71, III, CF/88; Lei nº 14.534/2023.
Nome e cargo do responsável condenado ou do servidor em ato de pessoal	Deve ser publicado	Informação funcional diretamente vinculada ao exercício da função pública e ao objeto da decisão.
Descrição da irregularidade, valor do débito ou fundamento da decisão de pessoal	Deve ser publicado	Essencial ao controle social e à execução ou cumprimento da decisão.
Dados de saúde, familiares ou bancários do responsável	Não deve ser publicado	Dados da vida privada sem relação com a irregularidade apurada ou com o ato de pessoal.
CPF em publicações de transparência ativa ordinária (portais, relatórios gerenciais)	Descaracterizado (**.999.999-**))	Segue a regra geral do Guia. A exceção aplica-se exclusivamente aos atos com eficácia jurídica específica.

4.3. Inclusão de nota metodológica no Teste de Interesse Público (item 4.2)

Sugere-se que o Teste de Interesse Público inclua, após a listagem dos exemplos de interesse público preponderante (passo 2), a seguinte observação:

Nota metodológica: O presente Teste destina-se primariamente à análise de pedidos de acesso à informação e de publicações em transparência ativa de caráter geral. Não se aplicam, nem deve ser invocadas para restringir, publicações decorrentes de competências constitucionais ou legais específicas de órgãos de controle externo cujo fundamento de divulgação é a eficácia jurídica do ato e não o princípio da transparência voluntária. Nessas hipóteses, a base legal do tratamento de dados é o art. 7º, II, da LGPD (cumprimento de obrigação legal ou constitucional), de modo que a análise de interesse público preponderante é presumida pela própria Constituição Federal.

5. Impacto Sistêmico sobre o Sistema de Controle Externo Brasileiro

Esta contribuição expressa preocupação institucional compartilhada pelas Cortes de Contas brasileiras — federal, estaduais e dos municípios —, signatárias deste documento técnico, cujas competências constitucionais são exercidas de forma uniforme em todo o território nacional. O conflito identificado não é particularidade de um único Tribunal: ele afeta, de forma idêntica, todo o Sistema de Controle Externo.

Os riscos práticos da omissão do Guia incluem:

- Prejuízo ao controle social, ao direito constitucional do acesso à informação (art. 5º, XXXIII), bem como a seu corolário da transparência na gestão da coisa pública, e também ao princípio republicano, da prestação de contas (art. 70,

parágrafo único), da participação do usuário na administração pública (art. 37, §3º, II e III), e da publicidade (art. 37, caput).

- Contestação judicial das publicações pretéritas dos Tribunais de Contas por responsáveis condenados, invocando o documento da CGU/ANPD como fundamento para exigir o mascaramento do próprio CPF em acórdão que os condena ao ressarcimento ao erário.
- Comprometimento da eficácia das comunicações à Justiça Eleitoral para fins de declaração de inelegibilidade, que dependem da identificação integral do responsável nos termos do art. 1º, I, g, da Lei Complementar nº 64/1990.
- Comprometimento de ação de execução fiscal de título executivo extrajudicial pela Procuradoria-Geral da União, que requer a identificação do devedor com seu CPF na integralidade.
- Dificuldade na execução fiscal pelas Procuradorias-Gerais dos Estados, cujos sistemas de cobrança e de bloqueio judicial identificam o devedor pelo CPF completo.
- Ruptura nos registros de decisões sobre atos de pessoal nos sistemas de controle de pessoal (SIAPE e equivalentes estaduais), comprometendo a rastreabilidade e o cumprimento das determinações pelos órgãos de origem.
- Insegurança jurídica para as Cortes de Contas que, diante da omissão do Guia, precisarão emitir pareceres jurídicos internos justificando o afastamento da diretriz geral — gerando retrabalho e inconsistência entre Tribunais.

A inclusão das ressalvas propostas é tecnicamente simples, não compromete o objetivo geral do Guia e resolve de forma definitiva um conflito que, na ausência de norma expressa, tenderá a multiplicar-se em recursos administrativos e ações judiciais em todo o Brasil.

6. Conclusão

Os Encarregados de Dados e as estruturas de governança em proteção de dados dos Tribunais de Contas brasileiros reiteram seu compromisso com a efetiva implementação da LGPD e com os objetivos do Guia elaborado pela CGU e pela ANPD.

A presente contribuição não busca afastar a diretriz geral de minimização e descaracterização de dados pessoais nas hipóteses ordinárias de transparência ativa — diretriz que é tecnicamente correta e deve ser preservada. O que se reivindica é que o Guia reconheça expressamente a singularidade constitucional das decisões proferidas pelas Cortes de Contas que, por sua natureza jurídica, exigem identificação integral do responsável como pressuposto de eficácia — e não como excesso de exposição de dados.

A inclusão das ressalvas propostas contribuirá para harmonizar transparência, proteção de dados pessoais, segurança jurídica e efetividade do controle externo, evitando interpretações conflitantes e assegurando tratamento uniforme em todo o Sistema de Controle Externo brasileiro.

Junho de 2026

Encarregados de Dados e Estruturas de Governança em Proteção de Dados dos Tribunais de Contas Brasileiros

Contribuição Técnica Conjunta à Consulta Pública CGU/ANPD

<i>Mônica Cotrim Chaves Encarregada de Dados do Tribunal de Contas da União (TCU)</i>	<i>Ana Carla Lemes Brum de Oliveira Encarregada de Dados Adilson Viegas de Freitas Junior Encarregado de Dados Substituto Tribunal de Contas do Estado do Mato Grosso do Sul (TCE-MS)</i>
<i>Morgana Bellazzi e Oliveira Carvalho Encarregada de Dados do Tribunal de Contas do Estado da Bahia (TCE-BA)</i>	<i>Hilda da Fonseca Duarte Caetano Encarregada de Dados do Tribunal de Contas do Estado do Pará (TCE-PA)</i>
<i>Francisco Raildo Cardoso Leitao Encarregado de Dados do Tribunal de Contas do Estado do Acre (TCE-AC)</i>	<i>Matheus Gustavo de Medeiros Batista Encarregado de Dados do Tribunal de Contas do Estado de Santa Catarina (TCE-SC)</i>
<i>Evaldo Luís Moreno Silva Encarregado de Dados do Tribunal de Contas do Estado do Paraná (TCE-PR)</i>	<i>Luís Eduardo Pires de Oliveira Vieira Encarregado de Dados do Tribunal de Contas dos Municípios do Estado de Goiás (TCM-GO)</i>
<i>Teotônio Barbosa de Santana Encarregado de Dados do Tribunal de Contas dos Municípios do Estado da Bahia (TCM-BA)</i>	<i>Márcia Soares Marques Encarregada de Dados do Tribunal de Contas do do Estado do Rio Grande do Norte (TCE-RN)</i>
<i>Maria Fernanda P. Toledo Weissman Encarregada de Dados do Tribunal de Contas do Município de São Paulo (TCM-SP)</i>	<i>Cássio Costa Filho Encarregado de Dados do Tribunal de Contas do Distrito Federal (TCDF)</i>

Referências Normativas

- Constituição Federal de 1988, arts. 5^a, 37 e 70-75 (sistema de controle externo), Lei Federal nº 12.527/2011 – Lei de Acesso à Informação (LAI), arts. 3º, 7º e 31.
- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), arts. 6º, 7º, II, 11, II, a, e 23.
- Lei Federal nº 14.129/2021 – Lei de Governo Digital, art. 29.
- Lei Federal nº 14.534/2023 – CPF como identificador único nos bancos de dados de serviços públicos.
- Lei Complementar Federal nº 64/1990, art. 1º, I, g – inelegibilidade por condenação em Tribunal de Contas.
- Decreto Federal nº 7.724/2012, arts. 13 e 55.
- Lei Federal nº 8.443/1992 - Lei Orgânica do Tribunal de Contas da União.
- Resolução TCU nº 354/2023 – publicação de CPF integral nos acórdãos do Tribunal de Contas da União.
- Enunciado CGU nº 12/2023 – proteção de dados pessoais e interesse público preponderante.
- Enunciado CGU nº 4/2022 – aplicação da LAI em pedidos sobre dados de pessoas naturais.
- CGU/ANPD. Guia de Transparência e Proteção de Dados Pessoais. Brasília, maio de 2026 (versão em consulta pública).
- TCE-MS. Guia Ouvidoria e Transparência: como a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD) fortalecem o Controle Social, (TCE-MS- setembro de 2025).
- IN TCE-MS nº 35/2024 – Dispõe sobre a publicação do CPF em decisões e Acórdãos do TCE-MS.

3. Proteção de dados pessoais prevista na LAI

No item 3.1, o quadro intitulado “IMPORTANTE” carece de complementação. Se o Guia é direcionado ao poder público, soa redundante destacar unicamente que o dado pessoal não pertence ao Estado — disso, não há quem não saiba. Falta acrescentar em que medida tal destaque é “crucial”: é crucial por quê? Quais limitações e/ou obrigações isso gera para quem custodia o dado? Caso se opte por não acrescentar essas complementações, é mais conveniente alterar o título do quadro para “LEMBRETE” apenas.

CONCEITO DE INTIMIDADE

Ainda no item 3.1, no segundo quadro (Intimidade, Vida Privada, Honra e Imagem), creio haver alguma má interpretação do conceito de Intimidade. Evidentemente, o conceito inserido neste Guia deve possuir origem oficial e, portanto, talvez não seja possível atualizá-lo aqui. Ainda assim, é importante esclarecer que a divulgação da intimidade não depende de consequências, como o conceito aqui descrito faz parecer. A simples divulgação da intimidade já é em si mesma um ato punível, independente daquilo que vier ou não a decorrer do vazamento. O que pode estar em jogo e ficar aberto a controvérsias é até que ponto o dado vazado efetivamente é íntimo. Confirmada a intimidade, já há a punição. Não há que se demonstrar se houve ou não “prejuízo(s)”.

HARMONIZAÇÃO DE PARÂMETROS E MÉTODO DE ENTREGA DE DADOS AO TITULAR

O item 3.2 deveria estar mais desenvolvido no que concerne à forma como órgãos e entidades devem fornecer tais informações. Muito destaque se dá à verificação da identidade do solicitante, a fim de confirmar a titularidade dos dados pessoais ao quais ele pede acesso. No entanto, a estrada da segurança não parece ter mão dupla: quando da entrega desses dados ao titular, o poder público não segue nem parâmetros (cada um age como lhe convém), nem método (cada um se vale de mecanismos distintos). A minha experiência com esse tipo de solicitação exemplifica bem o problema: após solicitar envio de dados pessoais que estavam sob guarda de certa autarquia, fui surpreendido com o envio dos dados via nuvem da empresa americana Hotmail!!! Embora pareça inacreditável, foi o que ocorreu. A desculpa da autarquia foi que o tamanho do arquivo era muito grande, impedindo seu envio por meio de sistema público. Desnecessário dizer que tudo o que carregamos na nuvem fica retido no servidor e/ou nos bancos de dados da empresa dona da nuvem.

Onde falta harmonia de parâmetros e método, sobra criatividade. No entanto, ser criativo no trato de dados alheios não é recomendável. Diante disso, é evidente a necessidade de harmonizar parâmetros e método de entrega de dados pessoais. Não havendo como encaminhar através de sistema público, que se envie por encomenda, com gravação em CD — mesmo que o custo fique a cargo do solicitante (possibilidade que em nada contraria a LAI ou a LGPD).

DADOS PROTEGIDOS *versus* ESTATÍSTICAS E PESQUISAS

O tópico “D” (Estatísticas e Pesquisas), do item 3.3, demonstra bem o que ocorre quando o poder público — que coleta dados indiscriminada e, muitas vezes, irresponsavelmente — não se mostra capaz de gerenciar, de maneira unificada, os dados sob sua guarda. Este Guia faz referência a outro Guia precisamente num dos pontos que é o tendão de Aquiles tanto da LGPD quanto da LAI: circunstâncias, ou “brechas”, que permitem ao poder público dispor dos dados que ele coletou (os quais, na maioria dos casos, jamais deveriam estar sob sua guarda). Esse subterfúgio legal é, sem dúvida, o pretexto utilizado por 11 em cada 10 órgãos e entidades de governo quando são ameaçados com qualquer possibilidade de perder o controle sobre os dados que coletaram. Nem mesmo solicitações de impedimento de tratativa são acatados com base nesse pretexto legal: para o poder público — e para as empresas privadas que trabalham em nome dele —, todo e qualquer dado pessoal pode ser tratado à revelia do titular, desde que seja para o interesse de todos e para o bem geral da nação...

Não bastasse essa falha da LGPD, este Guia ainda promove uma “dobradinha” com a LAI, fazendo parecer que, mesmo dados protegidos, são automaticamente desprotegidos para as mesmas finalidades — finalidades estas que serão acatadas sempre: sempre o poder público decidirá que dados pessoais, mesmo protegidos, poderão ser divulgados, porque disso dependem os bons rumos do bem-estar social e a obrigação para com a coletividade. Em suma, não apenas a brecha na LGPD e na LAI viabiliza que o poder público retenha dados à revelia do titular, como lhe dá a autorização para divulgar esses dados sob pretextos da ciência.

Mas há algo ainda mais incoerente neste ponto. Este mesmo Guia já versou sobre como uma informação pode ser negada, caso seu fornecimento exija trabalho exagerado do poder público. No entanto, nesta letra “D”, a tal restrição desaparece. Afinal, ao solicitar dados para estatísticas e pesquisas, fica patente que o solicitante exigirá do órgão/entidade muito mais do que é possível fornecer, haja vista o volume de dados necessários para a empreitada.

Imaginemos uma empresa que pretende compilar uma estatística, quantificando e qualificando as mulheres negras brasileiras que pariram o primeiro filho antes dos 18 anos. Ora, o trabalho e o custo para qualquer órgão/entidade do poder público agregar tais dados serão exorbitantes! Será, então, que se negaria o pedido de informação? Obviamente, não. Do contrário, constariam na letra “D” as limitações quanto aos protocolos da LAI que tratam de Estatísticas e Pesquisas. Aliás, na letra “D”, deixar-se-ia clara a indeferibilidade de praticamente todo pedido de informação com finalidade de estatística ou pesquisa, devido ao volume da demanda. Não é, contudo, o que lemos. Ao contrário, dando provas da descentralização do governo federal no assunto tratamento de dados, este Guia cita outro Guia, para avisar que, mesmo se o dado solicitado for protegido, ele poderá ser desprotegido sem qualquer problema, bastando o solicitante comprovar que o uso será científico.

Primeiro de tudo, neste Guia não deveria haver citação de outro Guia. O poder público não pode permitir que um único assunto seja normatizando, regularizado, formulado, reformulado etc. por mais de uma autoridade. É fundamental que uma regulação seja anulada assim que houver liberação de nova regulação, ou

que, pelo menos, as regulações se fundam numa só — reforçando para o povo a ideia de unidade federal —, gerando uma nova norma mais ampla (ou mais enxuta) e mais atualizada.

Ainda sobre esta malfada letra “D”, para evitar desproporções e incoerências, dever-se-ia:

1º Reforçar, neste Guia, a necessidade de órgãos e entidades de governo coletarem unicamente o dado que seja condizente com suas naturezas públicas. Aliás, é isso o que a lei determina, que o tratamento (a coleta inclusa) deve ocorrer dentro das finalidades do referido poder. Isso, hoje, não é realidade em larga escala federal e, conseqüentemente, nas demais esferas.

2º Trazer a letra “D” (Estatísticas e Pesquisas) para dentro da realidade legal, instruindo órgãos e entidades de governo que, da mesma forma como eles devem coletar apenas dados pertinentes à sua natureza pública, da mesma forma é que devem divulgá-los: a análise de protocolos da LAI com finalidade científica precisa pautar-se na finalidade do próprio órgão/entidade que fornecerá ou não a informação. Hoje, por conta da variedade de dados aleatórios e sem finalidade armazenados pelo poder público, é praticamente impossível a órgãos e entidades negarem-se a divulgar dados que, na verdade, eles nem sequer deveriam ter coletado.

A viabilidade do ponto nº 2 depende da execução do ponto nº 1.



Associação Brasileira de Governança de Dados

CONTRIBUIÇÃO À CONSULTA PÚBLICA

Guia de Transparência e Proteção de Dados Pessoais

Controladoria-Geral da União (CGU) • Agência Nacional de Proteção de Dados (ANPD)

Subsídios técnicos, análise regulatória comparada e propostas de aprimoramento

Apresentada por

govDADOS — Associação Brasileira de Governança de Dados

Conselho de Administração

Plataforma Brasil Participativo — Processo “guiadadospessoais”

Brasília/DF — junho de 2026

Sumário

Sumário.....	2
1. Apresentação e identificação do proponente.....	3
2. Sumário executivo	3
3. Metodologia e escopo	4
4. Análise crítica e propositiva do Guia.....	5
4.1. Capítulo 1 — Direito de acesso e seus limites	5
4.2. Capítulo 2 — Regime da LGPD e complementaridade com a LAI	5
4.3. Capítulo 3 — Proteção de dados pessoais prevista na LAI	5
4.4. Capítulo 4 — Roteiro decisório, Teste de Interesse Público e transparência por desenho	6
4.5. Capítulo 5 — Entendimentos sobre a publicidade de dados pessoais	7
5. Análise regulatória comparada	9
5.2. Estados Unidos — o teste de ponderação e a “obscuridade prática”	9
5.3. União Europeia — conciliação por desenho normativo	10
5.4. China — modelo estatocêntrico	10
5.5. Demais referências asiáticas — padrões técnicos e um alerta.....	11
6. A Resolução CONARQ nº 54/2023 e sua interface com o Guia.....	12
6.1. Síntese da Resolução	12
6.2. Por que importa para o Guia	12
6.3. Propostas de redação	12
7. Pontos não abordados pelo Guia e propostas adicionais.....	14
7.1. Interface com o regime arquivístico	14
7.2. Dados de pessoas falecidas	14
7.3. Tratamento automatizado e inteligência artificial	14
7.4. Padrões técnicos de anonimização e risco de reidentificação	14
7.5. Proteção reforçada de crianças e adolescentes (ECA Digital)	15
7.6. Gestão documental e papel do arquivista	15
7.7. Prazos de restrição versus arquivos permanentes	15
7.8. Incidentes de segurança e cadeia de comunicação	15
7.9. Reuso de dados abertos e transferência internacional	16
8. Quadro-resumo das sugestões.....	17
9. Conclusão e encaminhamento	19
Anexo — Referências normativas e fontes.....	20

1. Apresentação e identificação do proponente

A **govDADOS — Associação Brasileira de Governança de Dados** é entidade da sociedade civil, sem fins lucrativos, dedicada à promoção das boas práticas de governança de dados, proteção de dados pessoais e transparência pública no Brasil. Por meio de seu Conselho de Administração, a govDADOS submete a presente contribuição à Consulta Pública conduzida conjuntamente pela **Controladoria-Geral da União (CGU)** e pela **Agência Nacional de Proteção de Dados (ANPD)** sobre o *Guia de Transparência e Proteção de Dados Pessoais* (versão de maio de 2026), disponibilizada na plataforma Brasil Participativo.

A entidade reúne profissionais com atuação no setor público e privado — entre os quais analistas legislativos, arquivistas, advogados e encarregados de proteção de dados (DPO) — e tem interesse legítimo e qualificado no aperfeiçoamento de um instrumento orientativo cuja audiência abrange a integralidade da Administração Pública. O Guia tem mérito considerável: enfrenta com clareza a falsa antinomia entre a **Lei de Acesso à Informação (Lei nº 12.527/2011 — LAI)** e a **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 — LGPD)**, consolida entendimentos da CGU e estrutura um roteiro decisório útil. As contribuições a seguir partem do reconhecimento dessas qualidades e visam a robustecer o documento sob três eixos: (i) precisão técnico-jurídica; (ii) aderência às melhores práticas regulatórias internacionais; e (iii) cobertura de temas ainda não tratados, com destaque para a interface com o regime arquivístico e para o tratamento automatizado de dados.

Premissa metodológica adotada. A govDADOS subscreve integralmente a tese estruturante do Guia e do Enunciado CGU nº 4/2022: a LGPD **não cria hipótese de sigilo** nem amplia o rol de informações restritas no setor público. As hipóteses de restrição de acesso a informações pessoais decorrem da LAI (art. 31) e da legislação correlata; a LGPD oferece princípios e salvaguardas para qualificar o tratamento. Todas as sugestões abaixo preservam essa premissa, portanto, nenhuma delas deve ser lida como autorização para converter proteção de dados em barreira indevida à transparência.

2. Sumário executivo

Em síntese, a govDADOS propõe os seguintes aprimoramentos ao Guia:

- **Interface com o regime arquivístico.** Incorporar menção expressa à Resolução CONARQ nº 54/2023 e ao regime dos arquivos permanentes, hoje ausente do Guia, embora este trate de “recuperação de fatos históricos”, “guarda permanente” e do papel do Arquivo Nacional.
- **Dados de pessoas falecidas.** Suprir a omissão do Guia quanto aos dados de pessoas falecidas, articulando a não incidência da LGPD (art. 6º da Res. CONARQ nº 54/2023) com a persistência de proteções de honra, imagem e dos interesses da família.
- **Tratamento automatizado e IA.** Inserir diretrizes sobre uso de inteligência artificial na triagem e no tarjamento (mascaramento) de informações, exigindo revisão humana significativa, auditabilidade (logs/trilhas) e observância do art. 20 da LGPD.
- **Risco de reidentificação e efeito mosaico.** Reforçar a etapa de avaliação de risco para contemplar a reidentificação por cruzamento de dados (efeito mosaico) e a perda de “obscuridade prática”, com remissão a padrões técnicos (ISO/IEC 27559:2022).
- **Proteção de crianças e adolescentes por padrão.** Converter a proteção de menores de uma exceção “motivada caso a caso” em regra de proteção por padrão (privacy by default), em harmonia com a Lei nº 15.211/2025 (ECA Digital) e o Decreto nº 12.880/2026.
- **Gestão documental e papel do arquivista.** Integrar a gestão documental (Lei nº 8.159/1991) e a participação do profissional arquivista à seção de “transparência por desenho”.

- **Rigor técnico no Capítulo 5.** Tornar obrigatórios — e não apenas “boas práticas” — o mascaramento automatizado e auditável do CPF, a segregação nativa de dados protegidos em PADs e a anonimização por padrão de dados de menores.
- **Lições do direito comparado.** Aproveitar convergências com o modelo norte-americano (teste de ponderação, irrelevância da motivação do requerente, “obscuridade prática”) e europeu (arts. 86 e 89 do GDPR), e registrar o caso indiano (2025) como alerta sobre o risco de esvaziamento do interesse público.

O detalhamento de cada ponto, com fundamentação e propostas de redação, consta das seções 4 a 7. A seção 8 consolida todas as sugestões em quadro-resumo.

3. Metodologia e escopo

A contribuição resulta da análise integrada dos seguintes documentos: (i) o *Guia de Transparência e Proteção de Dados Pessoais* (CGU/ANPD, maio de 2026), nas versões consolidada e da consulta pública; e (ii) a **Resolução CONARQ nº 54, de 8 de dezembro de 2023**, que disciplina a aplicação da LGPD aos arquivos permanentes. A análise observou quatro movimentos sucessivos:

1. Análise crítica e propositiva do Guia, capítulo a capítulo, identificando acertos, imprecisões e oportunidades de reforço;
2. Benchmark regulatório internacional (Estados Unidos, União Europeia, China e demais referências asiáticas), com extração de lições aplicáveis ao caso brasileiro;
3. Análise da Resolução CONARQ nº 54/2023 e de sua interface — hoje não explicitada — com o Guia;
4. Mapeamento de lacunas (temas relevantes não abordados) e formulação de propostas de redação.

Adotou-se abordagem multidimensional, registrando, sempre que pertinente, perspectivas convergentes e divergentes, bem como os riscos de cada opção regulatória. As sugestões respeitam a hierarquia normativa (CF/88 > leis > decretos > resoluções) e a repartição de competências entre CGU, ANPD e CONARQ.

4. Análise crítica e propositiva do Guia

4.1. Capítulo 1 — Direito de acesso e seus limites

O capítulo é tecnicamente sólido ao firmar a publicidade como regra e o sigilo como exceção (art. 3º, I, da LAI) e ao distinguir classificação, sigilo legal, documentos preparatórios e dados pessoais. Sugere-se apenas um reforço: explicitar que a hipótese de negativa por “produção de informação” **não autoriza** o indeferimento quando a tarefa se resumir a localizar, reunir e tarjar dados pessoais para liberar o restante — operação que o próprio Guia, no Capítulo 3 (Enunciado CGU nº 12/2023), trata como dever, e não como “produção”. O esclarecimento previne que a complexidade do tarjamento seja usada como pretexto de recusa.

Sugestão de redação

“Para os fins deste Guia, não configura produção de informação (art. 13 do Decreto nº 7.724/2012) a atividade de localizar, reunir, consolidar e tarjar dados pessoais em documentos preexistentes. Identificada essa hipótese, o órgão deve conceder o acesso à parte não restrita do documento, promovendo o tarjamento dos dados pessoais protegidos, nos termos do art. 7º, §2º, da LAI e do Enunciado CGU nº 12/2023.”

4.2. Capítulo 2 — Regime da LGPD e complementaridade com a LAI

O capítulo acerta ao ancorar o tratamento para fins de transparência no **cumprimento de obrigação legal ou regulatória** (art. 7º, II, e art. 11, II, “a”, da LGPD), interpretado sistematicamente com o art. 23. Recomenda-se acrescentar referência expressa ao **art. 5º, LXXIX, da CF/88** (direito fundamental autônomo à proteção de dados, incluído pela EC nº 115/2022), que confere a essa ponderação estatura constitucional, e reforçar que o regime do Capítulo IV da LGPD (Poder Público) convive com a **execução de políticas públicas** (art. 7º, III) como base correlata em diversos cenários de transparência ativa.

Sugestão de redação

“O tratamento de dados pessoais para fins de transparência pública fundamenta-se no cumprimento de obrigação legal e regulatória (art. 7º, II, e art. 11, II, ‘a’, da LGPD) e na execução de políticas públicas (art. 7º, III), interpretados em conjunto com o art. 23 da LGPD e à luz do direito fundamental à proteção de dados (art. 5º, LXXIX, da CF/88, incluído pela EC nº 115/2022). A proteção de dados, nessa moldura, qualifica o tratamento e não constitui hipótese autônoma de sigilo.”

4.3. Capítulo 3 — Proteção de dados pessoais prevista na LAI

A sistematização das hipóteses de acesso por terceiros é clara e bem fundamentada. Três aprimoramentos são propostos:

- **Prazos de restrição.** O Guia adota corretamente o Enunciado CGU nº 1/2024 (presunção de 15 anos na ausência de prazo expresso, em lugar do teto de 100 anos). Convém alertar que essa lógica de *prazo de restrição* precisa ser harmonizada com o regime dos arquivos permanentes, nos quais a eliminação é vedada e o acesso é a regra a partir do reconhecimento do valor secundário — tema desenvolvido na seção 6.
- **Dados de pessoas falecidas.** O capítulo é silente quanto aos falecidos. Recomenda-se incluir orientação específica (seção 7.2 desta contribuição): a LGPD não alcança a pessoa falecida, mas a honra e a imagem (art. 31 da LAI; arts. 12 e 20 do Código Civil) e o interesse de familiares podem subsistir, e os arquivos permanentes seguem regra própria (art. 6º da Res. CONARQ nº 54/2023).
- **Termo de Responsabilidade Digital.** Sugere-se que o Termo de Responsabilidade exigido para acesso de terceiros (item 3.4) preveja formato eletrônico com registro em trilha de auditoria, vinculando expressamente a finalidade declarada e permitindo verificação posterior de uso — boa prática alinhada à responsabilização (accountability) do art. 6º, X, da LGPD.

Sugestão de redação

(1) “O acesso de terceiros a informações pessoais condiciona-se à assinatura de Termo de Responsabilidade, preferencialmente em formato eletrônico, que vincule expressamente a finalidade declarada, registre a identificação do requerente e gere trilha de auditoria apta à verificação posterior do uso, em observância ao princípio da responsabilização (art. 6º, X, da LGPD).”

(2) “Aos dados de pessoas falecidas aplica-se orientação específica: a LGPD não incide, ressalvada a tutela da honra e da imagem (art. 31 da LAI; arts. 12 e 20 do Código Civil) e, em arquivos permanentes, o art. 6º da Resolução CONARQ nº 54/2023.”

4.4. Capítulo 4 — Roteiro decisório, Teste de Interesse Público e transparência por desenho

O roteiro de seis etapas e o “Teste de Interesse Público” são a melhor parte do Guia e dialogam de perto com a experiência comparada (seção 5). Para torná-los mais robustos, propõe-se:

4.4.1. Reforçar a etapa de avaliação de risco (efeito mosaico e obscuridade prática)

A etapa 3 (avaliação de risco de dano) já recomenda verificar se a informação “já está acessível em outras fontes públicas”. Convém qualificar essa diretriz: dado individualmente inócuo pode, quando **agregado** ou cruzado com outras bases, produzir perfil sensível ou permitir reidentificação (o chamado **efeito mosaico**). A circunstância de uma informação ser pontualmente pública não significa que sua **compilação e disponibilização sistemática** em transparência ativa seja inócua — distinção que a Suprema Corte dos EUA capturou no conceito de *practical obscurity* (seção 5.2). Sugere-se inserir, na etapa 3, a obrigação de considerar o risco incremental de agregação e a possibilidade de reidentificação.

Sugestão de redação

“Na avaliação do risco de dano (Etapa 3), o órgão considerará não apenas se a informação já se encontra acessível isoladamente em outras fontes, mas também o risco incremental decorrente de sua agregação e do cruzamento com outras bases (efeito mosaico) e a possibilidade de reidentificação de titulares. A circunstância de um dado ser pontualmente público não autoriza, por si só, sua compilação e disponibilização sistemática quando disso resultar a perda da obscuridade prática que protegia o titular.”

4.4.2. Inserir diretriz sobre tratamento automatizado e inteligência artificial

O Guia foi concebido para decisões humanas, mas a prática já incorpora triagem automatizada de pedidos, mascaramento por software e, crescentemente, modelos de IA. Três salvaguardas devem ser explicitadas:

- decisões sobre concessão, recusa ou tarjamento que produzam efeitos sobre o titular não podem ser *inteiramente* automatizadas sem possibilidade de revisão humana significativa, à luz do art. 20 da LGPD;
- todo processo automatizado de mascaramento/anonimização deve gerar **trilhas de auditoria (logs)** que permitam à CGU e à ANPD verificar a integridade da aplicação a toda a base (cf. art. 47 da Lei nº 14.129/2021);
- bases de transparência ativa devem considerar o risco de coleta massiva por sistemas de IA generativa e de reidentificação assistida por aprendizado de máquina, incorporando esse vetor à análise de risco.

Sugestão de redação

“Quando a triagem de pedidos, o tarjamento ou a anonimização forem apoiados por sistemas automatizados ou de inteligência artificial: (i) decisões que produzam efeitos sobre o titular não poderão ser inteiramente automatizadas, assegurada a revisão humana significativa (art. 20 da LGPD); (ii) o processo de mascaramento deverá gerar trilhas de auditoria (logs) que permitam verificar a integridade

de sua aplicação à totalidade da base (art. 47 da Lei nº 14.129/2021); e (iii) a análise de risco considerará a possibilidade de coleta massiva e de reidentificação assistida por inteligência artificial.”

4.4.3. Integrar gestão documental e o profissional arquivista à “transparência por desenho”

A seção 4.3 do Guia trata de desenhar processos e sistemas para a transparência, mas não menciona a **gestão documental** (Lei nº 8.159/1991), os instrumentos arquivísticos (tabelas de temporalidade, classificação, instrumentos de pesquisa) nem o **profissional arquivista**. A Resolução CONARQ nº 54/2023 (art. 4º, XIII) determina a participação do arquivista nas decisões sobre tratamento de dados pessoais. Recomenda-se que a “transparência por desenho” se apoie expressamente na política de gestão documental e na atuação técnica do arquivista, garantindo coerência entre o ciclo de vida do documento e as decisões de acesso.

Sugestão de redação

“A transparência por desenho quando da produção documental apoia-se na política de gestão documental do órgão (Lei nº 8.159/1991) e nos respectivos instrumentos arquivísticos (plano de classificação, tabela de temporalidade e instrumentos de pesquisa), com a participação do profissional arquivista nas decisões sobre o tratamento de dados pessoais ao longo do ciclo de vida documental, na forma do art. 4º, XIII, da Resolução CONARQ nº 54/2023.”

4.5. Capítulo 5 — Entendimentos sobre a publicidade de dados pessoais

O capítulo é o de aplicação mais direta pelos órgãos e, por isso, é onde o **rigor técnico** precisa ser elevado: várias diretrizes hoje redigidas como “boa prática” deveriam ser formuladas como requisitos. Apresentam-se a seguir cinco propostas de nova redação.

4.5.1. CPF de agentes públicos — mascaramento automatizado e auditável

Problema. O Guia recomenda a descaracterização do CPF (***.999.999-**), mas não exige que a máscara seja gerada por processo automatizado e auditável. Sem isso, há risco de erro humano e de ocultação seletiva ou excessiva de dados públicos.

Sugestão de redação

“A descaracterização do CPF de agentes públicos deve ser realizada de forma automatizada pelos sistemas de recursos humanos e de transparência, garantindo a desambiguação de homônimos sem expor o titular a fraudes. Todo o processo de mascaramento deve gerar trilhas de auditoria (logs) que permitam à CGU, à ANPD e aos órgãos de fiscalização e controle verificar se o algoritmo de proteção foi aplicado de forma íntegra a toda a base, conforme o art. 47 da Lei nº 14.129/2021.”

4.5.2. Processos administrativos disciplinares (PADs) — segregação nativa

Problema. O Guia sugere, como “boa prática”, instruir os PADs prevendo sua publicidade futura. À luz da LGPD, a segregação de dados protegidos (intimidade/vida privada) deve ser requisito técnico obrigatório desde a autuação, evitando o retrabalho de tarjamento manual e o risco de exposição indevida.

Sugestão de redação

“Os órgãos são obrigados a estruturar a instrução de PADs com segregação nativa entre documentos de interesse público e documentos contendo dados de intimidade ou vida privada. O sistema de gestão processual deve permitir a geração automática de uma versão pública indexada, garantindo que o tarjamento de dados sensíveis seja acompanhado de fundamentação legal específica para cada campo ocultado, assegurando a rastreabilidade das decisões de sigilo.”

4.5.3. Listas de controle de acesso a prédios públicos — crianças e adolescentes

Problema. O Guia admite que o acesso seja negado a dados de crianças e adolescentes “mediante decisão motivada”. A Lei nº 15.211/2025 (ECA Digital) exige o nível mais elevado de proteção por padrão para menores, o que torna a proteção do nome do menor a regra absoluta, e não uma exceção a ser motivada caso a caso.

Sugestão de redação

“Nos registros de controle de acesso a prédios públicos, os dados de crianças e adolescentes devem ser anonimizados por padrão em qualquer consulta de terceiros. A identificação nominal desses titulares é vedada em sistemas de transparência ativa ou passiva, devendo ser fornecido apenas o nome do responsável legal acompanhante, em observância ao melhor interesse do menor e ao art. 7º da Lei nº 15.211/2025.”

4.5.4. Beneficiários de programas sociais — vedação ao perfilamento de menores

Problema. O Guia veda divulgar o nome de beneficiários menores a “terceiros não autorizados”, mas admite a divulgação parcial do CPF. Para evitar o perfilamento socioeconômico e comportamental de menores, deve-se aplicar a proteção reforçada da Lei nº 15.211/2025.

Sugestão de redação

“A transparência sobre beneficiários de programas sociais deve garantir o controle social sem permitir o perfilamento comportamental ou socioeconômico de menores. É vedada a divulgação de qualquer dado (incluindo CPF parcial ou NIS) que permita a reidentificação de crianças e adolescentes. Tais dados devem ser substituídos pela identificação exclusiva do responsável legal, operando o sistema com o grau máximo de privacidade desde a concepção, conforme o art. 26 da Lei nº 15.211/2025.”

4.5.5. Estudantes beneficiários de bolsas e ações afirmativas — menores

Problema. O Guia admite que a demanda por informações de menores bolsistas seja avaliada “caso a caso” quanto à preponderância do interesse público, o que fragiliza a proteção do menor diante de pedidos abusivos.

Sugestão de redação

“A divulgação de dados de estudantes menores beneficiários de bolsas ou cotas deve priorizar a anonimização irreversível dos dados sensíveis (raça, gênero, condição de saúde). O interesse público na fiscalização da política deve ser satisfeito via dados agregados ou extratos auditáveis, sendo vedada a divulgação nominal do menor, salvo se imprescindível para a defesa de direitos humanos, exigindo-se, neste caso, a assinatura de Termo de Responsabilidade Digital e o registro em trilha de auditoria do órgão.”

4.5.6. Dados biométricos e reconhecimento facial no controle de acesso

A tabela de controle de acesso classifica corretamente a biometria como dado a **não divulgar**, mas o Guia não enfrenta a *coleta e retenção* de biometria e reconhecimento facial para o próprio controle de acesso — operação de tratamento de dado sensível (art. 11 da LGPD) que demanda necessidade, proporcionalidade e base legal específicas. Recomenda-se nota orientando que sistemas de identificação biométrica em prédios públicos adotem alternativas menos invasivas quando suficientes, retenção mínima e avaliação de impacto, em linha com a tendência internacional de restringir o reconhecimento facial em espaços públicos (seções 5.4 e 5.5).

Sugestão de redação

“A coleta e a retenção de dados biométricos e o uso de reconhecimento facial para controle de acesso a prédios públicos constituem tratamento de dado pessoal sensível (art. 11 da LGPD) e exigem demonstração de necessidade e proporcionalidade, adoção de alternativas menos invasivas quando

suficientes, retenção mínima e realização de avaliação de impacto à proteção de dados pessoais (RIPD) previamente à implantação.”

5. Análise regulatória comparada

A tensão entre acesso à informação pública e proteção de dados pessoais é universal; o que varia é o **ponto de equilíbrio** e o desenho institucional adotado para resolvê-la. O quadro abaixo sintetiza os modelos analisados; as subseções extraem lições aplicáveis ao Guia.

Jurisdição	Acesso à informação	Proteção de dados	Regra de articulação	Autoridade
Brasil	LAI (Lei 12.527/2011)	LGPD 13.709/2018 (Lei)	LGPD não cria sigilo; restrições vêm da LAI (art. 31) + teste de interesse público	CGU / ANPD
EUA	FOIA (5 U.S.C. §552)	Privacy Act 1974; sem lei geral federal; CCPA/CPRA (estadual)	Exemptions 6 e 7(C): teste de ponderação; interesse público = “o que o governo faz”	Agências; OIP/DOJ
União Europeia	Reg. (CE) 1049/2001	GDPR 2016/679 (Reg.)	GDPR arts. 86 e 89 + Recital 154; Reg. 1049 art. 4(1)(b); jurisprudência (Bavarian Lager)	EDPB / EDPS
China	Regs. de Informação Governamental (OGI, rev. 2019)	PIPL (2021), DSL, CSL	Divulgação como princípio, com amplas exceções; modelo estatocêntrico	CAC (Adm. do Ciberespaço)
Japão	Lei de Acesso a Info. de Órgãos Administrativos (1999)	APPI (rev. 2020/2022)	Categorias técnicas legais de des-identificação (pseudonimizada/anonimizada)	PPC
Coreia do Sul	Official Information Disclosure Act (1996)	PIPA (rev. 2020/2023)	Regime de dado pseudonimizado p/ pesquisa, estatística e arquivo de interesse público	PIPC
Índia	RTI Act (2005)	DPDP Act 2023 + Rules 2025	Emenda ao art. 8(1)(j) do RTI esvaziou o teste de interesse público — ver alerta	Data Protection Board

5.2. Estados Unidos — o teste de ponderação e a “obscuridade prática”

O FOIA protege a privacidade por meio das **Exemptions 6 e 7(C)**, que não operam como sigilo absoluto: exigem ponderar o interesse de privacidade do indivíduo contra o interesse público na divulgação. Três lições convergem com o modelo brasileiro e podem reforçá-lo:

- **Conceito estrito de interesse público.** Em *U.S. DOJ v. Reporters Committee for Freedom of the Press* (1989), a Suprema Corte definiu que o interesse público relevante é apenas aquele que “esclarece o que o governo está fazendo” — convergente com a advertência do Guia de que “interesse coletivo é diferente de curiosidade geral”.
- **Irrelevância da motivação do requerente.** O propósito particular do solicitante é, em regra, irrelevante — o que dialoga diretamente com o art. 10, §3º, da LAI e merece destaque expresso no Guia.

Sugestão de redação

(1) “Recomenda-se que o Teste de Interesse Público registre que o interesse público apto a justificar o acesso é aquele que esclarece a atuação do Estado — sua organização, seus gastos e a regularidade

da conduta de seus agentes —, não se confundindo com a curiosidade geral nem com o interesse meramente privado do requerente.”

(2) “A motivação do solicitante é, em regra, irrelevante para a decisão de acesso (art. 10, §3º, da LAI), ressalvada a hipótese de informação relativa ao próprio requerente.”

- **Obscuridade prática (practical obscurity).** A Corte reconheceu que compilar dados dispersos — ainda que individualmente públicos — em uma base consolidada cria risco novo de privacidade. É o fundamento para incorporar o efeito mosaico à etapa de avaliação de risco do Guia (item 4.4.1).

Registre-se ainda que, em *FCC v. AT&T* (2011), firmou-se que pessoas jurídicas não têm “privacidade pessoal” — premissa coerente com a orientação do Guia de que dados de pessoas jurídicas não são dados pessoais.

5.3. União Europeia — conciliação por desenho normativo

A UE concilia o Regulamento (CE) nº 1049/2001 (acesso a documentos) com o GDPR por meio de dois dispositivos diretamente análogos a desafios brasileiros:

- **Art. 86 e Recital 154 do GDPR.** Autorizam a divulgação de dados pessoais em documentos oficiais para “conciliar o acesso do público aos documentos oficiais com o direito à proteção de dados” — exatamente a função que o Guia exerce.
- **Art. 89 do GDPR — arquivamento de interesse público.** Cria regime de salvaguardas e derrogações para tratamento com finalidade de arquivo de interesse público, pesquisa científica/histórica e estatística. É o paralelo europeu da Resolução CONARQ nº 54/2023 e demonstra que o tema arquivístico integra, na UE, o próprio núcleo da proteção de dados — reforçando a necessidade de o Guia brasileiro reconhecer essa interface (seção 6).

A jurisprudência (caso *Comissão v. Bavarian Lager*, C-28/08 P) consolidou que pedidos de acesso a documentos com dados pessoais devem satisfazer as condições da proteção de dados, exigindo do requerente a demonstração da necessidade — equilíbrio que o teste brasileiro também busca. Por fim, registra-se que o “**Digital Omnibus**” (proposta da Comissão de 19/11/2025, em tramitação) discute redefinir o conceito de “dado pessoal” e os critérios de pseudonimização; o EDPB e o EDPS manifestaram-se contra o estreitamento do conceito (fev/2026). A lição para o Brasil é de cautela: a fronteira entre dado pessoal, pseudonimizado e anonimizado é tecnicamente instável e exige padrões claros — o que recomenda a remissão a normas técnicas (item 7.4).

Sugestão de redação

“O tratamento de dados pessoais em documentos oficiais destina-se a conciliar o acesso público com o direito à proteção de dados; o tratamento para fins de arquivo de interesse público, pesquisa histórica e estatística sujeita-se a salvaguardas específicas (à semelhança do art. 89 do GDPR), remetendo-se, quanto a estes, à Resolução CONARQ nº 54/2023.”

5.4. China — modelo estatocêntrico

As *Regulations on Open Government Information* (revisadas em 2019) adotam, no plano formal, a divulgação como princípio, mas com exceções amplas (segredo de Estado, segredo comercial e privacidade pessoal). A **PIPL** (2021) admite, como base legal, o tratamento de informação “licitamente tornada pública” dentro de escopo razoável (art. 13), não prevê o “legítimo interesse” e exige avaliação de impacto (PIPIA) para dados sensíveis, decisões automatizadas, compartilhamento e transferência internacional; o reconhecimento facial em espaços públicos é admitido, em regra, apenas para fins de segurança pública. O modelo chinês é **estatocêntrico**: serve de contraponto — ilustra um equilíbrio que privilegia o controle estatal sobre o controle social, distante do paradigma democrático brasileiro, mas oferece referência útil quanto à exigência de avaliação de impacto prévia e à restrição do reconhecimento facial (item 4.5.6).

Sugestão de redação

“Em situações de maior risco — em especial o tratamento de dados sensíveis, o uso de identificação biométrica e o reconhecimento facial — recomenda-se a realização de avaliação de impacto prévia, restringindo-se a identificação biométrica em espaços públicos às hipóteses estritamente necessárias e proporcionais.”

5.5. Demais referências asiáticas — padrões técnicos e um alerta

- **Japão (APPI).** O Japão estrutura categorias técnico-legais de des-identificação — “informação pseudonimizada” (仮名加工情報) e “informação anonimizada” (匿名加工情報) — com obrigações próprias e padrões definidos por lei. É modelo de como conferir **segurança jurídica e técnica** à anonimização e à pseudonimização que o Guia menciona, porém sem padrão.
- **Coreia do Sul (PIPA).** A reforma de 2020 criou regime de “dado pseudonimizado” que autoriza o tratamento sem consentimento para fins estatísticos, de pesquisa científica e de arquivamento de interesse público (análogo ao art. 89 do GDPR e à Res. CONARQ nº 54/2023) — referência direta para o tratamento de dados em arquivos e pesquisas.
- **Índia (alerta).** Em 13–14/11/2025, a Índia notificou as *DPDP Rules, 2025*, colocando em vigor o art. 44(3) do DPDP Act, que alterou o art. 8(1)(j) do RTI Act para criar exceção quase irrestrita de “informação pessoal”, esvaziando o teste de interesse público que orientava as decisões de acesso. A reforma foi duramente criticada por ativistas e juristas (entre eles o ex-presidente do Tribunal Superior de Délhi, A. P. Shah) como retrocesso à transparência. É exatamente o **desfecho que o modelo brasileiro evita**: o Brasil — via Enunciado CGU nº 4/2022 e o próprio Guia — preserva o teste de ponderação e a primazia da LAI. Recomenda-se que o Guia registre esse contraste como reforço de sua arquitetura.

Sugestão de redação

(1) “As operações de anonimização e pseudonimização referidas neste Guia observarão padrões técnicos reconhecidos e as orientações técnicas da ANPD, considerando-se a anonimização e a pseudonimização como pontos de um espectro de des-identificação, e não como categorias estanques.”

(2) “A proteção de dados pessoais não constitui exceção absoluta ao direito de acesso: subsiste, em todos os casos, o teste de ponderação que admite a divulgação quando o interesse público preponderar sobre o risco ao titular, vedada a recusa de acesso fundada exclusivamente na natureza pessoal do dado.”

Lição transversal: padrões técnicos

Tanto a experiência asiática quanto a europeia convergem para a necessidade de **padrões técnicos de des-identificação**. Sugere-se que o Guia remeta à norma ISO/IEC 27559:2022 (*Privacy-Enhancing Data De-Identification Framework*) e ao Guia de Anonimização das autoridades de privacidade da Ásia-Pacífico (2025), bem como a futuras orientações técnicas da ANPD, conferindo objetividade às etapas de anonimização, pseudonimização e avaliação de risco de reidentificação.

6. A Resolução CONARQ nº 54/2023 e sua interface com o Guia

A omissão mais relevante do Guia, na avaliação da govDADOS, é a **ausência de qualquer menção** à Resolução CONARQ nº 54/2023 e ao regime dos arquivos permanentes — ainda que o Guia trate de “recuperação de fatos históricos”, “documentos destinados à guarda permanente” e do papel do Arquivo Nacional (Capítulo 3, alínea “g”).

6.1. Síntese da Resolução

A Resolução estabelece diretrizes e regras para a aplicação da LGPD aos **arquivos permanentes**, em qualquer suporte, e aplica-se aos integrantes do SINAR e a detentores de arquivos, públicos e privados. Seus pontos centrais:

- o tratamento de dados pessoais em arquivos permanentes (acesso e compartilhamento) configura **cumprimento de obrigação legal** do controlador (Lei nº 8.159/1991; art. 7º, II e III, da LAI; arts. 7º, II, 11, II, “a”, e 16, I, da LGPD);
- os dados de **pessoas falecidas** em arquivos permanentes não se sujeitam à LGPD (art. 6º);
- é **vedada a eliminação** de dados pessoais contidos em arquivos permanentes (art. 7º), que são inalienáveis e imprescritíveis (art. 2º);
- a revogação de consentimento após o reconhecimento do valor secundário não impede a conservação e o tratamento (art. 8º); a anonimização/pseudonimização não pode comprometer autenticidade e integridade (art. 9º);
- define direitos do titular (arts. 10 a 12, com prazo de resposta de 15 dias), obrigações dos agentes, regras de recolhimento com indicação de base legal e restrições (art. 17) e a **participação do arquivista** nas decisões (art. 4º, XIII);
- em incidente de segurança envolvendo arquivos privados de interesse público, a comunicação deve alcançar também o **CONARQ** (art. 15, parágrafo único).

6.2. Por que importa para o Guia

O Guia disciplina, sobretudo, o acesso a informações nas fases corrente e intermediária e o atendimento a pedidos de LAI. A Resolução nº 54/2023 disciplina a fase **permanente** — precisamente o destino dos documentos “destinados à guarda permanente” que o próprio Guia menciona. Sem a articulação entre os dois regimes, o agente público fica sem orientação sobre, por exemplo: como tratar pedido de acesso a documento já recolhido ao arquivo permanente; como conciliar o *prazo de restrição* da LAI (15/100 anos) com a **vedação de eliminação** e a regra de acesso dos arquivos permanentes; e qual o papel do Arquivo Nacional e dos arquivos setoriais na “recuperação de fatos históricos”.

6.3. Propostas de redação

Sugere-se inserir no Guia subseção específica sobre arquivos permanentes, com uma ou mais das cláusulas a seguir:

Sugestão de redação

(1) “O tratamento de dados pessoais em documentos recolhidos a arquivos permanentes rege-se pela Resolução CONARQ nº 54/2023, que disciplina o acesso, o compartilhamento e a conservação desses dados em cumprimento de obrigação legal (Lei nº 8.159/1991; art. 7º da LAI; arts. 7º, II, e 11, II, ‘a’, da LGPD).”

(2) “Nos arquivos permanentes, o acesso é a regra decorrente do reconhecimento do valor secundário do documento, sendo vedada a eliminação dos dados pessoais neles contidos (art. 7º da Resolução CONARQ nº 54/2023); não se lhes aplica automaticamente a lógica de prazo de restrição própria das

fases corrente e intermediária, recaindo a avaliação de acesso sobre restrições pontuais e instrumentos de pesquisa (arts. 18 a 20 da Resolução)."

(3) "O acesso de terceiros a documentos de arquivo permanente que contenham dados pessoais condiciona-se ao Termo de Responsabilidade previsto no art. 22 da Resolução CONARQ nº 54/2023."

(4) "As decisões sobre tratamento de dados pessoais em arquivos permanentes contarão com a participação do profissional arquivista (art. 4º, XIII, da Resolução CONARQ nº 54/2023)."

7. Pontos não abordados pelo Guia e propostas adicionais

7.1. Interface com o regime arquivístico

Desenvolvida na seção 6. É a lacuna de maior impacto, dada a centralidade da gestão documental para o exercício do direito de acesso (princípio que o próprio Guia reconhece, ao final do Capítulo 1).

Sugestão de redação

“Inclua-se subseção sobre arquivos permanentes que reconheça a Resolução CONARQ nº 54/2023 como norma de regência do tratamento de dados pessoais nessa fase (conforme as cláusulas do item 6.3 desta contribuição), assegurando a coerência entre o ciclo de vida documental e as decisões de acesso.”

7.2. Dados de pessoas falecidas

O Guia não trata dos dados de pessoas falecidas. Propõe-se orientação que articule três planos: (i) a LGPD, em regra, não alcança o falecido; (ii) ainda assim, a **honra e a imagem** subsistem como projeção da personalidade (art. 31 da LAI; arts. 12 e 20 do Código Civil), e familiares têm legitimidade para protegê-las; (iii) em arquivos permanentes, vale o art. 6º da Resolução CONARQ nº 54/2023 (não incidência da LGPD), inclusive quanto a pessoas ausentes com sucessão definitiva aberta. A ausência de orientação gera insegurança recorrente em pedidos sobre processos antigos e acervos históricos.

Sugestão de redação

“Dados de pessoas falecidas: a LGPD não se aplica à pessoa falecida; subsistem, contudo, a proteção da honra e da imagem (art. 31 da LAI; arts. 12 e 20 do Código Civil), que legitimam familiares a postular restrição, e, em arquivos permanentes, a regra do art. 6º da Resolução CONARQ nº 54/2023. A simples menção a pessoa falecida em documento público não impõe restrição automática, devendo o órgão avaliar o risco concreto à honra e à imagem e o interesse histórico do acervo.”

7.3. Tratamento automatizado e inteligência artificial

Desenvolvido no item 4.4.2. Reforça-se: o Guia deveria dedicar item próprio à governança algorítmica da transparência — revisão humana significativa (art. 20 da LGPD), auditabilidade do mascaramento (art. 47 da Lei nº 14.129/2021) e mitigação do risco de reidentificação assistida por IA. Trata-se de vetor em rápida expansão e de alto impacto institucional.

Sugestão de redação

“Decisões de acesso, recusa ou tarjamento apoiadas em sistemas automatizados ou de inteligência artificial observarão revisão humana significativa (art. 20 da LGPD) e auditabilidade do tratamento (art. 47 da Lei nº 14.129/2021), nos termos da sugestão de redação do item 4.4.2.”

7.4. Padrões técnicos de anonimização e risco de reidentificação

O Guia emprega “anonimização”, “pseudonimização” e “tarjamento” sem ancorá-los em padrão técnico nem em metodologia de avaliação de risco de reidentificação. A correta afirmação da ANPD — de que a anonimização *não é condição* para o compartilhamento — não deve degenerar em dispensa de desidentificação onde ela seja viável e adequada. Propõe-se: (i) remissão a padrões técnicos (ISO/IEC 27559:2022; Guia de Anonimização Ásia-Pacífico, 2025; futuras orientações da ANPD); (ii) inclusão de uma avaliação de risco de reidentificação (probabilidade de “singularização”, “vinculação” e “inferência”) na etapa 3 do roteiro; e (iii) reconhecimento de que pseudonimização e anonimização situam-se em um **espectro**, e não em categorias binárias — cautela que o próprio debate europeu (Digital Omnibus) evidencia.

Sugestão de redação

“As referências a anonimização, pseudonimização e tarjamento serão acompanhadas de remissão a padrões técnicos (ISO/IEC 27559:2022 e orientações da ANPD) e de uma avaliação de risco de reidentificação que considere as possibilidades de singularização, vinculação e inferência.”

7.5. Proteção reforçada de crianças e adolescentes (ECA Digital)

Desenvolvida nos itens 4.5.3 a 4.5.5. Propõe-se uma **regra transversal** no Guia: dados de crianças e adolescentes observam o melhor interesse e a proteção por padrão (Lei nº 15.211/2025 e Decreto nº 12.880/2026; art. 14 da LGPD), de modo que sua identificação nominal em transparência seja exceção qualificada, e não decisão casuística.

Sugestão de redação

“Regra geral de proteção de crianças e adolescentes: o tratamento de seus dados para fins de transparência observa o melhor interesse e a proteção por padrão (art. 14 da LGPD; Lei nº 15.211/2025 e Decreto nº 12.880/2026), sendo a identificação nominal de menor exceção qualificada e fundamentada, e não decisão casuística.”

7.6. Gestão documental e papel do arquivista

Desenvolvida no item 4.4.3 e na seção 6. A “transparência por desenho” deve apoiar-se na política de gestão documental (Lei nº 8.159/1991) e na atuação técnica do arquivista, sob pena de ficar restrita ao desenho de sistemas de TI, desconsiderando o ciclo de vida documental.

Sugestão de redação

“A transparência por desenho incorporará a política de gestão documental (Lei nº 8.159/1991) e a atuação do arquivista (art. 4º, XIII, da Resolução CONARQ nº 54/2023), nos termos da sugestão de redação do item 4.4.3.”

7.7. Prazos de restrição versus arquivos permanentes

O Guia não harmoniza a lógica de *prazo de restrição* (Enunciado CGU nº 1/2024 — 15 anos; teto de 100 anos do art. 55 do Decreto nº 7.724/2012) com a **inalienabilidade e a vedação de eliminação** dos arquivos permanentes. Em acervos de guarda permanente, o decurso do prazo conduz, em regra, à abertura — não há “eliminação” possível — e a avaliação de acesso recai sobre instrumentos de pesquisa e restrições pontuais (arts. 18 a 20 da Res. CONARQ nº 54/2023). Recomenda-se nota de harmonização.

Sugestão de redação

“Os prazos de restrição (art. 55 do Decreto nº 7.724/2012; Enunciado CGU nº 1/2024) não se transpõem automaticamente aos arquivos permanentes, nos quais a eliminação é vedada e o decurso do prazo conduz, em regra, à abertura do acesso, recaindo a avaliação sobre restrições pontuais (arts. 18 a 20 da Resolução CONARQ nº 54/2023).”

7.8. Incidentes de segurança e cadeia de comunicação

O Guia, focado na decisão de divulgar, não trata do **incidente de segurança** que exponha indevidamente dados pessoais sob transparência. Sugere-se nota de remissão à disciplina de comunicação de incidentes (LGPD, art. 48, e regulamentação da ANPD) e, no caso de arquivos privados de interesse público, à comunicação adicional ao CONARQ (art. 15 da Res. nº 54/2023).

Sugestão de redação

“Ocorrendo incidente de segurança que exponha indevidamente dados pessoais sob regime de transparência, o órgão observará a disciplina de comunicação de incidentes (art. 48 da LGPD e regulamentação da ANPD) e, tratando-se de arquivos privados de interesse público, comunicará também o CONARQ (art. 15, parágrafo único, da Resolução CONARQ nº 54/2023).”

7.9. Reuso de dados abertos e transferência internacional

A transparência ativa alimenta o ecossistema de dados abertos (art. 29 da Lei nº 14.129/2021), cujo reuso pode incluir agentes no exterior e novas finalidades. O Guia não trata do **reúso** nem da transferência internacional de dados pessoais assim disponibilizados. Recomenda-se nota: (i) remetendo às boas práticas de minimização e des-identificação na publicação para reuso; e (ii) registrando que a publicação não esvazia o regime de transferência internacional da LGPD (Capítulo V), tema que a Resolução nº 54/2023 também tangencia (art. 13, V, ao exigir indicação de agentes internacionais com quem haja compartilhamento).

Sugestão de redação

“A disponibilização de dados pessoais em transparência ativa para reuso (art. 29 da Lei nº 14.129/2021) observará a minimização e, quando viável, a des-identificação; a publicação não afasta o regime de transferência internacional de dados pessoais (Capítulo V da LGPD).”

8. Quadro-resumo das sugestões

Consolidam-se abaixo as contribuições, com o respectivo fundamento. A redação integral proposta para cada item consta das caixas *Sugestão de redação* distribuídas ao longo das seções 4 a 7.

#	Tema / item do Guia	Lacuna ou problema	Sugestão	Fundamento
1	Negativa por “produção de informação” (Cap. 1)	Risco de recusa quando basta tarjar e liberar	Explicitar que localizar/tarjar não é “produção”	LAI art. 7º §2º; Enunciado CGU 12/2023
2	Base legal (Cap. 2)	Falta âncora constitucional e da política pública	Citar art. 5º LXXIX CF e art. 7º III LGPD	CF/88 (EC 115/2022); LGPD arts. 7º, 23
3	Dados de falecidos (Cap. 3 / 7.2)	Tema não tratado	Orientar: LGPD não incide, mas honra/imagem e família subsistem	LAI art. 31; CC arts. 12 e 20; Res. 54 art. 6º
4	Termo de Responsabilidade (Cap. 3)	Sem registro/auditoria	Termo eletrônico vinculado à finalidade, com trilha	LGPD art. 6º, X
5	Avaliação de risco (Cap. 4.4.1)	Não trata de agregação/reidentificação	Incluir efeito mosaico e obscuridade prática	DOJ v. Reporters Committee (EUA)
6	IA e automação (Cap. 4.4.2 / 7.3)	Guia presume decisão humana	Revisão humana, logs auditáveis, risco de IA	LGPD art. 20; Lei 14.129/2021 art. 47
7	Transparência por desenho (Cap. 4.4.3 / 7.6)	Omite gestão documental e arquivista	Integrar Lei de Arquivos e o arquivista	Lei 8.159/1991; Res. 54 art. 4º, XIII
8	CPF (Cap. 5.1)	Mascaramento sem automação/auditoria	Mascaramento automatizado e auditável	Lei 14.129/2021 art. 47
9	PADs (Cap. 5.2)	Segregação só como “boa prática”	Segregação nativa obrigatória + versão pública	LAI art. 7º §3º; LGPD arts. 6º, 46
10	Menores em controle de acesso (Cap. 5.3)	Proteção como exceção motivada	Anonimização por padrão; vedar nome do menor	Lei 15.211/2025 art. 7º
11	Beneficiários menores (Cap. 5.4)	Admite CPF parcial de menor	Vedar dado reidentificável; usar responsável legal	Lei 15.211/2025 art. 26; LGPD art. 14
12	Bolsistas menores (Cap. 5.5)	Avaliação “caso a caso”	Anonimização irreversível + dados agregados	Lei 15.211/2025; LGPD art. 14
13	Biometria/reconhecimento facial (Cap. 5)	Não trata da coleta/retenção	Minimização, finalidade e avaliação de impacto	LGPD art. 11; ref. PIPL/AI Act
14	Arquivos permanentes (Seção 6)	Sem menção à Res. CONARQ 54/2023	Subseção de interface com o regime permanente	Res. CONARQ 54/2023; Lei 8.159/1991
15	Padrões técnicos (7.4)	Anonimização sem padrão	Remeter a ISO/IEC 27559:2022 e orientações ANPD	GDPR (debate Omnibus); APPI; PIPA
16	Prazos x permanência (7.7)	Lógica de prazo não harmonizada	Nota de harmonização com arquivos permanentes	Decreto 7.724/2012 art. 55; Res. 54 arts. 7º, 18-20

#	Tema / item do Guia	Lacuna ou problema	Sugestão	Fundamento
17	Incidentes (7.8)	Não trata de vazamento na transparência	Remissão a LGPD art. 48 e a CONARQ	LGPD art. 48; Res. 54 art. 15
18	Reúso/dados abertos (7.9)	Não trata de reúso e transf. internacional	Notas de minimização e Cap. V da LGPD	Lei 14.129/2021 art. 29; LGPD Cap. V

9. Conclusão e encaminhamento

O *Guia de Transparência e Proteção de Dados Pessoais* representa avanço maduro na harmonização entre a LAI e a LGPD e posiciona o Brasil entre as jurisdições que melhor equilibram transparência e privacidade — em contraste, por exemplo, com o recente esvaziamento do teste de interesse público observado na Índia. As contribuições aqui reunidas não pretendem alterar essa arquitetura, mas torná-la mais precisa, tecnicamente ancorada e completa.

As três prioridades da govDADOS são: (i) **reconhecer expressamente a interface com o regime arquivístico** (Resolução CONARQ nº 54/2023), hoje ausente; (ii) **enfrentar o tratamento automatizado e a inteligência artificial** na decisão de transparência, com revisão humana e auditabilidade; e (iii) **eleva a proteção de crianças e adolescentes a regra por padrão**, em harmonia com o ECA Digital. As demais sugestões reforçam o rigor técnico e a aderência às melhores práticas internacionais.

A govDADOS coloca-se à disposição da CGU e da ANPD para detalhar qualquer dos pontos, contribuir com redações específicas ou participar de audiências e grupos técnicos no curso do aperfeiçoamento do Guia.

govDADOS — Associação Brasileira de Governança de Dados

Conselho de Administração



Documento assinado digitalmente

ANDRE FREIRE DA SILVA

Data: 21/06/2026 09:53:25-0300

Verifique em <https://validar.iti.gov.br>

André Freire da Silva

Presidente do Conselho de Administração



Documento assinado digitalmente

HAILLA DALETH MELO RIBEIRO

Data: 20/06/2026 11:14:15-0300

Verifique em <https://validar.iti.gov.br>

Hailla Daleth

Vice- Presidente do Conselho de Administração

Brasília/DF, 20 junho de 2026

Anexo — Referências normativas e fontes

Brasil

- Constituição Federal de 1988 — art. 5º, X, XXXIII e LXXIX (EC nº 115/2022).
- Lei nº 12.527/2011 (Lei de Acesso à Informação — LAI).
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais — LGPD).
- Lei nº 8.159/1991 (Política Nacional de Arquivos).
- Lei nº 14.129/2021 (Lei do Governo Digital).
- Lei nº 15.211/2025 (ECA Digital) e Decreto nº 12.880/2026.
- Decreto nº 7.724/2012 (regulamento da LAI).
- Resolução CONARQ nº 54, de 8/12/2023.
- Enunciados CGU nº 4/2022, 1/2024, 12/2023, 7/2023, 5/2023, 10/2023, 14/2016, 1/2023, 2/2023, 3/2023.
- STF, Suspensão de Segurança nº 3.902/SP (rel. Min. Ayres Britto).
- ANPD, Guias Orientativos — Tratamento de dados pelo Poder Público; e para fins acadêmicos/pesquisa (2023).

Direito comparado e padrões técnicos

- EUA — Freedom of Information Act (5 U.S.C. §552), Exemptions 6 e 7(C); Privacy Act de 1974; U.S. DOJ v. Reporters Committee for Freedom of the Press (1989); FCC v. AT&T (2011).
- União Europeia — Regulamento (CE) nº 1049/2001; GDPR (Reg. UE 2016/679), arts. 86 e 89 e Recital 154; TJUE, Comissão v. Bavarian Lager (C-28/08 P); proposta de “Digital Omnibus” (19/11/2025) e manifestação EDPB/EDPS (2026).
- China — Regulations on Open Government Information (rev. 2019); PIPL (2021).
- Japão — Act on the Protection of Personal Information (APPI, rev. 2020/2022); Lei de Acesso a Informações de Órgãos Administrativos (1999).
- Coreia do Sul — Personal Information Protection Act (PIPA, rev. 2020/2023); Official Information Disclosure Act (1996).
- Índia — Right to Information Act (2005); Digital Personal Data Protection Act (2023) e DPDP Rules (2025); Puttaswamy v. Union of India (2017).
- ISO/IEC 27559:2022 — Privacy-Enhancing Data De-Identification Framework; Guia de Anonimização das autoridades de privacidade da Ásia-Pacífico (2025).

Documento elaborado como contribuição da govDADOS à Consulta Pública CGU/ANPD. As fontes de direito comparado foram consultadas em junho de 2026; marcos em tramitação (p. ex., o “Digital Omnibus” da UE) podem sofrer alterações no curso do processo legislativo.

Inclusão de Glossário

O Guia reúne conceitos de dois regimes jurídicos distintos: LAI e LGPD, além de expressões técnicas de anonimização, gestão documental, transparência e análise de riscos. Sem um glossário, termos próximos podem ser interpretados como equivalentes, por exemplo:

- dado pessoal × informação pessoal protegida;
- publicidade × acesso × divulgação;
- sigilo × restrição de acesso;
- anonimização × pseudonimização × tarjamento;
- interesse público × interesse público geral e preponderante;
- transparência ativa × transparência passiva;
- dado sensível × dado pessoal com maior risco de exposição.

O próprio histórico de elaboração de outros guias da ANPD registra a conveniência de incluir glossário e padronizar a terminologia utilizada, especialmente para facilitar a leitura por públicos com níveis distintos de conhecimento técnico.

Redação sugerida:

APÊNDICE I — GLOSSÁRIO DE TERMOS E EXPRESSÕES

O presente Glossário reúne conceitos legais, técnicos e orientativos utilizados no Guia de Transparência e Proteção de Dados Pessoais, com o objetivo de facilitar sua compreensão e promover maior uniformidade na aplicação das orientações pelos órgãos e entidades públicas.

As definições legais reproduzem ou sintetizam conceitos previstos na legislação aplicável. As definições técnicas e orientativas são apresentadas exclusivamente para os fins deste Guia e deverão ser interpretadas em conformidade com a Lei de Acesso à Informação, a Lei Geral de Proteção de Dados Pessoais, seus regulamentos e demais normas aplicáveis.

Na hipótese de divergência, prevalecerão as definições constantes da legislação e dos atos normativos vigentes.

Sugestão de Termos prioritários:

Acesso à informação e transparência

- acesso parcial;
- documento preparatório;
- informação classificada;
- informação de interesse coletivo ou geral;
- interesse público geral e preponderante;
- publicidade diferida;
- restrição de acesso;
- sigilo legal;
- transparência ativa;
- transparência passiva;
- transparência por desenho.

Proteção de dados pessoais

- agente de tratamento;
- controlador;

- dado anonimizado;
- dado pessoal;
- dado pessoal sensível;
- Encarregado;
- operador;
- pessoa titular;
- tratamento de dados pessoais;
- terceiro.

Técnicas de proteção

- agregação;
- anonimização;
- descaracterização;
- minimização;
- pseudonimização;
- reidentificação;
- supressão;
- tarjamento;
- versão pública de documento.

Processo decisório

- benefício coletivo;
- interesse público;
- necessidade;
- proporcionalidade;
- risco de dano;
- termo de responsabilidade;
- teste de interesse público.

Tecnologia

- decisão automatizada;
- inteligência artificial;
- supervisão humana;
- rastreabilidade;
- treinamento de modelo.

A transparência e o acesso à informação constituem valores fundamentais da Administração Pública e encontram amparo na Lei de Acesso à Informação (LAI). Contudo, a disponibilização de informações em meios de amplo acesso público deve observar, simultaneamente, as garantias previstas na Lei Geral de Proteção de Dados Pessoais (LGPD), de forma a assegurar o equilíbrio entre a publicidade dos atos administrativos e a proteção dos dados pessoais.

Nesse contexto, deve-se considerar que a atual capacidade de agregação e cruzamento de dados por meio de mecanismos de busca, bases públicas e ferramentas digitais potencializa significativamente os riscos decorrentes da exposição excessiva de informações identificáveis. Dados que, isoladamente, poderiam parecer inofensivos podem, quando combinados, permitir a identificação precisa de indivíduos, a construção de perfis e o acesso indireto a outras informações pessoais.

A observância da LAI não implica a divulgação irrestrita de todos os dados disponíveis à Administração. Ao contrário, o dever de transparência deve ser interpretado em conjunto com os princípios da necessidade, adequação e minimização previstos na LGPD, limitando a exposição de informações ao estritamente necessário para atender à finalidade de controle social e fiscalização da atuação administrativa.

A publicação de elementos identificadores em excesso, especialmente quando não possuem relevância direta para a compreensão, auditoria ou fiscalização do ato administrativo divulgado, não contribui de forma efetiva para a transparência pública e pode ampliar indevidamente os riscos à privacidade e à proteção dos titulares dos dados.

Assim, sempre que possível, devem ser adotadas medidas de mitigação, como a supressão de identificadores desnecessários, o mascaramento parcial de informações e a divulgação em grau compatível com a finalidade pretendida. Tais medidas não inviabilizam o acesso à informação nem comprometem o controle social, mas promovem a compatibilização entre os princípios da publicidade administrativa e da proteção de dados pessoais, em conformidade com o regime jurídico estabelecido pela LAI e pela LGPD.

Casos como a disponibilização do nome completo, juntamente com sua matrícula e outros dados pessoais não necessários expõe ao risco não podendo ser considerado controle social e sim divulgação irrestrita e sem controle no tratamento de dados pelo poder público.

Não está se falando em não publicar, mas em saber como fazê-lo. Ao disponibilizar outros meios mais assertivos e menos invasivos para que a sociedade possa realizar sua função social de controle iríamos alcançar melhor o objetivo, pois a divulgação aberta não representa controle social e sim exposição sem controle, pois o controle social se dá de forma ativa pela sociedade e não de forma passiva com a simples exposição.

Trata-se de contribuições à consulta pública relativa ao Guia de Transparência Proteção de Dados Pessoais, promovida pela Controladoria Geral da União.

Faz-se oportuno suscitar a necessidade de que o documento apresente, de forma mais estruturada, o arcabouço jurídico no qual se insere o direito à proteção de dados pessoais e os contornos e limites do tratamento de dados pessoais pela Administração Pública. Assim, com vistas a contribuir para as análises que serão realizadas, apresenta-se aspectos relevantes para consideração e superação de lacunas.

De plano, invoca-se a Lei nº 12.527/2011, a Lei de Acesso à Informação (LAI). A norma determina, no art. 31, que o tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais e ainda estabelece que as informações poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem (§ 1º, inciso II).

Ao relativizar o consentimento em casos específicos (art. 31, § 3º), o citado diploma legal reconhece que, em relação à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, **está vedada a identificação da pessoa a que as informações se referirem (§ 3º, II). Ademais, explicita que "aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido" (§ 2º).**

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

(...)

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

(grifos nossos)

Por seu turno, a Lei nº 13.079/2018, que institui a Lei Geral de Proteção de Dados Pessoais (LGPD) afirma, entre seus fundamentos, o respeito à privacidade e à autodeterminação informativa, conforme dispõe seu art. 2º, incisos I e II. Os mecanismos de proteção conferidos pela Lei incidem sobre os dados pessoais (informação relacionada à pessoa natural identificada ou identificável, art. 5º, I) e dado pessoal sensível (dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou

político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, art. 5º, II).

A LGPD define que as atividades de tratamento de dados pessoais deverão observar os seguintes princípios (art. 6º): (i) eleição de propósitos legítimos, específicos, explícitos e informados ao titular; (ii) compatibilidade, ou adequação, do tratamento com as finalidades informadas ao titular; (iii) limitação do tratamento ao mínimo necessário para a realização das atividades; (iv) garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento; e (v) utilização de medidas técnicas de segurança aptas a proteger os dados pessoais de acessos não autorizados ou de situações ilícitas de alteração, comunicação ou difusão.

Quanto aos órgãos governamentais, a lei prevê um rol taxativo de hipóteses em que se considera legítimo o tratamento de dados por pessoas jurídicas de direito público, a saber: (i) execução de políticas públicas (arts. 7º e 11); e (ii) cumprimento de atribuições institucionais, como a execução de competências ou atribuições legais do serviço público (art. 23).

A lei também exige que os agentes públicos informem as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, inclusive em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (art. 23, inciso I).

Portanto, no contexto do compartilhamento de dados, a LGPD traz dispositivos específicos que asseguram a observância, pelo Estado, do direito constitucional à proteção de dados pessoais na manutenção de bases de dados em plataformas estruturadas para uso compartilhado, cabendo aos gestores públicos o desenvolvimento de mecanismos de interoperabilidade em prol da confiabilidade, do aprimoramento da gestão de políticas públicas e da atuação articulada dos diversos órgãos estatais na prestação de serviços públicos. Vejamos:

Lei nº 13.709/2018

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, **respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.**

(grifos nossos)

Assim, ao autorizar o compartilhamento de dados pessoais para o atendimento às atribuições legais dos órgãos e entidades da Administração Pública, a LGPD vincula a obrigatoriedade de observância aos princípios de proteção dos dados pessoais constantes do art. 6º da Lei. O citado dispositivo foi regulamentado pelo Decreto n.º 10.046/2019, cuja constitucionalidade foi devidamente apreciada pelo STF.

Cite-se o Decreto:

Decreto nº 10.046/2019

Art. 4º O compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º é categorizado em três níveis, de acordo com sua confidencialidade:

I - compartilhamento amplo, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;

II - compartilhamento restrito, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; e

III - compartilhamento específico, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados.

(...)

§ 4º Nas solicitações de interoperabilidade que envolvam dados pessoais, serão explicitados, além do disposto no § 3º:

I - o propósito legítimo, específico e explícito;

II - a compatibilidade com a finalidade; e

III – o compartilhamento do mínimo necessário para atendimento da finalidade.

(grifos nossos)

Por sua vez, a Lei nº 14.129/2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, faz remissão à LGPD, especialmente prevendo que o compartilhamento de dados pessoais, fruto da ação integrada entre órgãos públicos, deverá ser implementado sob a égide daquela Lei Geral:

Art. 3º São princípios e diretrizes do Governo Digital e da eficiência pública:

(...)

IX - a atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle dos serviços públicos, com o compartilhamento de dados pessoais em ambiente seguro quando for indispensável para a prestação do serviço, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e, quando couber, com a transferência de sigilo, nos termos do art. 198 da Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), e da Lei Complementar nº 105, de 10 de janeiro de 2001;

(grifos nossos)

Vale destacar que a Lei do Governo Digital também sinaliza para a necessidade de observância à LGPD, na perspectiva da proteção dos dados pessoais, nas hipóteses de implementação de mecanismos de interoperabilidade de bases de dados pelo Poder Público:

Art. 38. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de dados pessoais, conforme estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverão gerir suas ferramentas digitais, considerando:

I - a interoperabilidade de informações e de dados sob gestão dos órgãos e das entidades referidos no art. 2º desta Lei, respeitados as restrições legais, os requisitos de segurança da informação e das comunicações, as limitações tecnológicas e a relação custo-benefício da interoperabilidade;

II - a otimização dos custos de acesso a dados e o reaproveitamento, sempre que possível, de recursos de infraestrutura de acesso a dados por múltiplos órgãos e entidades;

III - a proteção de dados pessoais, observada a legislação vigente, especialmente a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

(grifos nossos)

Dessa forma, tem-se que a Lei do Governo Digital remete à LGPD para disciplinar os processos de compartilhamento de dados pessoais entre os órgãos públicos e da adoção de mecanismos de interoperabilidade, trazendo à tona novamente a aplicação dos princípios consubstanciados no art. 6º da Lei Geral e em seu regulamento, a respeito da proteção de dados incidentes sobre as atividades em tela.

Portanto, tanto a LGPD como a Lei do Governo Digital impõem limites à Administração Pública para o tratamento de dados pessoais, e, eventual compartilhamento de informações entre órgãos governamentais deverá, com amparo nas diretrizes, regulamentos e observar os princípios gerais e demais mecanismos de proteção aos dados pessoais previstos na LGPD, sendo certo que esse é o entendimento externado pelo Supremo Tribunal Federal ao ser instado sobre o tema.

Com efeito, o STF, ao examinar o contexto das relações entre os gestores públicos e os titulares de dados pessoais, vem definindo mais precisamente os limites e as salvaguardas institucionais que se aplicam ao compartilhamento de informações entre órgãos e entidades da administração pública federal, considerando ainda que o tema se encontra sujeito à reserva de jurisdição.

De pronto, a partir da jurisprudência da Suprema Corte, invoca-se a ADI 6.387, de relatoria da Eminentíssima Ministra Rosa Weber, por meio da qual o STF reconhece a proteção de dados pessoais e o direito à autodeterminação informacional como direitos fundamentais autônomos na ordem jurídico-constitucional brasileira. Na ocasião, o STF barrou o compartilhamento de dados de operadoras de telefonia (nome, endereço, telefone) com o Instituto Brasileiro de Geografia e Estatística (IBGE), determinada pela Medida Provisória 954/2020, partindo da premissa de que os dados pessoais merecem a

tutela constitucional. O julgamento representou uma incursão emblemática da Corte no tema da proteção de dados pessoais, reconhecendo-o como direito fundamental.

Na sequência, têm-se os parâmetros necessários para aplicação do disposto no Decreto nº 10.046/2019, observados no julgamento conjunto da ADI 6.649 e da ADPF 695 e fixados pelo STF para calibrar, por meio de critérios objetivos e pragmáticos, as possibilidades do tratamento de dados pessoais:

ADI 6.649/DF e ADPF 695

1. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: **a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018), b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.**

2. O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, **“fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos”.**

(...)

4. O compartilhamento de informações pessoais em atividades de inteligência observará o disposto em legislação específica e os parâmetros fixados no julgamento da ADI 6.529, Rel. Min. Cármen Lúcia, quais sejam: **(i) adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público, (ii) instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; (iü) utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e (iv) observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.**

5. O tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito

de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de culpa ou dolo.

(grifos nossos)

A supracitada decisão tratou da inconstitucionalidade do Decreto nº 10.046/2019, conferindo-lhe uma interpretação conforme a Constituição, tendo em vista que o ato exorbitaria os poderes normativos conferidos ao Chefe do Executivo Federal e violaria o direito fundamental à proteção de dados pessoais. Na ocasião, o STF estabeleceu a interpretação das condições para aferição da adequação e da necessidade do compartilhamento pelos órgãos do Governo Federal e o fez calibrando, por meio de critérios objetivos e pragmáticos, as possibilidades do tratamento de dados pessoais por esses órgãos.

Dessa forma, devem ser devidamente conciliadas a atuação estatal no tratamento de dados pessoais e a proteção dos direitos dos cidadãos, por meio da definição de salvaguardas institucionais e procedimentos que preservem e assegurem o direito fundamental e submetam os órgãos públicos ao controle de legalidade sobre suas decisões nessa seara.

Por oportuno, colaciona-se a decisão do STF por ocasião do julgamento da ADI 6.529, por meio da qual a Corte Constitucional fixou o entendimento de que o compartilhamento de dados no âmbito do Sistema Brasileiro de Inteligência deve cumprir e preservar os direitos e garantias fundamentais dos cidadãos, bem como aqueles dispostos em acordos internacionais em que a República Federativa do Brasil seja parte ou signatária, e a legislação ordinária, com especial atenção aos deveres de motivação das solicitações, razoabilidade e proporcionalidade das demandas e proteção aos sigilos gravados por reserva de jurisdição.

ADI 6.529/DF

EMENTA: DIREITO CONSTITUCIONAL. AÇÃO DIRETA DE INCONSTITUCIONALIDADE. PARÁGRAFO ÚNICO DO ART. 4º DA LEI N. 9.883/99. INTERESSE PÚBLICO FORMALMENTE DEMONSTRADO COMO ÚNICO ELEMENTO LEGITIMADOR DO DESEMPENHO ADMINISTRATIVO. VEDAÇÃO AO ABUSO DE DIREITO E AO DESVIO DE FINALIDADE. OBRIGATORIEDADE DE MOTIVAÇÃO DO ATO ADMINISTRATIVO QUE SOLICITA DADOS DE INTELIGÊNCIA AOS ÓRGÃOS DO SISTEMA BRASILEIRO DE INTELIGÊNCIA. NECESSÁRIA OBSERVÂNCIA DA CLÁUSULA DE RESERVA DE JURISDIÇÃO. DEFERIMENTO PARCIAL DA MEDIDA CAUTELAR PARA DAR INTERPRETAÇÃO CONFORME AO PARÁGRAFO ÚNICO DO ART. 4º DA LEI N. 9.883/99.

1. A jurisprudência deste Supremo Tribunal é firme no sentido da necessidade de se identificarem as normas questionadas na ação direta de inconstitucionalidade, esclarecendo-se os argumentos justificadores do pleito. Ação conhecida parcialmente, quanto ao parágrafo único do art. 4º da Lei n. 9.883/1999

2. A efetividade das atividades de inteligência associa-se, com frequência, ao caráter sigiloso do processo e das informações coletadas. No Estado Democrático de Direito essa função

submete-se ao controle externo do Poder Legislativo (inc. X do art. 49 da Constituição) e do Poder Judiciário (inc. XXXV do art. 5º da Constituição) para aferição da adequação do sigilo decretado às estritas finalidades públicas a que se dirige.

3. Para validade do texto legal e integral cumprimento ao comando normativo infralegal do Poder Executivo, há de se adotar como única interpretação e aplicação juridicamente legítima aquela que conforma a norma à Constituição da República. É imprescindível vincularem-se os dados a serem fornecidos ao interesse público objetivamente comprovado e com motivação específica.

4. O fornecimento de informação entre órgãos que não cumpra os rigores formais do direito nem atenda estritamente ao interesse público, rotulado legalmente como defesa das instituições e do interesse nacional, configura abuso do direito, contrariando a finalidade legítima posta na norma legal.

5. Práticas de atos contra ou à margem do interesse público objetivamente demonstrado, especificado em cada categoria jurídica, devem ser afastadas pelo Poder Judiciário, quando comprovado o desvio de finalidade.

6. A ausência de motivação expressa impede o exame da legitimidade de atos da Administração Pública, incluídos aqueles relativos às atividades de inteligência, pelo que a motivação é imprescindível.

7. A prática de atos motivados pelo interesse público não torna juridicamente válidos comportamentos de órgãos do Sistema Brasileiro de Inteligência para fornecerem à ABIN dados configuradores de quebra do sigilo telefônico ou de dados. Competência constitucional do Poder Judiciário.

8. Ação direta de inconstitucionalidade julgada parcialmente procedente para, confirmando-se o julgado cautelar, dar interpretação conforme ao parágrafo único do art. 4º da Lei n. 9.883/1999 estabelecendo-se que: a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) qualquer solicitação de dados deverá ser devidamente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo presente interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo legal, decorrente do imperativo de respeito aos direitos fundamentais; d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso.

Assim, conforme referendado pelo Supremo Tribunal Federal nas diversas oportunidades aqui expostas, o compartilhamento de dados entre órgãos e instituições do Poder Público estabelecido a partir de contornos constitucionalmente adequados é matéria de extrema relevância para a proteção do direito constitucional à privacidade (art. 5º, caput e incisos X, da Constituição Federal), em razão da importância dessa garantia fundamental para uma sociedade democrática.

Mais ainda, o STF reconhece o direito à proteção de dados pessoais e à autodeterminação informacional como um novo direito fundamental, integrado ao texto constitucional de forma destacada do direito à privacidade como uma garantia de abstenção do Estado na esfera privada individual diante de um agir estatal desprovido de requisitos objetivos aptos a assegurar o controle de legalidade da conduta dos agentes públicos.

Por fim, na esteira do reconhecimento do direito à proteção de dados pessoais, suscitam-se os incisos X, XIV e XXXIII, do art. 5º, da CF/1988, visto que eventual violação àquele direito pode igualmente ensejar lesão aos seguintes direitos fundamentais, conforme já assinalou o STF:

Art. 5º:

(...)

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

(...)

XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

(...)

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

4. Garantindo a transparência pública com proteção dos dados pessoais

COLETA DE DADOS (ATRAVÉS) DE TERCEIROS

A respeito do tópico “Revisar fluxos de trabalho e procedimentos” (4.3 Transparência por desenho), seria interessante ampliar a abordagem especificamente quanto à coleta de dados de terceiros. Os exemplos incluídos nesta parte parecem obscurecer e estreitar a orientação, cuja redação foi muito breve.

Além de faltar neste Guia mais aprofundamento quanto ao problema da coleta (o Guia deveria focar um pouco mais didaticamente na coleta com finalidade natural ao órgão/entidade), faltou também versar sobre o problema de coleta de dados de terceiros. Não apenas isso, mas algo ainda mais questionável: coleta de dados de terceiros através de terceiros, de modo indireto (e enviesado).

Um caso concreto: recentemente, o INEP abriu inscrições para o ENEM. Ao se inscrever, o candidato era forçado a responder a uma pesquisa “socioeconômica”, a qual, como sabemos, nada mais é do que coleta de dados à revelia, uma vez que, se o candidato não respondesse à pesquisa, sua matrícula não era efetivada — prática, a propósito, comum não apenas ao INEP, mas a vários outros órgãos de governo. O maior problema, porém, era que a pesquisa não apenas coletava dados do candidato, mas também o usava como meio de obter dados de sua família, com questões do tipo “até que série seu pai estudou?” e outras relacionadas (incluindo renda).

Assim, seria importante tratar neste Guia a respeito de dados que passam a estar em guarda do governo após obtidos pelo poder público mediante terceiros. Em alguma parte desta Consulta Pública, um representante do Hospital Israelita demonstrou a mesma preocupação, ao contribuir com casos concretos em que dados de um paciente acabavam sendo coletados juntamente com os de terceiros, como em situações de acompanhantes de pacientes. Esses exemplos são preocupantes, mas bastante comuns. Parece haver certa irresponsabilidade do poder público tanto com a coleta indiscriminada de dados sem finalidade, como ainda mais com respeito a dados de terceiros através de não titulares desses dados.

Ao longo deste item 4, versou-se em diversos pontos sobre como dispor de dados pessoais solicitados por terceiros/não titulares. Faltou trazer à baila a outra versão desse problema, que consiste no uso, por parte do poder público, de terceiros para obtenção de dados cuja titularidade não lhes pertence.

**Consulta Pública - Guia de Transparência e Proteção de Dados Pessoais - Agência
Nacional de Proteção de Dados (ANPD)**

Consolidação das Contribuições do Laboratório de Inovação e Direitos Digitais da UFBA

Ficha técnica:

Coordenação

Amanda Oliveira de Aragão
Arnaldo de Santana

Redação

Amanda Oliveira de Aragão
Gabriel Ferreira dos Santos
Henrique Perez Carneiro
Larissa Alves dos Santos

Revisão

Amanda Oliveira de Aragão
Arnaldo de Santana
Jeiel de Santana Barbosa

1. INTRODUÇÃO

O Laboratório de Inovação e Direitos Digitais (LABIDD) da Universidade Federal da Bahia (UFBA) parabeniza a Autoridade Nacional de Proteção de Dados (ANPD) pela elaboração do Guia de Transparência e Proteção de Dados Pessoais e pela abertura do presente processo de consulta pública. A construção participativa de orientações regulatórias é fundamental para o fortalecimento da segurança jurídica, da governança pública e da proteção dos direitos fundamentais no contexto da transformação digital do Estado.

A crescente digitalização da Administração Pública torna cada vez mais necessária a harmonização entre o direito de acesso à informação e a proteção de dados pessoais. Nesse cenário, o Guia é uma importante iniciativa para promover maior clareza interpretativa e uniformidade na aplicação conjunta da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados Pessoais (LGPD).

Em consonância com sua missão institucional de fomentar uma governança digital ética, democrática e centrada nos direitos fundamentais, o LABIDD realizou uma análise detalhada do texto submetido à consulta. As contribuições apresentadas em anexo buscam colaborar, de forma construtiva, para o aprimoramento do Guia, especialmente quanto à sua precisão conceitual, segurança interpretativa e aplicabilidade prática.

Por fim, reiteramos nossos cumprimentos pela condução da iniciativa e colocamo-nos à disposição para contribuir com futuras discussões relacionadas à transparência, governança de dados e proteção de direitos fundamentais no ambiente digital.

2. CONTRIBUIÇÕES

2.1. Direito de acesso à informação e seus limites

Contexto:

A Seção 1 do Guia apresenta fundamentos importantes sobre o direito de acesso à informação, as hipóteses de restrição de acesso e a articulação entre transparência pública e proteção de dados pessoais. Contudo, alguns trechos poderiam apresentar maior precisão conceitual e operacional quanto aos critérios de aplicação das restrições previstas na Lei de Acesso à Informação (LAI), especialmente no que se refere à fundamentação das negativas de acesso, à interpretação das exceções ao princípio da publicidade e à harmonização entre LAI e Lei Geral de Proteção de Dados Pessoais (LGPD).

Além disso, conceitos como “pedido desproporcional”, “documento preparatório” e “interesse público” permanecem relativamente abertos, o que pode gerar insegurança jurídica e assimetrias interpretativas na atuação dos órgãos públicos. Nesse contexto, recomenda-se o fortalecimento de parâmetros relacionados à proporcionalidade, necessidade, motivação administrativa e governança informacional, de modo a reforçar a aplicação uniforme do princípio da máxima divulgação e evitar restrições excessivamente amplas ao acesso à informação.

Proposta:

- **Aprimoramento dos Critérios de Restrição de Acesso à Informação (Seção 1):** Recomenda-se explicitar que as hipóteses de restrição ao acesso à informação devem observar não apenas previsão legal expressa, mas também critérios de necessidade, proporcionalidade, motivação concreta e interpretação restritiva, em conformidade com o princípio da máxima divulgação previsto na LAI.

- **Delimitação da Aplicação de Hipóteses Restritivas:** Sugere-se esclarecer que a classificação de informações exige fundamentação individualizada quanto aos riscos concretos decorrentes da divulgação, não sendo suficiente o mero enquadramento abstrato nas hipóteses legais de sigilo. Da mesma forma, recomenda-se delimitar objetivamente a noção de “documento preparatório”, reforçando seu caráter temporário e sua vinculação a processo decisório efetivamente em curso.
- **Harmonização entre Transparência Pública e Proteção de Dados:** Recomenda-se reforçar expressamente que a existência de dados pessoais em documentos ou bases públicas não implica restrição automática de acesso, exigindo análise contextual e ponderação entre transparência, privacidade e interesse público. Também se sugere detalhar a proteção autoral das hipóteses de sigilo previstas na LAI, evitando interpretações ampliativas sobre a restrição de acesso à informação pública.
- **Fortalecimento da Governança Informacional e da Motivação Administrativa:** Sugere-se incorporar orientações mais objetivas sobre a caracterização de pedidos “desproporcionais” e de “produção de informação”, evitando negativas excessivamente amplas fundadas em dificuldades operacionais. Recomenda-se, ainda, reforçar o dever permanente de gestão documental, organização informacional e governança de dados no âmbito da Administração Pública, em alinhamento com os princípios da eficiência, transparência e proteção de dados pessoais.

2.2. **Direito à proteção de dados pessoais e da privacidade nos termos da Lei Geral de Proteção de Dados - LGPD**

Contexto:

A Seção 2 do Guia aborda o direito à proteção de dados pessoais e à privacidade no contexto da Administração Pública, apresentando os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), o regime jurídico aplicável ao tratamento de dados pelo Poder Público e a compatibilização entre proteção de dados e transparência pública. O texto contribui para esclarecer que a proteção de dados pessoais deve ser

interpretada em harmonia com a Lei de Acesso à Informação (LAI), evitando leituras equivocadas que transformem a LGPD em fundamento autônomo de sigilo administrativo.

Contudo, alguns pontos poderiam receber maior aprofundamento operacional e regulatório, especialmente quanto à gestão de riscos no compartilhamento e na divulgação de dados pessoais pelo Poder Público. Em particular, a Seção 2.2 menciona que “o uso secundário, o compartilhamento e a divulgação de dados pessoais devem ser devidamente justificados, à luz do interesse público envolvido e dos riscos potenciais de dano aos titulares”, mas não orienta os órgãos públicos quanto à necessidade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) em hipóteses de tratamento de alto risco. Essa lacuna é especialmente relevante considerando que órgãos públicos frequentemente realizam operações envolvendo bases de dados em larga escala, inclusive contendo dados pessoais sensíveis, o que pode configurar tratamento de alto risco nos termos dos parâmetros já adotados pela própria ANPD. A ausência de referência ao RIPD reduz a operacionalização prática do princípio da responsabilização e prestação de contas (*accountability*), além de limitar a incorporação de mecanismos preventivos de governança e mitigação de riscos.

Além disso, a redação da Seção 2.3 poderia reforçar que, embora a LGPD não crie novas hipóteses de sigilo nem altere o regime jurídico das restrições de acesso previstas na LAI, seus princípios e regras orientam quanto a forma de tratamento, disponibilização, minimização e proteção dos dados pessoais constantes das informações públicas.

Proposta:

- **Inclusão de Diretriz sobre Relatório de Impacto à Proteção de Dados Pessoais - RIPD (Seção 2.2):** Sugere-se incluir orientação expressa no sentido de que, quando o compartilhamento, uso secundário ou divulgação de dados pessoais configurar tratamento de alto risco, recomenda-se a elaboração prévia de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), nos termos do art. 38 da LGPD.

Exemplo:

- Quando o compartilhamento ou a divulgação de dados pessoais configurar tratamento de alto risco, recomenda-se a

elaboração prévia do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), nos termos do art. 38 da LGPD. Para fins de identificação do tratamento de alto risco, deve-se observar os critérios definidos no art. 4º da Resolução CD/ANPD nº 2/2022, adotado pela própria ANPD como parâmetro até a edição de regulamentação específica.

- Além disso, recomenda-se que o RIPD seja revisado periodicamente, com a definição da periodicidade de revisão baseada no nível de risco do tratamento, de modo que tratamentos mais sensíveis ou dinâmicos demandem revisões mais frequentes, enquanto tratamentos de menor risco possam observar intervalos mais espaçados, conforme avaliação justificada pelo agente de tratamento.

- **Vinculação aos Critérios de Alto Risco Adotados pela ANPD:**

Recomenda-se esclarecer que a identificação de tratamento de alto risco deve observar os parâmetros previstos no art. 4º da Resolução CD/ANPD nº 2/2022, atualmente utilizados pela própria ANPD como referência regulatória até a edição de regulamentação específica sobre RIPD. Nesse sentido, devem ser considerados critérios gerais, como tratamento em larga escala e potencial impacto significativo aos direitos fundamentais dos titulares, bem como critérios específicos, incluindo utilização de dados pessoais sensíveis, decisões automatizadas, monitoramento de áreas acessíveis ao público e uso de tecnologias emergentes ou inovadoras.

- **Fortalecimento da Governança Preventiva no Compartilhamento e**

Divulgação de Dados: Sugere-se reforçar que operações de compartilhamento e divulgação de dados pessoais pelo Poder Público, especialmente quando envolverem bases massivas ou dados sensíveis, devem incorporar mecanismos preventivos de gestão de riscos, documentação das decisões administrativas, avaliação de impactos e adoção de salvaguardas técnicas e organizacionais adequadas, em consonância com os princípios da necessidade, segurança, prevenção e responsabilização previstos na LGPD.

- **Aprimoramento da Redação sobre Compatibilização entre LGPD e**

LAI (Seção 2.3): Sugere-se substituir a redação: “É fundamental

reforçar que a LGPD não cria hipóteses de sigilo no âmbito da Administração Pública, nem altera o rol de informações restritas.” Por: “Embora a LGPD não crie novas hipóteses de sigilo nem altere o regime jurídico de restrições de acesso previsto na LAI, seus princípios e regras orientam a forma de tratamento, disponibilização, minimização e proteção dos dados pessoais constantes das informações públicas.”

- Complementarmente, recomenda-se reforçar expressamente que a presença de dados pessoais em documentos, processos ou bases públicas não implica restrição automática de acesso, exigindo análise contextual, motivada e proporcional entre transparência, proteção da privacidade e interesse público.

2.3. Proteção de dados pessoais prevista na LAI

Contexto:

A Seção 3 do Guia aborda a proteção de dados pessoais prevista na Lei de Acesso à Informação (LAI), especialmente quanto ao conceito de informação pessoal protegida, às hipóteses de acesso por titulares e terceiros e às responsabilidades decorrentes do tratamento dessas informações. O capítulo contribui para esclarecer a distinção entre dados pessoais e informações pessoais protegidas, bem como para compatibilizar o regime de transparência pública com a proteção da privacidade e dos direitos da personalidade.

Contudo, alguns trechos podem ser aprimorados para oferecer maior precisão conceitual e segurança operacional aos agentes públicos responsáveis pela análise de pedidos de acesso envolvendo dados pessoais. Em especial, recomenda-se o fortalecimento de orientações sobre a função institucional do Estado como custodiante de dados pessoais, os limites da aplicação do chamado “sigilo de 100 anos”, os critérios para exigência de informações contextuais mínimas em pedidos de acesso por terceiros e os parâmetros técnicos aplicáveis à anonimização e pseudonimização de dados.

Também se observa a necessidade de esclarecer de forma mais explícita a compatibilização entre o art. 10, §3º da LAI (que veda exigências relativas à motivação do requerente) e as hipóteses excepcionais previstas no art. 31, §3º da mesma lei, nas quais determinadas informações contextuais mínimas

podem ser necessárias para verificar objetivamente o enquadramento da solicitação em uma base legal autorizativa específica.

Além disso, a redação atualmente utilizada para tratar da impossibilidade de reidentificação em processos de anonimização estabelece padrão técnico absoluto incompatível com o próprio conceito de anonimização previsto na LGPD e com o estado da arte científico sobre riscos de reidentificação, especialmente em ambientes públicos marcados por interoperabilidade e compartilhamento de bases de dados¹.

Proposta:

- **Aprimoramento Conceitual sobre Informação Pessoal Protegida (Seção 3.1):** Sugere-se incluir ressalva expressa de que, embora o Estado não seja titular dos dados pessoais tratados pela Administração Pública, exerce função institucional de custódia e tratamento dessas informações, estando sujeito a deveres reforçados de legalidade, segurança, governança, proporcionalidade e responsabilização no tratamento de dados pessoais.
 - Recomenda-se, ainda, inserir esclarecimento de que as categorias utilizadas na tabela explicativa sobre intimidade, vida privada, honra e imagem possuem caráter exemplificativo e podem apresentar zonas de sobreposição no caso concreto, devendo a avaliação da proteção considerar o contexto do tratamento, a finalidade da divulgação, o potencial lesivo da exposição e a existência de interesse público relevante.
- **Aprimoramento da Redação sobre Restrição de Acesso por até 100 Anos:** Sugere-se reformular a explicação sobre o prazo máximo de

¹ A impossibilidade técnica de anonimização perfeita está documentada na literatura científica consolidada:

- Narayanan, Arvind; Shmatikov, Vitaly. "Myths and fallacies of 'personally identifiable information'". Communications of the ACM, v. 53, n. 6, p. 24-26, 2010. Os autores demonstraram, no estudo do banco de dados da Netflix, a reidentificação de usuários com acurácia superior a 90% a partir de dados aparentemente anônimos, mediante cruzamento com informações publicamente disponíveis.
- Sweeney, Latanya. "Simple demographics often identify people uniquely." Carnegie Mellon University, 2000. O estudo demonstrou que 87% da população americana era identificável unicamente a partir de três variáveis: código ZIP, gênero e data de nascimento; presentes em dados públicos do censo.

restrição de acesso previsto no art. 31 da LAI para esclarecer que o prazo de até 100 anos possui natureza excepcional e deve ser aplicado apenas quando estritamente necessário e proporcional à proteção dos direitos da personalidade envolvidos, mediante fundamentação concreta e individualizada.

- **Esclarecimento sobre Exigência de Informações Contextuais Mínimas em Pedidos de Acesso por Terceiros (Seção 3.3):**

Sugere-se inserir nota introdutória ou parágrafo explicativo no início da Seção 3.3 esclarecendo que, como regra geral, o art. 10, §3º da LAI veda que o órgão público exija do requerente qualquer justificativa ou motivação para pedidos de informações de interesse público geral, em observância ao princípio da máxima divulgação:

- "Como regra geral, o art. 10, §3º da LAI veda que o órgão exija do requerente qualquer justificativa ou motivação para o pedido de informação. Essa vedação reflete o princípio da máxima divulgação e é absoluta para pedidos de informações de interesse público geral.
- Entretanto, algumas das hipóteses autorizativas de acesso a informações pessoais protegidas previstas no art. 31, §3º da LAI têm como pressuposto lógico a apresentação de informações contextuais mínimas pelo requerente, não porque o órgão possa julgar a legitimidade da motivação pessoal, mas porque o próprio texto legal condiciona a exceção ao enquadramento em uma finalidade específica que o órgão precisa ser capaz de verificar.
- Isso ocorre, por exemplo, na hipótese de pesquisas e estatísticas (art. 31, §3º, III), que exige que a pesquisa tenha 'objetivos de evidente interesse público ou geral': sem informações mínimas sobre o objeto e os objetivos da pesquisa, o órgão não consegue verificar esse requisito. O mesmo ocorre na hipótese de defesa de direitos humanos (art. 31, §3º, IV), que exige avaliação da necessidade da informação para a proteção do direito ameaçado.
- A exigência de informações mínimas nessas hipóteses não viola o art. 10, §3º da LAI porque não se trata de julgar se a motivação do requerente é 'aceitável', mas de verificar se o caso concreto se enquadra objetivamente nos pressupostos

da exceção legal aplicada. Nas hipóteses em que a finalidade está embutida na própria base legal, como no cumprimento de ordem judicial ou de obrigação legal específica, nenhuma informação contextual adicional é necessária."

- **Aprimoramento da Redação sobre Anonimização e Reidentificação (Seção 3.4):** Sugere-se substituir a expressão "sem possibilidade de reidentificação" por formulação compatível com o art. 5º, inciso XI da LGPD, reconhecendo que a anonimização deve ser avaliada considerando os meios técnicos razoáveis e disponíveis na ocasião do tratamento.
 - Recomenda-se a seguinte redação: "Quando as informações forem fornecidas de forma anonimizada ou pseudonimizada, de modo que a reidentificação do titular não seja possível por meios técnicos razoáveis e disponíveis na ocasião do tratamento, nos termos do art. 5º, inciso XI da LGPD, a assinatura de termo de responsabilidade poderá ser dispensada. O órgão deve documentar os critérios técnicos adotados para a anonimização, considerando o risco de reidentificação por cruzamento com outras bases de dados disponíveis, especialmente em contexto de dados públicos."
- Sugere-se, adicionalmente, incorporar referência à necessidade de avaliação contínua dos riscos de reidentificação, especialmente em ambientes públicos marcados pela interoperabilidade de bases de dados e pela possibilidade de cruzamento informacional em larga escala.

2.4. Garantindo a transparência pública com proteção dos dados pessoais

Contexto:

A Seção 4 do Guia trata da compatibilização entre transparência pública e proteção de dados pessoais, apresentando orientações práticas para tomada de decisão administrativa em pedidos de acesso à informação envolvendo dados pessoais. O capítulo representa importante esforço de operacionalização conjunta da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente ao propor roteiros decisórios voltados à ponderação entre publicidade, privacidade e interesse público.

Contudo, alguns dispositivos ainda conferem excessiva margem de subjetividade ao agente público, especialmente quanto à utilização do consentimento como fundamento para acesso a informações pessoais de terceiros, à identificação do interesse público preponderante e à motivação das decisões administrativas. Também se observa a necessidade de incorporar parâmetros metodológicos mais objetivos para aplicação do teste de proporcionalidade, bem como diretrizes operacionais relacionadas à arquitetura da informação, governança tecnológica e contratação de soluções digitais compatíveis com os princípios de transparência e proteção de dados.

Além disso, a redação atual da Seção 4.1 pode induzir interpretação excessivamente ampla do consentimento no contexto das relações entre cidadão e Administração Pública, desconsiderando a assimetria estrutural existente entre Estado e administrado. A lógica do Direito Administrativo é marcada pela verticalidade e pela presença de prerrogativas públicas, circunstância que frequentemente compromete a liberdade necessária para caracterização de consentimento válido nos termos da LGPD.

Nesse contexto, recomenda-se o fortalecimento de mecanismos de fundamentação, governança e controle decisório, de modo a reduzir arbitrariedades, ampliar a segurança jurídica e assegurar que a transparência pública seja implementada em conformidade com os princípios da finalidade, necessidade, proporcionalidade, *accountability* e proteção de direitos fundamentais.

No mais, um dos principais desafios observados reside na efetividade da atuação do Encarregado pelo tratamento de dados pessoais (DPO). Em muitos casos, essa função acaba sendo exercida de forma meramente formal ou burocrática, frequentemente acumulada com outras atribuições administrativas e sem a devida especialização técnica necessária para o adequado desempenho do papel. Diante disso, entende-se pertinente que o guia dedique atenção específica à valorização institucional do DPO, como agente central de governança em proteção de dados. Isso porque é justamente o DPO o responsável por articular, orientar e monitorar a implementação das diretrizes que o próprio guia busca consolidar, sendo sua capacitação e estrutura de atuação elementos essenciais para a efetividade do regime de proteção de dados na administração pública.

Proposta:

- **Cautela com o Consentimento face à Assimetria de Poder (Seção 4.1 - Passo 3):** Sugere-se incluir nota de alerta no Passo 3 esclarecendo que o consentimento não deve ser buscado pela Administração Pública como mecanismo para contornar a ausência de base legal adequada de Direito Público para compartilhamento ou divulgação de dados pessoais. Recomenda-se orientar expressamente os agentes públicos a avaliarem se a eventual autorização apresentada foi obtida de forma efetivamente livre, informada e imune a pressões decorrentes da relação assimétrica entre Estado e cidadão.
 - Recomenda-se, ainda, alteração metodológica no roteiro decisório para que o agente público avalie prioritariamente o enquadramento da solicitação nas hipóteses de interesse público e geral preponderante ou de defesa de direitos humanos, atualmente previstas nos Passos 4 e 5. Considerando que a LAI estabelece a publicidade como regra geral da atuação administrativa, a fundamentação baseada em institutos próprios do regime jurídico de Direito Público oferece maior segurança jurídica e alinhamento com o Capítulo IV da LGPD, evitando banalização do consentimento como fundamento residual para divulgação de dados pessoais.
 - Nesse sentido, recomenda-se incorporar ressalva de que a base legal do consentimento no âmbito do Poder Público possui aplicação residual e excepcional, conforme entendimento já consolidado pela doutrina especializada e por orientações da própria ANPD, especialmente em situações nas quais a manifestação de vontade do titular esteja condicionada ao exercício de direitos, acesso a serviços públicos ou relações marcadas por subordinação material e jurídica.
- **Aprimoramento Metodológico da Identificação do Interesse Público e Geral Preponderante (Seção 4.2):** Sugere-se substituir a referência genérica à “ponderação” por metodologia estruturada baseada nos três subcritérios clássicos do teste de proporcionalidade, a serem aplicados cumulativamente nos Passos 4 e 6 do roteiro decisório:

- **Adequação:** A divulgação do dado pessoal específico é um meio idôneo para alcançar a finalidade de interesse público identificada?
 - **Necessidade:** Inexiste outro meio menos gravoso para a privacidade do titular (como anonimização, pseudonimização ou apresentação de dados agregados) que atinja o mesmo resultado de controle social?
 - **Proporcionalidade em sentido estrito:** As vantagens democráticas da publicidade superam, no caso concreto, os prejuízos causados aos direitos do titular?
-
- **Vinculação da Motivação Administrativa e Teoria dos Motivos Determinantes (Seção 4.2 – Passo 6):** Sugere-se incluir orientação expressa acerca da necessidade de fundamentação qualificada da decisão administrativa, esclarecendo que os fundamentos indicados pela autoridade pública vinculam a validade do ato administrativo, nos termos da Teoria dos Motivos Determinantes e do art. 50, inciso I, da Lei nº 9.784/1999. Recomenda-se alertar expressamente que²:
 - (i) motivações genéricas baseadas em conceitos abstratos;
 - (ii) ausência de análise de alternativas menos gravosas;
 - (iii) omissão de avaliação concreta de riscos; ou
 - (iv) utilização de premissas fáticas incorretas pode ensejar nulidade do ato administrativo, nos termos dos arts. 20 e 21 da LINDB.
 - **Fortalecimento da Transparência por Desenho e da Privacidade desde a Concepção (Seção 4.3):** Sugere-se incorporar diretriz metodológica expressa determinando que a Transparência por Desenho seja implementada de forma integrada à Privacidade desde a Concepção (*Privacy by Design*). Nesse sentido, recomenda-se que plataformas e sistemas de governo eletrônico incorporem, desde sua arquitetura inicial:
 - (i) mecanismos nativos de criptografia;
 - (ii) funcionalidades automáticas de anonimização e pseudonimização;

² Sugere-se, ainda, esclarecer que o descumprimento desses deveres analíticos pode sujeitar a decisão à invalidação pelos órgãos de controle e à responsabilização pessoal do agente público.

- (iii) controles para prevenção de divulgação excessiva de dados pessoais; e
 - (iv) ferramentas voltadas à disponibilização prioritária de dados agregados e contextualizados.
- Recomenda-se destacar que a adoção dessas medidas busca assegurar simultaneamente a efetividade do controle social, a conformidade com a LAI e a proteção adequada dos direitos fundamentais dos titulares de dados pessoais.
- **Vinculação às Contratações Públicas de Tecnologia e Governança Digital (Seção 4.3):** Sugere-se incluir orientação expressa para que os órgãos públicos incorporem requisitos de Privacidade desde a Concepção (*Privacy by design*) diretamente nos Estudos Técnicos Preliminares (ETP) e nos Termos de Referência (TR) relacionados à contratação de soluções de Tecnologia da Informação, em conformidade com a Lei nº 14.133/2021.
 - Recomenda-se prever que editais e contratos administrativos incluam, como requisitos técnicos não funcionais:
 - (i) funcionalidades nativas de mascaramento automático de documentos;
 - (ii) trilhas seguras de auditoria;
 - (iii) mecanismos de extração facilitada de dados agregados;
 - (iv) controles de rastreabilidade e governança informacional; e
 - (v) medidas técnicas compatíveis com as exigências da LGPD e da Lei de Governo Digital (Lei nº 14.129/2021).
- Sugere-se reforçar que a integração entre transparência, proteção de dados e governança tecnológica deve ocorrer desde a modelagem técnica, contratual e operacional das soluções digitais adotadas pela Administração Pública, reduzindo retrabalho, insegurança jurídica e riscos de exposição indevida de dados pessoais.
- Sugere-se, por fim, que o guia reforce o fortalecimento institucional da figura do Encarregado pelo tratamento de dados pessoais (DPO) na Administração Pública, de modo a assegurar que suas atribuições sejam exercidas de forma efetiva e não meramente formal. Isso envolve a previsão de parâmetros mínimos de qualificação técnica, a recomendação de estrutura de apoio adequada e a orientação para

que o exercício da função não seja acumulado de maneira a comprometer sua independência e capacidade operacional.

- Busca-se, assim, consolidar o DPO como agente central de governança em proteção de dados, responsável por articular a implementação das diretrizes do próprio guia e reduzir riscos de desconformidade, insegurança jurídica e fragilidades na proteção de dados pessoais.

2.5. Entendimentos sobre a publicidade de dados pessoais

Contexto:

A Seção 5 do Guia detalha a publicidade de dados em cenários consolidados, como processos disciplinares, licitações e programas sociais.

No entanto, observa-se uma lacuna quanto ao uso de tecnologias de biometria e sistemas de reconhecimento facial para controle de acesso a prédios públicos ou vigilância, atividades que a ANPD classifica como de alto risco. O tratamento desses dados sensíveis pode afetar significativamente a privacidade e a autodeterminação informativa, exigindo cautela redobrada quando envolvem crianças, adolescentes ou idosos.

Embora o Guia já oriente sobre listas de controle de acesso físico, ele não estabelece limites claros sobre a publicidade ativa do funcionamento dessas tecnologias e o necessário sigilo dos dados sensíveis por elas gerados.

Proposta:

- **Inclusão do item "Dados biométricos e tecnologias de reconhecimento facial no setor público"**, com as seguintes diretrizes:
 - Transparência sobre o uso da tecnologia: Em observância ao princípio da transparência, o órgão deve divulgar proativamente a finalidade específica, a base legal e o período de retenção dos modelos biométricos, garantindo que o cidadão seja informado antes da coleta.
 - Publicação de versões públicas dos Relatórios de Impacto (RIPD) para tratamentos dessa natureza.
 - Natureza Sensível e Negativa de Acesso: Dados biométricos, como digitais e representações matemáticas de faces, são dados sensíveis.

- Pedidos de acesso por terceiros via LAI a essas informações devem ser negados para proteger a intimidade, permitindo-se apenas o fornecimento de dados estatísticos agregados sobre o uso da tecnologia que não permitam a reidentificação.
- Melhor Interesse de Grupos Vulneráveis: Quando o sistema captar dados de crianças e adolescentes, o órgão deve publicizar como o princípio do "melhor interesse" foi garantido, adotando salvaguardas adicionais para evitar a exposição indevida ou discriminação algorítmica.
- Transparência por Desenho: Os fluxos de trabalho devem ser estruturados para segregar *logs* de acesso (que podem ser públicos, como nome e horário de entrada) dos dados biométricos propriamente ditos, que devem permanecer sob sigilo.
- Limitação do Legítimo Interesse: O uso do legítimo interesse como base legal para biometria no setor público deve ser evitado em tratamentos compulsórios ou no exercício de prerrogativas estatais típicas, priorizando-se a base de "cumprimento de obrigação legal" ou "execução de políticas públicas".

À

Controladoria-Geral da União (CGU) e Agência Nacional de Proteção de Dados (ANPD)

Assunto: *Tomada de Subsídios sobre o Guia Orientativo “Fornecedores de Produtos ou Serviços de Tecnologia da Informação”, no âmbito do ECA Digital.*

Prezados(as),

Em atenção à Consulta Pública aberta em 09 de junho de 2026, promovida pela Controladoria-Geral da União (CGU) e pela Agência Nacional de Proteção de Dados (ANPD), o escritório de advocacia **Szazi, Bechara, Storto, Reicher e Figueirêdo Lopes Advogados (SBSA Advogados)**¹ vem apresentar recomendações e sugestões com relação ao Guia de Transparência e Proteção de Dados Pessoais, com o objetivo de aprimorar o documento na parte relativa ao tratamento de dados pessoais em contextos que envolvem organizações da sociedade civil (OSCs) na sua relação jurídica e financeira com a Administração Pública.

Fundado em 2002, SBSA Advogados é escritório pioneiro e especializado em Direito do Terceiro Setor, Responsabilidade Social, Meio Ambiente, Direito Público e Direitos Humanos, com mais de duas décadas de atuação dedicada a organizações da sociedade civil que promovem direitos fundamentais, incluindo direitos de crianças e adolescentes, pessoas com deficiência, povos indígenas, comunidades tradicionais e grupos em situação de vulnerabilidade. O escritório é reconhecido como escritório de referência no campo do Direito do Terceiro Setor pelas principais publicações internacionais de avaliação de escritórios de advocacia, com classificação Band 1 pelo *Chambers Latin America* e reconhecimento pelo *The Legal 500 Latin America*².

Ao longo dessa trajetória, o escritório consolidou posição de referência não apenas no Direito do Terceiro Setor - com participação ativa de seus sócios na formulação da Lei nº 9.790/1999 (Lei das OSCIPs) e da Lei nº 13.019/2014 (Marco Regulatório das Organizações da Sociedade Civil - MROSC), mas também em Direito Público, Responsabilidade Social, Meio Ambiente, Direitos Humanos, Proteção de Dados Pessoais e Direito Digital, áreas que se articulam de forma integrada na assessoria às organizações da sociedade civil e a seus parceiros públicos e privados. A interseção entre proteção de dados e terceiro setor tem sido

¹ Sociedade de advogados inscrita no CNPJ/MF sob o n. 05.276.071/0001-35, com sede em Curitiba/PR, na Rua Marechal Deodoro, nº 869, 2º andar, e sua filial inscrita no CNPJ/MF sob o n. 05.276.071/0002-16, localizada na Capital do Estado de São Paulo, na Av. Nove de Julho, nº 4865 – 8º andar, conj. 81.

² Reconhecimentos disponíveis em: <https://chambers.com/law-firm/szazi-bechara-storto-reicher-e-figueiredo-lobes-advogados-sbsa-brazil-95:193994> e <https://www.legal500.com/firms/236615-szazi-bechara-storto-reicher-e-figueiredo-lobes-advogados/c-brazil/about>. Acesso em: 18 jun. 2026.

objeto de atenção crescente do escritório junto à ANPD, da qual é interlocutor sistemático em processos regulatórios relevantes para o setor, incluindo contribuição apresentada à tomadas de subsídios e consultas públicas promovidas pela ANPD. A presente contribuição se insere nessa mesma linha de engajamento regulatório, motivada pela convicção de que a qualidade das orientações sobre transparência e proteção de dados no contexto das parcerias entre Estado e sociedade civil é condição para a legitimidade e a efetividade dessas relações.

INTRODUÇÃO

O Guia constitui ferramenta valiosa para a aplicação harmônica da Lei de Acesso à Informação (Lei nº 12.527/2011 - LAI) e da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD), oferecendo ao agente público um roteiro decisório estruturado (Capítulo 4) e parâmetros setoriais consolidados (Capítulo 5) para situações recorrentes. Entendemos, contudo, que o documento, na versão submetida à consulta, não enfrenta de forma expressa uma realidade institucional cada vez mais relevante: a execução de políticas públicas por meio de parcerias com OSCs, nos termos da Lei nº 13.019/2014 (Marco Regulatório das Organizações da Sociedade Civil - MROSC).

Essa lacuna é especialmente relevante porque a presença de uma OSC entre o cidadão (titular de dados, beneficiário final de um serviço público) e o Estado (parceiro, financiador, fiscalizador) introduz uma camada adicional na cadeia de tratamento de dados pessoais que o Capítulo 5 do Guia, tal como redigido, não contempla de forma direta. Sem essa explicitação, órgãos públicos repassadores de recursos a OSCs (que são, nos termos do art. 64 do Decreto nº 7.724/2012, os destinatários dos pedidos de acesso relativos ao conteúdo dessas parcerias) ficam sem parâmetro claro para responder a pedidos de acesso fundamentados na LAI relativos à execução dessas parcerias, recaindo, na prática, em soluções pouco uniformes: por vezes excessivamente protetivas (negando acesso a informações que deveriam ser públicas, sob alegação genérica de “dados pessoais”, prática que o próprio Enunciado CGU nº 12/2023, já citado no Guia, busca coibir) e por vezes insuficientemente protetivas (expondo dados de beneficiários finais em situação de vulnerabilidade, sob a justificativa de que “a parceria é pública”).

Esta contribuição integra o conjunto de manifestações que a SBSA Advogados tem apresentado à ANPD, sempre no sentido de promover o reconhecimento das particularidades das organizações da sociedade civil nos processos regulatórios da ANPD, sem prejuízo da efetiva proteção dos direitos fundamentais em jogo, sejam eles o direito de acesso à informação e ao controle social sobre o uso de recursos públicos, sejam os direitos à privacidade e à proteção de dados pessoais dos indivíduos envolvidos, especialmente quando em situação de vulnerabilidade.

Curitiba • PR
R. Marechal Deodoro, 869
2º andar • Cj. 201 • Centro
80060.010 • 55.41.3233.9040

São Paulo • SP
Av. Nove de Julho, 4865
8º e 11º andar • Torre A • Jd. Paulista
01407.902 • 55.11.3061.9040

Brasília • DF
SAUS • Quadra 1 • Bloco N
Edifício Terra Brasília • 3º andar • Sala 303
Asa Sul • 70070-941 • 55.61.3225.7980

A seguir, apresentamos: (1) o diagnóstico da lacuna identificada, à luz da estrutura do próprio Guia; (2) a aplicação da LAI e do MROSC às OSCs, com a sistematização das obrigações de transparência ativa e passiva já existentes; (3) a fundamentação adicional sobre a posição da OSC na cadeia de tratamento de dados pessoais; (4) referências de direito comparado; (5) a redação sugerida para inclusão de nova subseção no Capítulo 5; (6) o ajuste sugerido na tabela do item 4.2; (7) o ajuste complementar ao Passo 5 do roteiro decisório; e (8) considerações finais.

1. Diagnóstico: a posição da OSC na cadeia de tratamento de dados pessoais entre o cidadão e o Estado

O Capítulo 5 do Guia organiza-se a partir de categorias de relação jurídica com o Estado: agente público, fornecedor (licitações e contratos), beneficiário de programa social, estudante bolsista. Essas categorias pressupõem, em geral, uma relação bilateral: de um lado o Estado, de outro o indivíduo ou a empresa contratada.

Quando a execução de uma política pública se dá por meio de parceria com OSC (Lei nº 13.019/2014), surge uma relação triangular: o Estado repassa recursos públicos à OSC (relação OSC-Estado, regida por termo de fomento ou por termo de colaboração, conforme os arts. 2º, VII e VIII, e 16 da Lei nº 13.019/2014, sendo o acordo de cooperação o instrumento aplicável às parcerias sem transferência de recursos financeiros, nos termos do art. 2º, VIII-A, da mesma lei); a OSC, por sua vez, presta serviços a beneficiários finais (pessoas físicas) no exercício dessa parceria (relação OSC-beneficiário). A documentação que evidencia essa execução (planos de trabalho, relatórios de monitoramento, prestações de contas, pareceres técnicos de acompanhamento) fica, em regra, sob custódia tanto da OSC quanto do órgão público parceiro, mas é este último (e não a OSC) o destinatário, em regra, dos pedidos de acesso à informação relativos ao conteúdo da parceria, nos termos do art. 64 do Decreto nº 7.724/2012, como se detalha no item 2 desta contribuição. A OSC, por sua vez, está sujeita a um dever de transparência ativa específico e limitado (art. 63 do mesmo Decreto), que não se confunde com o regime de transparência passiva aplicável aos órgãos públicos.

Essa documentação contém, tipicamente, três camadas distintas de dados pessoais, que merecem tratamento diferenciado à luz do próprio roteiro decisório do Capítulo 4 do Guia:

- (i) **Primeira camada: dados de identificação institucional da OSC e de seus representantes na execução da parceria.** Nome da entidade, CNPJ, e dados do(s) responsável(is) técnico(s) e dirigente(s) que figuram no plano de trabalho como interlocutores da parceria. Essa camada é estruturalmente análoga à do “representante legal da empresa contratada”, já tratada na tabela de licitações

e contratos do Guia (página 37), que prevê a divulgação do nome completo e cargo, com CPF descaracterizado.

- (ii) **Segunda camada: dados de equipe técnica operacional da OSC vinculada à execução do objeto.** Profissionais (assistentes sociais, educadores, profissionais de saúde) que executam diretamente o serviço. Diferentemente da primeira camada, essa categoria já possui tratamento expresso no próprio MROSC, como se detalha no item 2.2 abaixo - o que reforça a necessidade de o Guia dialogar com essa legislação setorial.
- (iii) **Terceira camada: dados de beneficiários finais pessoas físicas dos serviços executados pela OSC.** Pacientes, alunos, famílias atendidas, pessoas em situação de vulnerabilidade social. O próprio Guia já trata, na tabela do item 4.2 (página 28), o cenário do “prontuário médico de usuário do SUS” e das “beneficiárias de programa de proteção à vítima”, concluindo, em ambos os casos, pela negativa de acesso individualizado, com possibilidade de fornecimento de dados agregados ou anonimizados. Entendemos que essa mesma lógica decisória deve se aplicar, de forma expressa, quando o serviço de saúde, assistência social, educação ou proteção é executado por OSC parceira, e não diretamente por órgão público - a mudança do executor não altera a natureza do dado nem o risco ao titular.

2. A aplicação da LAI e do MROSC às OSCs: obrigações já existentes que o Guia pode sistematizar

Um ponto que entendemos central (e que a versão atual do Guia **não** explora) é que a LAI já incide diretamente sobre as OSCs que executam recursos públicos, e não apenas sobre os órgãos públicos que repassam esses recursos. O Guia trata exclusivamente da perspectiva do órgão público que responde a pedidos de acesso; propomos que passe a reconhecer também a perspectiva da OSC como sujeito de obrigações de transparência, o que tornaria o documento referência útil tanto para órgãos públicos quanto para as próprias entidades parceiras - ampliando seu impacto prático.

2.1. O regime diferenciado de transparência da OSC perante a LAI: ativa limitada, passiva direcionada ao órgão público

É importante precisar, antes de prosseguir, qual é exatamente o regime de transparência aplicável à OSC por força da LAI - e esse regime não é equivalente ao do órgão público, tampouco lhe é subsidiário em todos os pontos. O art. 63 do Decreto nº 7.724/2012, que regulamenta a LAI no âmbito federal, estabelece que as entidades privadas sem fins lucrativos que recebem

Curitiba • PR
R. Marechal Deodoro, 869
2º andar • Cj. 201 • Centro
80060.010 • 55.41.3233.9040

São Paulo • SP
Av. Nove de Julho, 4865
8º e 11º andar • Torre A • Jd. Paulista
01407.902 • 55.11.3061.9040

Brasília • DF
SAUS • Quadra 1 • Bloco N
Edifício Terra Brasília • 3º andar • Sala 303
Asa Sul • 70070-941 • 55.61.3225.7980

recursos públicos para realização de ações de interesse público devem dar publicidade ativa apenas a três conjuntos de informação: (i) cópia do estatuto social atualizado; (ii) relação nominal atualizada dos dirigentes da entidade; e (iii) cópia integral dos instrumentos de parceria, seus aditivos, e os relatórios finais de prestação de contas. Trata-se de rol taxativo, e não exemplificativo.

Mais relevante ainda para os fins desta contribuição: o art. 64 do mesmo Decreto estabelece, de forma expressa, que os pedidos de informação referentes aos instrumentos de parceria (para além do que já consta do dever de transparência ativa do art. 63) devem ser apresentados diretamente ao órgão público responsável pelo repasse dos recursos, e não à OSC. Há, portanto, uma escolha regulatória deliberada de não impor à OSC o mesmo regime de transparência passiva (resposta a pedidos LAI) que vincula os órgãos públicos: a entidade tem um dever de publicidade ativa limitado e específico, e a responsabilidade por responder pedidos de acesso adicionais sobre a parceria recai sobre o ente público repassador, que detém a documentação completa e está estruturalmente mais preparado para aplicar a ponderação entre transparência e proteção de dados que o roteiro do Capítulo 4 do Guia exige.

Essa distinção é central para a presente contribuição, e a reforça, pois é exatamente porque o órgão público (e não a OSC) é o sujeito que responde, em regra, aos pedidos de acesso sobre a parceria, que o Guia precisa orientá-lo especificamente sobre como tratar a documentação dessas parcerias, que contém as três camadas de dados pessoais já descritas no item 1. Ao mesmo tempo, essa distinção também impõe um limite à própria proposta desta contribuição: as sugestões aqui apresentadas não devem ser lidas como criação de um dever de transparência passiva equivalente para a OSC, sob pena de sobrecarregá-la com obrigações que o legislador, de forma deliberada, optou por não lhe atribuir.

2.2. O art. 11 do MROSC como núcleo de transparência ativa específico para parcerias

A Lei nº 13.019/2014³ já estabelece, no caput do art. 11, a obrigação de a OSC divulgar, em seu sítio na internet (caso mantenha) e em locais visíveis de suas sedes sociais e estabelecimentos, todas as parcerias celebradas com o poder público. O parágrafo único do mesmo artigo (aplicável também às informações que o art. 10 impõe ao órgão público divulgar)

³ LOPES, Laís de Figueirêdo. Novo Regime Jurídico da Lei nº 13.019/2014 e do Decreto Federal nº 8.726/2016: construção, aproximações e diferenças das novas relações de fomento e de colaboração do Estado com Organizações da Sociedade Civil. In: MOTTA, Fabrício; MÂNICA, Fernando Borges; SALINAS, Natasha Schmitt Caccia (Coord.). Parcerias com o Terceiro Setor: as inovações da Lei nº 13.019/14. 2ª ed. Belo Horizonte: Fórum, 2018, p. 29-57. Disponível em: <https://sbsa.com.br/lopes-lais-de-figueiredo-lopes-novo-regime-juridico-da-lei-13-109-2014-e-do-decreto-federal-8-726-2016-construcao-aproximacoes-e-diferencas-das-novas-relacoes-de-fomento-e-de-colaboracao/>. Acesso em: 18 jun. 2026.

detalha o conteúdo mínimo dessa divulgação, incluindo, no inciso VI, de forma especialmente relevante para esta contribuição, o valor total da remuneração da equipe de trabalho vinculada à execução do objeto e paga com recursos da parceria, as funções desempenhadas por seus integrantes e a remuneração prevista para o exercício⁴.

A existência desse dispositivo confirma que o legislador do MROSC já enfrentou, ainda que indiretamente, a questão da publicidade de dados pessoais (remuneração de profissionais identificáveis) no contexto de parcerias com OSCs - fornecendo ao Guia um ponto de partida normativo concreto para a “segunda camada” de dados (equipe técnica operacional). É preciso notar, contudo, que o art. 11, parágrafo único, VI, ampara apenas a divulgação do valor total e agregado da remuneração da equipe, das funções desempenhadas e da remuneração prevista, não a divulgação individualizada por nome. A individualização nominal (associação direta entre nome, cargo e valor) encontra previsão apenas em ato infralegal (o art. 42, § 4º, do Decreto nº 8.726/2016), e não deve ser equiparada, sem mais, à divulgação da remuneração de servidores públicos prevista no próprio Guia, que pressupõe vínculo estatutário ou empregatício direto com a Administração Pública, circunstância ausente na relação entre a OSC e sua equipe técnica. Essa diferença de hierarquia normativa e de natureza do vínculo suscita questão relevante para os fins desta contribuição: tratando-se de tratamento de dado pessoal de terceiro sem vínculo direto com a Administração, é necessário avaliar se um decreto regulamentador satisfaz o padrão de base legal exigido pelo art. 23 da LGPD para esse tipo de divulgação - questão que esta contribuição não pretende resolver, mas que recomenda seja enfrentada de forma expressa pelo Guia, e não presumida.

2.3. O art. 87 do MROSC como precedente normativo de exceção por proteção da segurança do titular

O próprio MROSC já reconhece, no art. 87, que as exigências de transparência e publicidade nele previstas (em todas as etapas que envolvem o termo de fomento ou de colaboração, desde a fase preparatória até o fim da prestação de contas, naquilo em que for necessário) podem ser excepcionadas quando se tratar de programa de proteção a pessoas ameaçadas ou em situação que possa comprometer sua segurança, na forma do regulamento. Trata-se de precedente normativo direto, no próprio marco legal das parcerias com OSCs, para a “terceira camada” de dados (beneficiários finais em situação de vulnerabilidade) - e que dialoga precisamente com a lógica já adotada pelo Guia para “beneficiárias de programa de proteção à vítima” (página 28) e para usuários do SUS.

⁴ LOPES, Laís de Figueirêdo; SANTOS, Bianca dos; BROCHARDT, Viviane. Entenda o MROSC: Marco Regulatório das Organizações da Sociedade Civil – Lei 13.019/2014. Brasília: Presidência da República, 2016. Disponível em: <https://sbsa.com.br/lopes-lais-de-figueiredo-lopes-et-al-entenda-o-mrosc-marco-regulatorio-das-organizacoes-da-sociedade-civil-lei-13-019-2014/>. Acesso em: 18 jun. 2026.

A combinação dos arts. 11 e 87 do MROSC demonstra que a legislação aplicável a parcerias com OSCs já contempla, em sua estrutura, a mesma lógica de gradação que o Guia propõe para o setor público em geral: divulgação ampla de dados institucionais e de remuneração de equipe vinculada à execução (regra geral de transparência), com exceção pontual e fundamentada para dados cuja divulgação comprometa a segurança do titular (beneficiário em situação de vulnerabilidade). Falta ao Guia apenas tornar essa articulação explícita, de modo que o agente público que recebe um pedido LAI sobre uma parceria com OSC saiba que pode e deve dialogar com os arts. 11 e 87 do MROSC, e não apenas com as categorias genéricas do Capítulo 5 pensadas para outros contextos.

2.4. Distinção entre prestação de contas a financiadores públicos e privados

É importante que o Guia também reconheça, ainda que brevemente, que muitas OSCs operam com financiamento misto (recursos públicos e privados, de pessoas físicas, empresas, outras OSCs nacionais e internacionais)⁵. A obrigação de transparência decorrente da LAI e do MROSC incide sobre a parcela de recursos públicos e sua destinação, não sobre a totalidade das operações financeiras e institucionais da entidade. Essa delimitação é relevante para que pedidos de acesso dirigidos a OSCs (ou a órgãos públicos sobre documentação de OSCs) não sejam interpretados, por arrastamento, como autorização para acesso à integralidade da prestação de contas da entidade a outros financiadores - o que extrapolaria o objeto da LAI e poderia, inclusive, expor informações protegidas por relações contratuais privadas sem qualquer base legal.

3. A LGPD e as OSCs: precedente regulatório da ANPD e princípio de proporcionalidade aplicável ao contexto das parcerias

Em contribuição apresentada à ANPD no âmbito da Tomada de Subsídios sobre o Guia Orientativo de Aplicação do ECA Digital (Lei nº 15.211/2025) a Fornecedores de Produtos e Serviços de Tecnologia, SBSA Advogados defendeu que as organizações da sociedade civil não devem ser equiparadas a fornecedores comerciais de tecnologia para fins de incidência das obrigações mais gravosas da legislação de proteção de dados, em razão de sua finalidade não lucrativa, de sua função de interesse público e da natureza dos tratamentos de dados por elas realizados. Naquela oportunidade, argumentamos que a lógica de modulação proporcional já reconhecida pela ANPD na Resolução CD/ANPD nº 2/2022 - que confere tratamento

⁵ A respeito dessa realidade de financiamento visto, recomendamos a leitura de PANNUNZIO, Eduardo; SOUZA, Aline Gonçalves de. Sustentabilidade econômica das Organizações da Sociedade Civil: desafios do ambiente jurídico brasileiro atual. São Paulo: FGV Direito SP / CPJA, [s.d.]. Disponível em: <https://sbsa.com.br/gestao-de-organizacoes-da-sociedade-civil/>. Acesso em: 18 jun. 2026.

diferenciado a "agentes de tratamento de pequeno porte", categoria que expressamente inclui pessoas jurídicas sem fins lucrativos (associações, fundações, organizações religiosas e partidos políticos) - é manifestação de um princípio mais amplo: o de que a forma de cumprimento das obrigações de proteção de dados e de transparência deve ser proporcional à natureza, ao porte e à finalidade da entidade, sem que isso implique redução dos direitos dos titulares de dados.

Esse mesmo princípio, que poderíamos denominar de "modulação na via de cumprimento, não na titularidade do direito", é diretamente aplicável ao presente Guia. O ponto central não é que OSCs mereçam menor transparência ou maior proteção de dados pessoais do que outras categorias de parceiros do Estado. É que a cadeia de obrigações e a alocação de responsabilidades entre o órgão público repassador, a OSC executora e os beneficiários finais tem uma configuração específica (triangular, como descrito no item 1) que o Guia, ao tratar exclusivamente da perspectiva do órgão público, ainda não capturou adequadamente.

Vale destacar que a intersecção entre LGPD e terceiro setor tem sido objeto de atenção crescente no debate regulatório brasileiro. A própria ANPD, ao incluir expressamente as pessoas jurídicas sem fins lucrativos no rol de agentes de tratamento de pequeno porte (art. 2º, II, da Resolução CD/ANPD nº 2/2022), reconheceu que as OSCs ocupam posição peculiar no ecossistema de proteção de dados: tratam, em regra, grandes volumes de dados pessoais sensíveis (saúde, origem racial, vulnerabilidade socioeconômica, dados de crianças e adolescentes), mas o fazem em contexto de interesse público, com recursos limitados e sob regime de transparência já regulado por extensa legislação específica (o MROSC e variadas outras). A extensão dessas considerações ao plano da transparência ativa e passiva (que é precisamente o objeto do presente Guia) é, portanto, um passo natural e necessário na construção de uma regulação coerente e efetiva para esse universo.

Finalmente, é relevante registrar que o tema da publicidade de dados pessoais no contexto de parcerias com OSCs é objeto de debate permanente no campo do Direito do Terceiro Setor. A ausência de orientação clara sobre o que deve ou não ser divulgado em parcerias com OSCs tem sido fonte de insegurança jurídica para gestores públicos e para as próprias entidades, e tem sido instrumentalizada, em alguns casos, tanto para negar acesso legítimo a informações públicas quanto para expor indevidamente dados de beneficiários em situação de vulnerabilidade. A presente contribuição busca, portanto, preencher exatamente essa lacuna que a literatura especializada e a prática regulatória já identificaram.

4. Referências de direito comparado

4.1. União Europeia: Sistema de Transparência Financeira como modelo de "núcleo público mínimo"

Curitiba • PR
R. Marechal Deodoro, 869
2º andar • Cj. 201 • Centro
80060.010 • 55.41.3233.9040

São Paulo • SP
Av. Nove de Julho, 4865
8º e 11º andar • Torre A • Jd. Paulista
01407.902 • 55.11.3061.9040

Brasília • DF
SAUS • Quadra 1 • Bloco N
Edifício Terra Brasília • 3º andar • Sala 303
Asa Sul • 70070-941 • 55.61.3225.7980

A Comissão Europeia mantém, desde 2007 para fundos administrados diretamente e desde 2010 para o Fundo Europeu de Desenvolvimento, um sistema público de busca que permite a qualquer cidadão descobrir os nomes dos beneficiários dos fundos atribuídos anualmente pela Comissão Europeia, bem como o montante e a finalidade do financiamento e a localização geográfica do destinatário. As informações disponíveis nesse sistema incluem a identidade dos beneficiários, a finalidade da despesa, a localização geográfica do beneficiário, o montante e tipo de despesa, e o serviço responsável pela concessão do financiamento⁶.

Esse sistema foi desenhado a partir de parecer formal da Autoridade Europeia para a Proteção de Dados (AEPD) sobre o Regulamento Financeiro da União, no qual a Autoridade reconheceu expressamente que “a transparência, em especial, tem de ser reforçada, fornecendo informações sobre os beneficiários de fundos comunitários” como princípio de boa gestão financeira a ser apoiado, ao mesmo tempo em que recomendou que sua implementação adotasse “uma abordagem proativa” que observasse devidamente os direitos à proteção de dados e à privacidade dos titulares envolvidos⁷.

O modelo europeu oferece, assim, precedente direto e verificável para a proposta de “núcleo público mínimo” desta contribuição: a identidade da entidade beneficiária (incluindo organizações sem fins lucrativos), o valor, a finalidade e a origem do recurso são tratados como informação pública por definição (análoga, no contexto brasileiro, à “primeira camada” de dados institucionais da OSC parceira), deixando para análise específica apenas os dados pessoais que extrapolam essa informação essencial.

4.2. Tribunal de Justiça da União Europeia: Caso C-184/20 e o limite da proporcionalidade mesmo em regimes de transparência anticorrupção

Esse precedente, embora não trate diretamente de OSCs, oferece parâmetro relevante para a “segunda camada” de dados (equipe técnica/dirigentes) discutida nesta contribuição. O caso teve origem em lei lituana de combate à corrupção que exigia que agentes públicos e dirigentes de entidades que recebem fundos públicos fizessem declarações detalhadas de seus

⁶ Comissão Europeia. Sistema de Transparência Financeira (*Financial Transparency System*). Disponível em: https://commission.europa.eu/about/service-standards-and-principles/transparency/funding-recipients_pt. Acesso em: 13 jun. 2026.

⁷ Autoridade Europeia para a Proteção de Dados (AEPD). Parecer sobre o Regulamento Financeiro aplicável ao Orçamento Geral das Comunidades Europeias. Disponível em: https://edps.europa.eu/sites/default/files/publication/06-12-12_financial_regulation_pt.pdf. Acesso em: 13 jun. 2026.

interesses privados e dos de seus cônjuges/parceiros, incluindo doações, transações e situações semelhantes, publicadas integralmente na internet pela Comissão de Ética⁸.

O Tribunal de Justiça da União Europeia (TJUE), em julgamento de 1º de agosto de 2022, reconheceu que a finalidade de transparência e combate a conflitos de interesse constitui objetivo legítimo de interesse público, capaz de fundamentar o tratamento de dados pessoais com base no art. 6(1)(e) do RGPD - equivalente, no direito brasileiro, ao cumprimento de obrigação legal/regulatória do art. 7º, II, da LGPD. Contudo, o Tribunal estabeleceu que, mesmo amparada em finalidade legítima, a divulgação pública, online, de dados nominais relativos ao parceiro do declarante, ou a pessoas próximas a ele, é capaz de revelar informações sobre aspectos sensíveis da vida privada dos titulares, incluindo, por exemplo, sua orientação sexual⁹, e que tal divulgação ia além do que era estritamente necessário¹⁰ para o objetivo perseguido. O Tribunal reforçou, ainda, que os direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais não são absolutos, mas devem ser ponderados em relação à sua função social e equilibrados com outros direitos fundamentais¹¹, e que qualquer limitação a esses direitos deve observar o princípio da proporcionalidade, sendo a medida apropriada, adequada e estritamente necessária.

Esse precedente é diretamente transponível ao Guia: ao definir o que pode ser divulgado sobre dirigentes e responsáveis técnicos de OSCs parceiras (em nome da transparência sobre o uso de recursos públicos), o Guia deve circunscrever a divulgação ao indivíduo identificado formalmente no instrumento de parceria, em sua função naquela parceria, sem que essa lógica se estenda a familiares, dependentes ou outras pessoas vinculadas por relação meramente pessoal - exatamente o critério de “informação essencial versus informação acessória” que propomos incorporar ao Passo 5 do roteiro decisório (item 6 desta contribuição).

4.3. Reino Unido: a posição das “charities” perante o *Freedom of Information Act*

A experiência britânica ilustra, de forma complementar, a distinção entre o regime aplicável a uma entidade do terceiro setor em si e o regime aplicável à documentação que ela produz no contexto de uma relação com órgão público. De um lado, o *Freedom of Information Act* (FOIA) não necessariamente cobre toda organização que recebe recursos públicos - por exemplo, não abrange algumas *charities* que recebem *grants* e certas organizações do setor

⁸ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Caso C-184/20, OT v. *Vyriausioji tarnybinės etikos komisija* (Comissão Principal de Ética no Serviço Público da Lituânia). Julgamento de 1º de agosto de 2022. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid=264887&doclang=PT>. Acesso em: 18 jun. 2026.

⁹ Op. cit.

¹⁰ Op. cit.

¹¹ Op. cit.

privado¹², ou seja, a OSC não se torna, ela própria, sujeito passivo de pedidos de acesso à informação apenas por receber recursos públicos.

De outro lado, quando a *charity* celebra acordo de parceria ou de prestação de serviços com órgão público, a documentação relativa a essa relação pode, sim, ser objeto de pedido de acesso dirigido ao próprio órgão público. Conforme orientação de escritório especializado em direito do terceiro setor, *charities* que celebram acordos de subvenção com autoridades públicas costumam ser obrigadas a submeter relatórios de desempenho, e tais documentos também podem estar sujeitos ao FOIA; da mesma forma, quando a *charity* está envolvida na execução de um contrato de serviços públicos, a documentação interna gerada sobre o desempenho do contrato pode estar sujeita à divulgação¹³. A mesma fonte ressalva, contudo, que o FOIA reconhece a necessidade de proteger informação sensível, prevendo exceções relacionadas a interesses comerciais, quebra de confidencialidade ou dados pessoais¹⁴.

Esse modelo confirma, por via comparada, a estrutura da proposta apresentada nesta contribuição: a documentação de uma parceria entre OSC e órgão público é, em princípio, acessível, sujeita às mesmas ressalvas de dados pessoais de beneficiários finais já consolidadas no Guia para outros contextos (saúde, assistência social, proteção a vítimas) - modelo que, no Brasil, o art. 87 do MROSC já antecipa de forma específica para o terceiro setor, como visto no item 2.3.

5. Proposta de inclusão no Guia: nova subseção no Capítulo 5, denominada “Dados Pessoais com Organizações da Sociedade Civil”

Sugerimos a inclusão desta subseção ao final do Capítulo 5, após “Dados de estudantes beneficiários de bolsas e ações afirmativas”, mantendo a estrutura de texto corrido com tabela ilustrativa, no mesmo formato adotado pelas demais subseções do capítulo.

Redação sugerida

Dados pessoais em parcerias com organizações da sociedade civil (Lei nº 13.019/2014)

¹² Information Commissioner's Office (ICO). What is the FOI Act and are we covered?. Disponível em: <https://ico.org.uk/for-organisations/foi/what-is-the-foi-act-and-are-we-covered/>. Acesso em: 14 jun. 2026.

¹³ Russell-Cooke. Charities and the Freedom of Information Act: an overview. Disponível em: <https://www.russell-cooke.co.uk/news-and-insights/news/charities-and-the-freedom-of-information-act-an-overview>. Acesso em: 15 jun. 2026.

¹⁴ Op.cit.

A execução de políticas públicas por meio de parcerias com organizações da sociedade civil (OSCs), nos termos da Lei nº 13.019/2014 (Marco Regulatório das Organizações da Sociedade Civil - MROSC), gera documentação - planos de trabalho, relatórios de monitoramento e avaliação, prestações de contas técnicas e financeiras - que pode estar sob custódia tanto do órgão público parceiro quanto da própria OSC executora. É importante destacar que, por força do art. 63 do Decreto nº 7.724/2012, a própria OSC, na condição de executora de recursos públicos, está sujeita a um dever de transparência ativa limitado e taxativo (cópia do estatuto social atualizado, relação nominal de dirigentes, cópia do instrumento de parceria e relatórios finais de prestação de contas). Pedidos de acesso à informação referentes ao conteúdo da parceria que extrapolem esse rol devem ser dirigidos ao órgão público responsável pelo repasse dos recursos, nos termos do art. 64 do mesmo Decreto, e não à OSC, que não está sujeita ao mesmo regime de transparência passiva aplicável aos órgãos públicos. É justamente por isso que o presente Guia, destinado a orientar o agente público, precisa endereçar com clareza como tratar essa documentação, cuja análise deve distinguir três camadas de dados pessoais, com regime de divulgação diferenciado:

Em primeiro lugar, os dados de identificação institucional da parceria - razão social e CNPJ da OSC, objeto, valor, vigência, órgão concedente e modalidade da parceria (termo de fomento, termo de colaboração, acordo de cooperação) - não constituem dados pessoais e compõem o núcleo mínimo de transparência ativa, nos termos do art. 11, caput, da Lei nº 13.019/2014, devendo ser divulgados independentemente de requerimento.

*Em segundo lugar, os dados do(s) dirigente(s) e responsável(is) técnico(s) formalmente indicado(s) no plano de trabalho como interlocutores da parceria têm posição equiparável à do representante legal de empresa contratada (subseção “Dados pessoais em processos licitatórios e contratos administrativos” deste Guia): podem ser divulgados nome completo, cargo na entidade e função na parceria, com CPF fornecido de forma descaracterizada (***.999.999-**), conforme já decorre, quanto aos dirigentes, do art. 63, II, do Decreto nº 7.724/2012. Quanto à equipe técnica vinculada à execução do objeto, a legislação do MROSC trata o tema de forma fragmentada entre diferentes níveis normativos: o art. 11, parágrafo único, VI, da Lei nº 13.019/2014 exige a divulgação, em formato agregado, do valor total da remuneração da equipe de trabalho vinculada à execução do objeto, das funções desempenhadas por seus integrantes e da remuneração prevista; já o art. 42, §4º, do Decreto nº 8.726/2016 determina a divulgação individualizada desses valores, vinculados a nome e cargo. Recomenda-se que o Guia reconheça essa diferença de nível normativo e de grau de exposição, e que a aplicação do art. 42, §4º, observe os princípios da necessidade e da minimização sempre que a individualização não for estritamente necessária ao controle social pretendido. Recomenda-se, ainda, que o Guia oriente os órgãos públicos e as próprias OSCs a avaliar, à luz do art. 23 da LGPD, se a divulgação individualizada de remuneração de profissionais sem vínculo formal com a Administração Pública (fundamentada exclusivamente em decreto*

regulamentador, e não em lei em sentido formal) encontra base legal suficiente para esse tratamento de dado pessoal, especialmente diante da assimetria de poder entre a OSC empregadora e o profissional cuja remuneração é divulgada, fator que fragiliza eventual alegação de consentimento como base legal supletiva. Em nenhum dos casos a divulgação se estende a familiares, dependentes ou terceiros sem vínculo formal com a execução da parceria, ainda que mencionados incidentalmente em documentos internos da entidade.

Em terceiro lugar, os dados pessoais de beneficiários finais dos serviços executados pela OSC com recursos públicos - pacientes, alunos, famílias atendidas, pessoas em situação de vulnerabilidade socioeconômica ou de violência - seguem as categorias específicas já previstas neste Guia para a respectiva natureza do serviço (saúde, assistência social, educação, proteção à vítima), independentemente de o serviço ser executado diretamente pelo órgão público ou por OSC parceira. Essa conclusão está em linha com o próprio art. 87 da Lei nº 13.019/2014, que excepciona as exigências de transparência e publicidade da parceria quando se tratar de programa de proteção a pessoas ameaçadas ou em situação que possa comprometer sua segurança. Quando a prestação de contas contiver listas nominais de beneficiários atendidos, o órgão público responsável pelo repasse (como regra geral, principal destinatário de pedidos de acesso sobre a parceria, nos termos do art. 64 do Decreto nº 7.724/2012), ao receber o pedido de acesso relativo a essa documentação deve aplicar o roteiro decisório do Capítulo 4, priorizando o fornecimento de dados agregados (quantitativo de atendimentos, valores, indicadores de resultado, distribuição territorial) em detrimento da identificação individualizada, exceto quando esta for o próprio objeto do controle social pretendido - por exemplo, em caso de denúncia fundamentada sobre elegibilidade de beneficiário específico.

Por fim, é importante observar que a obrigação de transparência decorrente da LAI e do MROSC incide sobre a parcela de recursos públicos recebidos pela OSC e sua destinação, não sobre a integralidade das operações institucionais e financeiras da entidade - especialmente quando esta possui financiamento misto (recursos públicos e privados). Pedidos de acesso relativos a uma parceria específica não devem ser interpretados como autorização para acesso a informações sobre outras fontes de financiamento da OSC, alheias ao objeto do pedido.

A tabela a seguir resume os parâmetros sugeridos:

Camada de dado pessoal	Exemplos	Regra geral de divulgação	Observações
Identificação institucional da parceria	Razão social, CNPJ da OSC, objeto, valor,	Deve ser divulgado	Não constitui dado pessoal; integra transparência ativa

Curitiba • PR
R. Marechal Deodoro, 869
2º andar • Cj. 201 • Centro
80060.010 • 55.41.3233.9040

São Paulo • SP
Av. Nove de Julho, 4865
8º e 11º andar • Torre A • Jd. Paulista
01407.902 • 55.11.3061.9040

Brasília • DF
SAUS • Quadra 1 • Bloco N
Edifício Terra Brasília • 3º andar • Sala 303
Asa Sul • 70070-941 • 55.61.3225.7980

	vigência, órgão concedente		nos termos do art. 11, caput, da Lei nº 13.019/2014
Dirigente/responsável técnico da parceria	Nome completo, cargo, função no projeto, CPF	Pode ser divulgado, CPF descaracterizado	Posição equiparável a representante legal de contratado; não se estende a familiares ou terceiros
Equipe técnica vinculada à execução	Nome e remuneração de profissionais pagos com recursos da parceria	O valor total da remuneração da equipe é informação de transparência ativa, nos termos do art. 11, parágrafo único, VI, da Lei nº 13.019/2014. A divulgação individualizada (nome, cargo e valor) tem fundamento no art. 42, §4º, do Decreto nº 8.726/2016, cuja aplicação prática recomenda-se que a ANPD e a CGU avaliem com cautela, à luz da proporcionalidade e da necessidade de evitar exposição excessiva de profissionais sem vínculo formal de representação da parceria.	Distinção entre nível legal (agregado) e infralegal (individualizado); aplicar critério de necessidade do Passo 5 do roteiro decisório
Beneficiários finais pessoas físicas	Pacientes, alunos, famílias atendidas	Não deve ser divulgado de forma individualizada	Seguir categoria específica do serviço; art. 87 da Lei nº 13.019/2014 já prevê exceção por segurança do titular; priorizar dados agregados

6. Ajuste pontual sugerido no Guia: linha adicional na tabela do item 4.2 do Guia (“tipo de titular/proximidade com o Estado”)

Curitiba • PR
R. Marechal Deodoro, 869
2º andar • Cj. 201 • Centro
80060.010 • 55.41.3233.9040

São Paulo • SP
Av. Nove de Julho, 4865
8º e 11º andar • Torre A • Jd. Paulista
01407.902 • 55.11.3061.9040

Brasília • DF
SAUS • Quadra 1 • Bloco N
Edifício Terra Brasília • 3º andar • Sala 303
Asa Sul • 70070-941 • 55.61.3225.7980

A tabela do item 4.2 (página 23) estrutura-se sobre cinco categorias de titular (agente público, fornecedor, beneficiário de recursos públicos, usuário de serviços públicos), atribuindo a cada uma delas um gradiente de "proximidade com o Estado" e, portanto, de "expectativa de privacidade". Essa estrutura é útil e bem construída para os casos paradigmáticos que tem em mente, mas apresenta uma imprecisão relevante quando aplicada ao universo das organizações da sociedade civil: a categoria "Beneficiário de recursos públicos" foi concebida para o cidadão pessoa física destinatário de transferência de renda direta (Bolsa Família, BPC), e não para a OSC pessoa jurídica que recebe recursos para executar atividades de interesse público em regime de mútua cooperação com o Estado.

Essa distinção não é meramente terminológica. Ela tem consequências práticas diretas: a OSC executora de parceria não é "beneficiária" de um programa social no sentido da tabela - ela é, tecnicamente, um agente de execução de política pública, mais próxima, nessa função, da categoria "Fornecedor" do que da categoria "Beneficiário de recursos públicos". Tratá-la como beneficiária pode levar à aplicação de uma expectativa de privacidade mais alta do que a devida para os seus dirigentes e equipe, e paradoxalmente mais baixa do que a devida para os beneficiários finais dos serviços que ela presta.

Propomos, assim, que a tabela do item 4.2 receba uma linha adicional, e não apenas uma nota de rodapé, explicitando a posição das OSCs executoras de parcerias como categoria própria:

Tipo de Titular	Proximidade com o Estado	Expectativa de Privacidade	O que pode ser publicado? (em tese)
OSC executora de parceria com o poder público (dirigentes e responsáveis técnicos pelo objeto)	Média alta (análoga a fornecedor)	Média baixa	Nome completo; cargo na entidade; função na parceria; valor total da remuneração da equipe vinculada à execução do objeto, em formato agregado (art. 11, parágrafo único, VI, da Lei nº 13.019/2014), sendo que a divulgação individualizada, quando aplicável, segue o art. 42, §4º, do Decreto nº 8.726/2016, observado o princípio da necessidade, e condicionada à avaliação, pelo órgão público e pela OSC, da suficiência da base

Curitiba • PR
R. Marechal Deodoro, 869
2º andar • Cj. 201 • Centro
80060.010 • 55.41.3233.9040

São Paulo • SP
Av. Nove de Julho, 4865
8º e 11º andar • Torre A • Jd. Paulista
01407.902 • 55.11.3061.9040

Brasília • DF
SAUS • Quadra 1 • Bloco N
Edifício Terra Brasília • 3º andar • Sala 303
Asa Sul • 70070-941 • 55.61.3225.7980

			legal infralegal para esse tratamento de dado pessoal, nos termos do art. 23 da LGPD; CPF descaracterizado; não se estende a familiares ou terceiros sem vínculo formal

Ao mesmo tempo, deve ser registrado que os destinatários finais dos serviços prestados pela OSC com recursos públicos (crianças e adolescentes atendidos em programas socioeducativos, pacientes de clínicas conveniadas, famílias assistidas em programas de renda mínima, mulheres em situação de violência acolhidas em casas-abrigo) não são "beneficiários de recursos públicos" no sentido da categoria da tabela, mas usuários de um serviço público executado de forma indireta. Esses indivíduos apresentam, frequentemente, expectativa de privacidade ainda mais elevada do que a reconhecida para usuários de serviços públicos diretos, justamente porque sua presença em uma parceria com OSC pode revelar, por si só, situação de vulnerabilidade (condição socioeconômica, histórico de violência, condição de saúde) que nenhum dos critérios da tabela atual captura adequadamente. A nova subseção sugerida no item 5 desta contribuição é o veículo adequado para esse tratamento específico.

7. Ajuste complementar: inclusão de critério adicional no Passo 5 do Roteiro Decisório (item 4.1 do Guia)

O Passo 5 do roteiro decisório do Guia ("Análise da necessidade e da minimização dos dados") é, a nosso ver, o passo em que a aplicação ao contexto das parcerias com OSCs mais frequentemente falha na prática. Isso ocorre não porque o critério de minimização seja inadequado, mas porque, sem orientação específica, o agente público tende a aplicá-lo tomando como referência o dado em si (é um nome? é um CPF? é uma remuneração?) sem considerar a relação funcional entre o titular e o recurso público envolvido - que é o que, no contexto de uma parceria, determina se aquele dado é essencial ou acessório para o controle social pretendido.

O caso C-184/20 do Tribunal de Justiça da União Europeia¹⁵, já referido no item 4 desta contribuição, oferece precisamente esse critério relacional: o Tribunal estabeleceu que, mesmo em regimes de transparência com base legal clara, a minimização exige distinguir entre a informação estritamente necessária para demonstrar a relação entre o titular e a função

¹⁵ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Caso C-184/20, OT v. *Vyriausioji tarnybinės etikos komisija* (Comissão Principal de Ética no Serviço Público da Lituânia). Julgamento de 1º de agosto de 2022. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?docid=264887&doclang=PT>. Acesso em: 18 jun. 2026.

exercida ou o recurso administrado - e a informação que, embora relacionada ao titular, revela aspectos de sua vida pessoal sem conexão direta com essa função ou recurso. No caso concreto, a lei lituana exigia que dirigentes de entidades beneficiárias de recursos públicos declarassem publicamente não apenas seus próprios interesses, mas também os de cônjuges e parceiros - dados que o Tribunal considerou acessórios à finalidade de transparência e, portanto, excessivos à luz do princípio da minimização, independentemente de a divulgação ser legalmente prevista.

Esse critério é diretamente transponível ao roteiro do Guia e especialmente útil no contexto de parcerias com OSCs, onde é comum que a documentação de execução mencione, de forma incidental, pessoas sem vínculo formal com a parceria: familiares de dirigentes que participaram de eventos, voluntários não formalizados, doadores individuais da entidade, ou beneficiários que consentiram com o uso de sua imagem em materiais de comunicação da OSC mas não com a divulgação de seus dados em resposta a pedido de acesso à informação. Todos esses dados aparecem em documentos que são, em tese, parte da prestação de contas da parceria, mas nenhum deles é necessário para o controle social sobre o uso do recurso público.

Propomos, portanto, a inclusão da seguinte pergunta adicional na lista de aspectos a serem considerados no Passo 5 do roteiro decisório (página 25 do Guia):

“O dado pessoal cuja divulgação está sendo avaliada é estritamente necessário para demonstrar a relação entre o titular e o recurso público ou a função exercida - ou revela, de forma acessória, aspectos de sua vida pessoal, ou de pessoas a ele relacionadas, sem conexão direta com essa função ou recurso? Nesse último caso, a divulgação deve ser restringida mesmo que o documento em que o dado consta seja, em tese, público.”

Essa formulação é mais precisa do que simplesmente perguntar "o dado é necessário?" - porque esclarece que o parâmetro de necessidade não é o documento, mas a relação funcional do titular com o objeto do controle social. Um processo de prestação de contas de parceria pode ser publicamente acessível em sua integralidade financeira e técnica sem que isso implique a divulgação de todos os dados pessoais que nele aparecem incidentalmente - distinção que o Guia, em seu estado atual, não torna suficientemente explícita, e que esta pergunta adicional busca operacionalizar para o agente público.

CONSIDERAÇÕES FINAIS

As sugestões apresentadas nesta contribuição partem de uma constatação simples, mas com implicações práticas relevantes: o Guia de Transparência e Proteção de Dados Pessoais foi construído, em seu Capítulo 5, a partir de categorias que refletem relações bilaterais típicas da Administração Pública (Estado-servidor, Estado-contratado, Estado-

Curitiba • PR
R. Marechal Deodoro, 869
2º andar • Cj. 201 • Centro
80060.010 • 55.41.3233.9040

São Paulo • SP
Av. Nove de Julho, 4865
8º e 11º andar • Torre A • Jd. Paulista
01407.902 • 55.11.3061.9040

Brasília • DF
SAUS • Quadra 1 • Bloco N
Edifício Terra Brasília • 3º andar • Sala 303
Asa Sul • 70070-941 • 55.61.3225.7980

beneficiário de programa social). Essas categorias são bem construídas para os contextos que descrevem, mas deixam sem orientação um universo crescente de relações trilaterais (nas quais o Estado repassa recursos a uma OSC, que os aplica em favor de beneficiários finais) que é exatamente o modelo pelo qual grande parte das políticas públicas brasileiras nas áreas de assistência social, educação, cultura, saúde e direitos humanos tem sido executada nas últimas décadas, especialmente após a promulgação da Lei nº 13.019/2014.

O resultado dessa lacuna não é neutro. Na ausência de orientação clara, o órgão público (que, nos termos do art. 64 do Decreto nº 7.724/2012, é o sujeito que responde, em regra, a pedidos de acesso sobre o conteúdo das parcerias com OSCs) tem aplicado, por analogia, as categorias disponíveis - com resultados inconsistentes: ora tratam dirigentes de OSCs como se fossem beneficiários de programas sociais (atribuindo-lhes expectativa de privacidade mais alta do que a devida para quem administra recursos públicos), ora expõem dados de beneficiários finais em situação de vulnerabilidade como se fossem simplesmente "informações sobre a execução de uma parceria" (sem reconhecer que esses dados podem ser tão sensíveis quanto um prontuário médico ou o registro de um usuário de programa de proteção à vítima). Em ambos os casos, o resultado é o oposto do que o Guia pretende: nem mais transparência, nem mais proteção de dados, apenas mais insegurança jurídica para todos os envolvidos.

A proposta que apresentamos resolve esse problema pela via mais simples e mais consistente com o próprio método do Guia: não criando regime de exceção, mas estendendo explicitamente a lógica que o Guia já desenvolveu para outras categorias (especialmente agentes públicos, fornecedores e usuários de serviços de saúde) ao contexto específico das parcerias com OSCs, articulando essa extensão com os dispositivos que o próprio MROSC já contém sobre transparência ativa (art. 11, parágrafo único, VI, da Lei nº 13.019/2014, e art. 42, §4º, do Decreto nº 8.726/2016) e sobre proteção de beneficiários em situação de risco (art. 87 da Lei nº 13.019/2014), preservando, ao mesmo tempo, a opção regulatória já adotada pelos arts. 63 e 64 do Decreto nº 7.724/2012 de não equiparar o regime de transparência passiva da OSC ao do órgão público. Não estamos propondo que o Guia invente regras novas, estamos propondo que ele torne visíveis as regras que já existem, espalhadas entre a LAI, a LGPD e o MROSC, e que permaneçam inaplicadas por falta de um roteiro que as integre. Da mesma forma, a presente contribuição não pressupõe que a divulgação individualizada de remuneração da equipe técnica das OSCs seja, sem mais, uma prática já consolidada ou obrigatória - ao contrário, recomenda que o próprio Guia se posicione sobre os limites dessa prática à luz da LGPD, evitando que decretos regulamentadores sejam lidos como base legal automática para o tratamento de dados pessoais de profissionais sem vínculo direto com a Administração Pública.

Curitiba • PR
R. Marechal Deodoro, 869
2º andar • Cj. 201 • Centro
80060.010 • 55.41.3233.9040

São Paulo • SP
Av. Nove de Julho, 4865
8º e 11º andar • Torre A • Jd. Paulista
01407.902 • 55.11.3061.9040

Brasília • DF
SAUS • Quadra 1 • Bloco N
Edifício Terra Brasília • 3º andar • Sala 303
Asa Sul • 70070-941 • 55.61.3225.7980

Entendemos que o momento é especialmente oportuno. O Brasil conta hoje com mais de 685 mil organizações da sociedade civil ativas, segundo dados do IPEA¹⁶, e com um volume crescente de recursos públicos sendo repassados via MROSC a entidades que executam serviços de interesse coletivo. A qualidade da transparência sobre esse repasse (e a proteção adequada dos dados dos indivíduos que são atendidos por essas entidades) é condição para a legitimidade democrática de todo esse sistema. Um Guia que oriente os agentes públicos a distinguir o que deve ser público (a parceria, seus valores, seus responsáveis), o que está sujeito a regime de transparência ativa próprio e limitado por parte da OSC, e o que deve ser protegido (os dados de beneficiários vulneráveis) é, nesse contexto, não apenas uma ferramenta técnica, mas uma contribuição concreta à construção de uma Administração Pública mais transparente e mais responsável, sem sobrecarregar as organizações da sociedade civil com obrigações que a própria regulamentação da LAI optou, deliberadamente, por não lhes atribuir.

SBSA Advogados permanece à disposição da CGU e da ANPD para aprofundar, em audiências públicas ou contribuições complementares, os pontos aqui apresentados.

Atenciosamente,

p. Szazi, Bechara, Storto, Reicher e Figueirêdo Lopes Advogados (SBSA Advogados)

Laís de Figueirêdo Lopes
OAB/SP nº 182.480

Aline Gonçalves Videira de Souza
OAB/SP nº 296.651

Paula Raccanello Storto
OAB/SP nº 185.055

**Pedro Henrique Monteiro de Barros da
Silva Néto**
OAB/SP nº 488.756

¹⁶ Conforme consulta no Mapa das OSCs do IPEA, disponível em: <https://mapaosoc.ipea.gov.br/mapa>. Acesso em 17.06.26.

Contribuições da RNP à Consulta pública

Guia de transparência e
Proteção de dados pessoais

A Rede Nacional de Ensino e Pesquisa, através de seu Encarregado pelo Tratamento de Dados Pessoais, vem trazer contribuições ao documento “Guia de Transparência e Proteção de Dados Pessoais”, promovido pela Controladoria-Geral da União (CGU) e Agência Nacional de Proteção de Dados Pessoais (ANPD), em Consulta Pública aberta.

A RNP reitera seu reconhecimento à qualidade do Guia e coloca-se à disposição da CGU e da ANPD para os esclarecimentos que se fizerem necessários.

SEÇÃO 1 – Direito de acesso à informação e seus limites

SUGESTÃO DE INCLUSÃO: Incluir, na lista exemplificativa de documentos preparatórios, os projetos de PD&I em andamento como exemplo expresso de restrição temporária de acesso:

“• Documentos relacionados a projetos de pesquisa, desenvolvimento científico e inovação tecnológica em andamento: informações que subsidiam projetos não concluídos (como protótipos, testes de conceito, especificações técnicas, rascunhos de patentes e negociações com parceiros) podem ter o acesso restrito até o encerramento da pesquisa.”

JUSTIFICATIVA: recomendamos a inclusão deste novo exemplo para refletir de forma mais abrangente a realidade das entidades de ensino, pesquisa e desenvolvimento tecnológico. A explicitação desse contexto diretamente no Guia é de grande valia, pois a LAI já protege a atividade de pesquisa em diversos dispositivos (ex: art. 7º, §1º e art. 23, VI da LAI). Antes da conclusão de um projeto, tramitam documentos técnicos e negociais altamente sensíveis. Adicionar este exemplo confere maior segurança jurídica para que protejam a inovação, harmonizando o Guia com as diretrizes do Marco Legal de CT&I (Lei no 13.243/2016).

SEÇÃO 3 – Proteção de dados pessoais prevista na LAI

SUGESTÃO DE INCLUSÃO: complementar a tabela resumo do Guia com disposição expressa sobre o alcance da LAI às entidades privadas sem fins lucrativos (art. 2º da LAI):

“Alcance da lei: todas os órgãos e entidades do poder público e, no que couber, as entidades privadas sem fins lucrativos que recebam recursos públicos, hipótese em que a publicidade se restringe à parcela dos recursos públicos recebidos e à sua destinação (art. 2º da LAI).”

JUSTIFICATIVA: recomendamos a inclusão deste complemento para refletir de forma integral o dispositivo previsto no art. 2º, parágrafo único, da LAI. Haja vista que a legislação também se aplica a entidades privadas sem fins lucrativos que executam ações de interesse público, como é o caso da RNP, a explicitação desse limite diretamente na tabela resumo do Guia confere maior clareza e precisão à aplicabilidade da Lei, auxiliando de forma mais didática tanto os cidadãos requerentes quanto os gestores dessas instituições.

SUGESTÃO DE INCLUSÃO: acrescentar ao final da alínea “d” parágrafo que firme a presunção de interesse público para o tratamento de dados, sem consentimento, por órgãos de pesquisa:

“Presume-se atendido o requisito de evidente interesse público ou geral quando a demanda for formulada por órgão de pesquisa (art. 5o, XVIII, da LGPD) e a finalidade for pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.”

JUSTIFICATIVA: a LAI e a LGPD autorizam o tratamento e o compartilhamento de dados pessoais para fins de pesquisa independentemente do consentimento do titular, desde que presente o evidente interesse público ou geral. Na prática, porém, a exigência de que o servidor avalie subjetivamente o mérito e o interesse público de cada projeto gera insegurança jurídica: na dúvida sobre se o requisito está atendido, o gestor tende a exigir o consentimento, muitas vezes inviável em bases de pesquisa, ou simplesmente a negar o acesso, paralisando a pesquisa científica. A fixação de uma presunção de interesse público para as demandas formuladas por órgãos de pesquisa esclarece que, nessas hipóteses, a dispensa de consentimento já decorre da lei, deslocando o foco da análise do julgamento subjetivo sobre a relevância do estudo para a simples verificação da regularidade institucional do demandante.

SEÇÃO 4 – Garantindo a transparência pública com proteção dos dados pessoais

SUGESTÃO DE INCLUSÃO: incluir o pesquisador/colaborador científico como nova categoria na Tabela de Titulares:

*“• Tipo de titular: pesquisador / colaborador científico e acadêmico.
• Proximidade com o Estado: média.
• Expectativa de privacidade: média.
• O que pode ser publicado? (em tese): nome completo; vínculo institucional; número de matrícula acadêmica; título do projeto de pesquisa financiado ou apoiado por infraestrutura pública.”*

JUSTIFICATIVA: recomendamos a inclusão destas novas categorias na tabela exemplificativa contida no Guia, de forma a refletir a realidade do Sistema Nacional de Ciência, Tecnologia e Inovação. As categorias atuais limitam-se a relações administrativas ou assistenciais. O pesquisador que utiliza infraestruturas públicas possui uma relação diferenciada com o Estado. Nesse sentido, a explicitação deste titular auxiliará as instituições de ensino e os órgãos de fomento a calibrarem corretamente o Teste de Interesse Público, que servirá como apoio necessário para ponderar, no caso concreto, se o direito de acesso à informação e o benefício coletivo superam o direito à privacidade e à proteção dos dados pessoais do titular.

SUGESTÃO DE INCLUSÃO: inserir ao roteiro do Teste de Interesse Público mecanismo de tipificação de hipóteses para dispensa de avaliação caso a caso:

“Para otimização do fluxo de trabalho e eficiência administrativa, os órgãos e entidades poderão adotar matrizes internas de decisão consolidada (presunções operacionais) para situações recorrentes e de baixa

complexidade. Essas matrizes dispensam a reaplicação integral do Teste de Interesse Público, observados os seguintes parâmetros:

a) consolidação prévia das hipóteses em que há evidente presunção de interesse público na divulgação (ex: dados vinculados a desembolsos financeiros públicos); e

b) consolidação prévia das hipóteses em que há evidente presunção de restrição de acesso (ex: dados de saúde, vulnerabilidade social ou outros dados sensíveis)."

JUSTIFICATIVA: recomendamos a inclusão desta orientação para otimizar a gestão administrativa e garantir a eficiência no atendimento à LAI pelas instituições de ensino, pesquisa e inovação. A aplicação individualizada e casuística do Teste de Interesse Público para cada pedido de acesso a informações pessoais impõe um ônus operacional às entidades. Nesse sentido, a criação de "presunções operacionais" padroniza os cenários mais comuns e cotidianos, preservando a análise detalhada apenas para os casos complexos ou que apresentem riscos atípicos à privacidade e proteção de dados pessoais.

SEÇÃO 5 – Entendimentos sobre a publicidade de dados pessoais

SUGESTÃO DE INCLUSÃO: reformular a orientação de divulgação nominal de beneficiários de ações afirmativas para priorizar dados agregados:

"A transparência das ações afirmativas é assegurada preferencialmente mediante a divulgação de dados agregados e estatísticos que demonstrem o cumprimento dos critérios e da reserva de vagas, sem identificação nominal individualizada da condição racial."

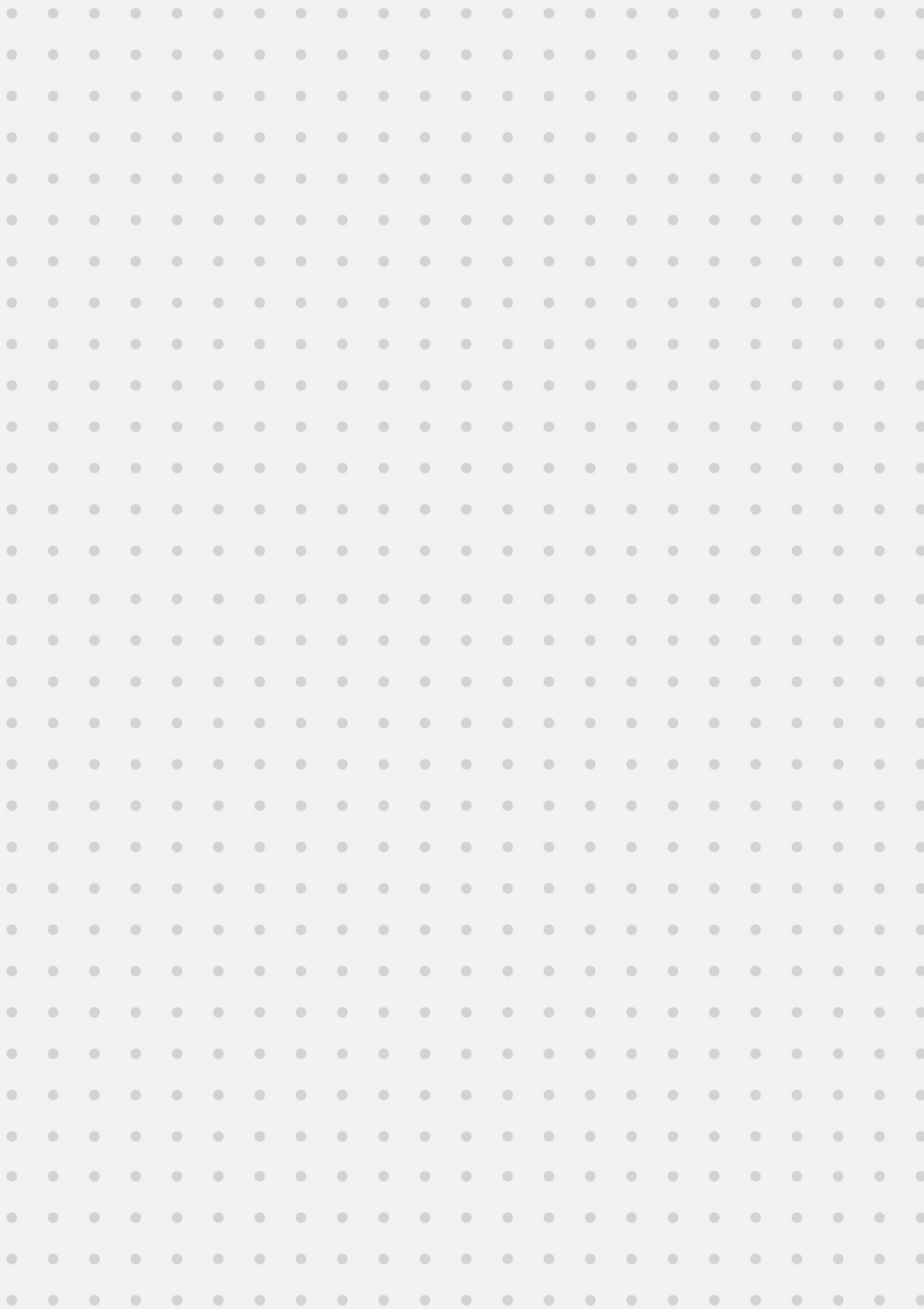
JUSTIFICATIVA: recomendamos a alteração para alinhar a orientação ao regime legal de proteção de dados pessoais sensíveis (art. 11 da LGPD). Vincular publicamente o nome de um estudante à cota racial revela, por inferência, sua origem racial ou étnica. O próprio texto do Guia alerta, na mesma seção, sobre o risco de estigmatização decorrente da exposição desse tipo de dado. Recomendamos, portanto, que seja dada preferência a dados agregados, garantindo o controle e a comprovação do preenchimento das vagas, sem expor desnecessariamente a identidade e a privacidade dos estudantes.

Cordialmente,

Documento assinado digitalmente
 **YURI ALEXANDRO DA SILVA FERREIRA**
Data: 21/06/2026 23:16:06-0300
Verifique em <https://validar.iti.gov.br>

Yuri Alexandro

Encarregado pelo Tratamento de Dados Pessoais
RNP – Rede Nacional de Ensino e Pesquisa



ENCARREGADO DE PROTEÇÃO DE DADOS

Referência: Processo nº E-20/001.002520/2025

AO EXCELENTÍSSIMO SENHOR DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL PROTEÇÃO DE DADOS (ANPD).

Assunto: Contribuição ao *Guia de Transparência e Proteção de Dados Pessoais — Acesso à Informação*. Sugestão técnica para vedação de formatos que possibilitem a raspagem automatizada (*scraping*) de dados remuneratórios de agentes públicos.

I. Introdução e Contexto

A Defensoria Pública do Estado do Rio de Janeiro (DPRJ), por meio de sua Encarregada de Proteção de Dados Pessoais, apresenta a presente manifestação como subsídio e contribuição ao *Guia de Transparência e Proteção de Dados Pessoais*, elaborado conjuntamente por esta Autoridade Nacional de Proteção de Dados (ANPD) e pela Controladoria-Geral da União (CGU).

O debate institucional contemporâneo exige que a aplicação da Lei de Acesso à Informação (Lei nº 12.527/11 — LAI) e da Lei Geral de Proteção de Dados (Lei nº 13.709/18 — LGPD) ocorra de forma coordenada, complementar e dialogada. Ambas as normas são estruturadas sob os valores constitucionais republicanos e visam reduzir a assimetria informacional. No entanto, a disponibilização ativa de dados pessoais relativos à remuneração de servidores públicos deve ser acompanhada de salvaguardas técnicas adequadas. O objetivo é evitar que o dever de transparência seja desvirtuado e passe a servir como vetor de riscos severos à segurança e à privacidade dos titulares.

Com efeito, o exercício do direito fundamental de acesso à informação exige a existência de um interesse legítimo de saber, caracterizado por vieses coletivos e sociais, e dotado de pertinência real para o cidadão.

O entendimento jurídico e social evoluiu de modo a compreender o interesse público ou coletivo não como a mera soma mecânica de desejos particulares, mas sim como

a busca por um bem comum maior, focado em necessidades vitais e existenciais para o convívio social harmónico.

Existe uma linha divisória clara e expressa que distingue o interesse coletivo da "curiosidade geral" ou "curiosidade alheia". O acesso a documentos e dados públicos não tem por escopo mitigar a curiosidade dos indivíduos, mas sim concretizar os preceitos afetos à cidadania, à democracia e à transparência.

Por essa razão, a publicidade ativa deve visar única e exclusivamente o interesse público determinado do controlo social dos gastos. É considerado um desvio de finalidade ilegal a utilização ou extração dessas informações para propósitos comerciais, perfilamento preditivo ou para a satisfação de mera curiosidade.

No tratamento e divulgação de informações que envolvam dados pessoais, o aplicador da norma deve realizar um juízo de ponderação contextual e equilibrado entre o direito à privacidade e o direito de acesso. A flexibilização da proteção de dados em prol da transparência só é legítima quando houver um interesse público geral e preponderante na situação concreta. Este interesse evidente demonstra-se quando a abertura do dado gera benefícios claros e diretos para a coletividade, tais como a análise do uso adequado de recursos públicos, a fiscalização da probidade dos agentes estatais ou o controle da integridade de processos administrativos. Se a divulgação de um dado individualizado não produzir esse benefício público relevante para a sociedade, deve prevalecer a proteção da privacidade do titular, negando-se o acesso.

Portanto, o propósito da presente sugestão é propor uma releitura do art. 8º, §§ 3º e 4º, da LAI, e do art. 8º, III, do Decreto nº 7.724/12, a partir da positivação do direito fundamental à proteção de dados pessoais na Constituição da República (art. 5º, LXXIX) e da promulgação da LGPD, releitura esta possível a partir da suposta antinomia e da adoção de técnicas de ponderação de normas constitucionais.

II. Do Risco da Raspagem de Dados (*Data Scraping*) em Planilhas Abertas

Tradicionalmente, diversos órgãos públicos, incluindo esta Defensoria Pública, estruturaram seus Portais da Transparência disponibilizando a relação de pessoal e respectivas remunerações em arquivos únicos de formato aberto e editável, como planilhas em extensão .xlsx ou blocos consolidados .html. Constatou-se, todavia, que a manutenção de dados remuneratórios e identificadores parciais nesse formato específico facilita a aplicação da técnica de "raspagem" (*data scraping*). Trata-se de uma modalidade de extração automatizada de informações por sistemas robóticos externos.

Essa extração em massa subverte a finalidade pública exigida pela Constituição da República, pela LAI e pela LGPD, pelas seguintes razões:

Desvio de Finalidade: O acesso à remuneração de agentes públicos tem como propósito legítimo o controle social dos gastos públicos e a moralidade administrativa. A raspagem automatizada, contudo, é comumente operada por empresas e indivíduos com propósitos estritamente econômicos, comerciais ou ilícitos.

Perfilamento Consumista e Preditivo: A consolidação automatizada desses dados permite que agentes privados realizem o perfilamento de servidores públicos para direcionar campanhas publicitárias agressivas ou fazer previsão de consumo. Essas práticas são alheias ao escopo do controle social.

Potencialização de Fraudes Estatais: Os dados extraídos em massa, quando cruzados e aliados a táticas de engenharia social, funcionam como insumos de alta precisão para a aplicação de golpes financeiros e fraudes diversas. Isso fragiliza a integridade física e financeira do servidor e de seus familiares.

Embora o artigo 8º, § 3º, inciso II, da LAI preveja a gravação de relatórios em formatos abertos e não proprietários, a realidade fática da era digital demonstra que a literalidade desse dispositivo gera uma antinomia com o dever de proteção ativa de dados (*duty to protect*). Portanto, impõe-se uma filtragem hermenêutica e técnica de "transparência por desenho" (*transparency by design*). Essa abordagem assegura o fornecimento do dado pessoal individualizado ao cidadão, mas impede a sua pilhagem automatizada por robôs comerciais.

Ressalte-se que disponibilização das informações individualizadas sobre as remunerações atende à transparência ativa, na medida em que a identificação dos servidores públicos — nomes, cargos, funções, lotações — é igualmente disponibilizada de forma ostensiva pelos órgãos públicos em seus portais. Assim, o cidadão consegue acessar o nome do servidor público no próprio portal, informação que possibilita o exercício do direito fundamental de acesso à informação, para obtenção da informação sobre a remuneração mensal.

III. Das Propostas de Aperfeiçoamento para o Guia

Com fulcro nos princípios da finalidade, adequação, necessidade e segurança previstos na LGPD, bem como nas diretrizes de minimização ratificadas pelo Tribunal de Contas da União (TCU) no Acórdão 1511/2025 – Plenário, a Defensoria Pública do Estado do Rio de Janeiro propõe a inclusão das seguintes recomendações no texto do Guia:

1. Restrição de Formato Massivo Restrita Exclusivamente a Dados Remuneratórios:

Recomendar que as informações individualizadas sobre a remuneração mensal de agentes públicos sejam disponibilizadas por meio de ferramentas que impeçam ou dificultem a raspagem automatizada e o *download* em blocos unificados (como

planilhas editáveis). Ressalta-se, de forma categórica, que esta sugestão de restrição técnica se refere única e exclusivamente às remunerações dos servidores públicos, em razão dos riscos de segurança e engenharia social apontados. Portanto, ela não se aplica e não deve criar óbices a outras informações de transparência ativa obrigatória — tais como execução orçamentária, repasses financeiros, procedimentos licitatórios e contratos administrativos —, as quais devem seguir em formatos abertos, estruturados e legíveis por máquina para o pleno exercício do controle social.

2. Adoção de Barreiras de Verificação e Identificação Mínima: Orientar que o acesso eletrônico a dados remuneratórios individualizados seja protegido por testes públicos de Turing ("captcha") ou, preferencialmente, por autenticação prévia via conta unificada Gov.Br. Essa medida valida o solicitante e mitiga o tráfego automatizado de robôs preditivos, sem impor restrições ilegítimas ao cidadão que deseja exercer o direito de acesso.

3. Segregação Estrita de Rubricas Privadas: Reforçar que o dever de transparência ativa não alcança dados da vida privada do servidor, tais como descontos relativos a pensões alimentícias, empréstimos consignados ou dados bancários e médicos. Tais valores devem constar exclusivamente sob rubricas genéricas e não discriminadas (ex.: "outros descontos").

IV. Conclusão

A transparência administrativa é preceito geral e pilar da nossa estrutura democrática. Contudo, ela não se confunde com opacidade técnica ou, no extremo oposto, com a exposição imotivada e vulnerável de dados funcionais para a exploração econômica predatória por terceiros.

Ao vedar o formato de planilhas abertas massivas para dados remuneratórios e promover sistemas inteligentes de consulta individualizada protegidos por captchas ou por autenticação através da conta Gov.Br, o Poder Público atinge o ponto ideal de equilíbrio: garante o controle social dos gastos com pessoal, sem transformar seus agentes públicos em alvos vulneráveis na internet.

Esta Defensoria Pública renova os protestos de estima e se coloca à disposição para debater os aspectos técnicos desta cooperação.

Rio de Janeiro, 4 de julho de 2026.

Adriana Araujo João – defensora pública

Matrícula nº 820.952-0



Documento assinado eletronicamente por **ADRIANA ARAUJO JOÃO, Defensora Pública**, em 04/07/2026, às 11:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.rj.def.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2142756** e o código CRC **F9D0EEDD**.

Referência: Processo nº E-20/001.002520/2025

Avenida Marechal Câmara, 314 - Bairro Centro
Rio de Janeiro - RJ - CEP 20020-080
- www.defensoria.rj.def.br

CONTRIBUIÇÃO TÉCNICA

Publicidade de títulos acadêmicos e currículos de agentes públicos

Guia de Transparência e Proteção de Dados Pessoais

Contribuinte	Ana Maria Carvalheiro
Qualificação	Bacharela em Ciência da Computação, autora e pesquisadora em governança digital, proteção de dados e cidadania digital
Objeto	Aperfeiçoamento do entendimento sobre divulgação de formação acadêmica e experiência profissional de agentes públicos

1. Síntese da contribuição

A proposta é fortalecer o entendimento apresentado no Guia, estabelecendo critérios objetivos para que a transparência sobre currículos de agentes públicos seja útil ao controle social, verificável e compatível com a proteção de dados pessoais. A publicidade deve alcançar as informações diretamente relacionadas à capacidade, à aptidão e ao conhecimento técnico exigidos para o exercício do cargo ou da função, sem se converter em exposição indiscriminada da vida privada.

PROPOSTA DE REDAÇÃO

Informações curriculares de agentes públicos diretamente relacionadas ao exercício do cargo ou da função são passíveis de acesso público, incluindo formação acadêmica, títulos obtidos, instituição de ensino, experiência profissional relevante, vínculos institucionais e data da última atualização. A divulgação deve ser padronizada, acessível, atualizada e limitada aos dados necessários para a avaliação da capacidade, aptidão e conhecimento técnico, vedada a exposição de endereço residencial, contatos pessoais, documentos de identificação, dados familiares, dados bancários e dados sensíveis sem pertinência funcional. O órgão deve disponibilizar canal para correção de informações inexatas e indicar, sempre que possível, a fonte ou o procedimento de verificação dos dados divulgados.

2. Fundamentos e justificativa

A transparência curricular de agentes públicos atende ao princípio constitucional da publicidade e contribui para o controle social das nomeações, designações e ocupações de cargos e funções públicas. O Enunciado CGU nº 7/2023 reconhece que títulos, experiência acadêmica e experiência profissional podem ser acessados publicamente quando utilizados para avaliar a capacidade, a aptidão e o conhecimento técnico necessários ao exercício da função pública.

A Lei de Acesso à Informação e a Lei Geral de Proteção de Dados Pessoais devem ser aplicadas de forma complementar. A existência de dados pessoais no currículo não justifica a negativa integral de acesso: informações protegidas podem ser omitidas, tarjadas ou separadas, permitindo a divulgação da parte de interesse público. Ao mesmo tempo, os princípios da finalidade, adequação, necessidade, qualidade dos dados, transparência, segurança e responsabilização exigem que o órgão publique apenas o que seja pertinente e proporcional.

A padronização proposta reduz decisões casuísticas, evita currículos incompletos ou desatualizados e facilita a comparação entre os requisitos do cargo e a qualificação apresentada. Também protege o agente público contra a circulação de informações inexatas, ao prever data de atualização, fonte de verificação e procedimento de retificação.

3. Conteúdo mínimo recomendado para divulgação

- nome completo, órgão ou entidade, cargo ou função, unidade de exercício e período de ocupação;
- formação acadêmica, instituição de ensino, área de conhecimento, grau ou título e ano de conclusão, quando pertinente;
- experiência profissional relevante para as atribuições desempenhadas, com indicação da organização, função e período;
- qualificações técnicas, certificações profissionais e produção acadêmica diretamente relacionadas à atividade pública;
- data da última atualização e canal institucional para solicitar correção de informação inexata ou desatualizada.

4. Matriz orientativa de publicidade e proteção

Dado ou documento	Tratamento recomendado	Justificativa
Nome, cargo, órgão, unidade e período de exercício	Divulgação integral	Dados diretamente associados ao exercício da função pública e ao controle social.
Formação acadêmica, títulos e instituição de ensino	Divulgação integral	Permitem avaliar a qualificação técnica declarada para o cargo ou função.
Experiência profissional e vínculos institucionais relevantes	Divulgação integral	Relacionam-se à aptidão e à capacidade profissional do agente.
Ano de conclusão, área de conhecimento e certificações	Divulgação integral	Aprimoram a verificabilidade, desde que pertinentes à função.
Cópias de diplomas, certificados ou documentos comprobatórios	Divulgação parcial ou sob demanda	Devem ser tarjados números de documentos, assinaturas, códigos de validação e outros elementos desnecessários.
CPF, RG, endereço residencial, telefone pessoal, e-mail pessoal e dados bancários	Não divulgar	Dados da vida privada sem pertinência para a avaliação da capacidade funcional.
Informações de saúde, religião, opinião política, origem racial ou étnica e outros dados sensíveis	Não divulgar, salvo base legal e necessidade específica	Exigem proteção reforçada e, em regra, não são necessários à transparência curricular.

5. Recomendações de implementação

- Adotar formulário ou ficha curricular institucional padronizada, com campos definidos e linguagem clara.
- Publicar os dados em página acessível, pesquisável e compatível com tecnologias assistivas, evitando arquivos exclusivamente digitalizados.
- Atualizar o conteúdo na nomeação, designação, alteração relevante de qualificação ou encerramento do vínculo, registrando a data da atualização.
- Prever procedimento de validação documental e canal para correção de dados incompletos, inexatos ou desatualizados.
- Aplicar o princípio da divulgação parcial: documentos que contenham dados protegidos devem ser disponibilizados com ocultação apenas das informações não pertinentes.
- Manter registro da decisão administrativa sobre quais campos são públicos, parcialmente públicos ou protegidos, com justificativa baseada em interesse público, necessidade e proporcionalidade.

6. Resultado esperado

A incorporação dessas diretrizes ao Guia aumentará a previsibilidade e a segurança jurídica das decisões, fortalecerá a integridade das nomeações e permitirá que a sociedade avalie a compatibilidade entre a formação do agente público e as atribuições exercidas. Ao mesmo tempo, a delimitação dos campos publicáveis evitará a exposição de dados sem pertinência funcional e concretizará a transparência responsável, por desenho e com proteção de dados pessoais.

7. Referências normativas

BRASIL. Constituição da República Federativa do Brasil de 1988. Princípios da Administração Pública e direito de acesso à informação.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.

CONTROLADORIA-GERAL DA UNIÃO. Enunciado CGU nº 7/2023 - Títulos acadêmicos e currículos de agentes públicos.

CONTROLADORIA-GERAL DA UNIÃO. Texto-base da Consulta Pública do Guia de Transparência e Proteção de Dados Pessoais.

Ana Maria Carvalheiro

Brasília-DF, 10 de julho de 2026

1. SOBRE O CAPÍTULO 5 – TRANSPARÊNCIA EM BOLSAS E AUXÍLIOS A SERVIDORES

- **Proposta:** Explicitar no Guia a obrigação de transparência ativa na concessão de bolsas de pesquisa, extensão e auxílios de qualificação (como o PIQ) destinados a **servidores públicos**.
- **Diretrizes a incluir:** Orientar que os órgãos publiquem previamente os **editais/chamadas públicas com critérios objetivos de seleção**; a **relação dos servidores contemplados** (nome, matrícula parcialmente tarjada, cargo, projeto e valor); e demonstrativo de demandas deferidas x indeferidas. A gestão de recursos públicos afasta a alegação de sigilo para fechar critérios ou escolhas discricionárias.

2. SOBRE O CAPÍTULO 5 – COMISSÕES REMUNERADAS E GECC

- **Proposta:** Incluir no rol de dados de agentes públicos sujeitos à transparência ativa as informações sobre **composição de comissões de concurso, bancas examinadoras e pagamentos por GECC** (Gratificação por Encargo de Curso ou Concurso - art. 76-A da Lei nº 8.112/1990).
- **Diretrizes a incluir:** Garantir a publicação dos **critérios técnicos de escolha dos integrantes** (estimulando editais de credenciamento e rodízio) e o demonstrativo transparente dos **valores pagos por GECC** vinculados à matrícula funcional do servidor, em observância aos princípios da impessoalidade e moralidade.

3. SOBRE O CAPÍTULO 5 – SERVIDORES CEDIDOS, MOVIMENTAÇÃO DE PESSOAL E ISONOMIA

- **Problema Identificado:** A opacidade na movimentação de pessoal (servidores cedidos, requisitados ou em composição de força de trabalho) e a ausência de critérios claros para o deferimento ou indeferimento das solicitações geram profunda assimetria e arbitrariedade. Embora existam editais e seleções publicadas em plataformas federais oficiais (como o SouGov), observa-se um uso recorrente e genérico da justificativa de "quadro reduzido" para negar a saída de determinados servidores, ao passo que outras cessões são concedidas de forma discricionária. Isso compromete a isonomia, o dimensionamento do quadro local e a previsibilidade de direitos como a remoção interna, a redistribuição e a abertura de novos concursos.
- **Proposta de Regulamentação no Guia:** Detalhar, no tópico de *Lotação e Exercício do Agente Público* (Capítulo 5), a obrigatoriedade de disponibilização em **transparência ativa** dos dados sobre movimentações de pessoal e seus respectivos processos decisórios.
- **Diretrizes Específicas a Incluir no Guia:**
 1. **Democratização e Motivação dos Indeferimentos:** Exigência de transparência ativa e critérios objetivos para as decisões de liberação ou retenção de servidores (inclusive nas oportunidades ofertadas via SouGov). As negativas baseadas em "necessidade do serviço" ou "déficit de pessoal" devem ser fundamentadas com indicadores reais do setor, garantindo que a discricionariedade do gestor seja motivada e isonômica, coibindo negativas arbitrárias ou favorecimentos;

2. **Duração, Regras e Prazo de Retorno:** Publicação do ato formal de movimentação, da modalidade de ingresso (se por edital público/SouGov ou negociação direta) e do **prazo pactuado para o retorno do servidor à instituição de origem**, evitando afastamentos indeterminados ou informais;
3. **Correlação com o Quadro Vago e Planejamento Institucional:** Obrigatoriedade de correlacionar os quantitativos de servidores cedidos/afastados com a ocupação do quadro efetivo, evidenciando o impacto real da força de trabalho no planejamento dos ciclos de remoção interna, redistribuição e concursos públicos;
4. **Harmonização entre LAI e LGPD na Movimentação:** Explicitar que a condição de servidor cedido e o órgão de destino são informações de interesse público e do exercício da função estatal, **não constituindo dado pessoal protegido contra a transparência ativa**, devendo ser divulgados nome, matrícula parcialmente tarjada, órgão de destino, portaria de cessão e previsão de retorno.

CONTRIBUIÇÕES TÉCNICAS AO GUIA ORIENTATIVO: LAI E LGPD NA ADMINISTRAÇÃO PÚBLICA

Apresentam-se sugestões de aprimoramento ao texto do Guia Orientativo promovido pela Controladoria-Geral da União (CGU) e pela Autoridade Nacional de Proteção de Dados (ANPD), com foco no aperfeiçoamento da governança pública, inovação tecnológica e proteção de direitos fundamentais:

1. COMPLEMENTAÇÃO AO CAPÍTULO 3 (Item 3.3, alínea 'd' – Estatísticas e Pesquisas)

- **Seção Correspondente:** Capítulo 3, Item 3.3, alínea 'd' (*Orientações para fornecer informações pessoais para pesquisa compatibilizando as disposições da LAI e da LGPD*).
- **Sugestão de Aprimoramento:** Recomenda-se incluir no Guia a orientação para que os órgãos públicos e instituições de ensino/pesquisa adotem ambientes virtuais controlados de amostragem (*Data Cleanrooms*) e protocolos padronizados de pseudonimização. Essa medida assegura a utilidade estatística dos dados acadêmicos para o avanço da ciência e da inovação pública, garantindo pleno alinhamento aos princípios da minimização, segurança e finalidade previstos no art. 6º da LGPD.

2. COMPLEMENTAÇÃO AO CAPÍTULO 4 (Item 4.3 – Transparência por Desenho)

- **Seção Correspondente:** Capítulo 4, Item 4.3 (*Transparência por desenho e revisão de fluxos de trabalho*).
- **Sugestão de Aprimoramento:** Recomenda-se aprofundar as diretrizes do Item 4.3 para orientar a inclusão de requisitos funcionais de *Privacy and Transparency by Design* desde a fase de modelagem, desenvolvimento e contratação de sistemas de informação públicos (em alinhamento à Lei do Governo Digital – Lei nº 14.129/2021). A arquitetura dos sistemas deve prever nativamente a segregação de bancos de dados, permitindo a extração automatizada de dados abertos com mascaramento automático de identificadores sensíveis, reduzindo o custo operacional e o tempo de resposta a pedidos via LAI.

3. COMPLEMENTAÇÃO AO CAPÍTULO 2 (Item 2.1 – Princípios e Direitos dos Titulares)

- **Seção Correspondente:** Capítulo 2, Item 2.1 (*Princípios e hipóteses legais aplicáveis ao tratamento de dados pessoais pelo Poder Público*).
- **Sugestão de Aprimoramento:** Propõe-se a inclusão de diretrizes para a padronização dos fluxos operacionais de atendimento aos direitos dos titulares de dados (art. 18 da LGPD) no setor público. Recomenda-se a integração dos canais formais de Ouvidoria e da Plataforma Fala.BR com os sistemas de identificação digital do Poder Público, adotando os níveis de autenticação da Plataforma Gov.br (Níveis Prata e Ouro) como parâmetro seguro de verificação de identidade, garantindo celeridade, interoperabilidade e proteção contra acessos não autorizados.

Ref.: Consulta Pública da ANPD e da CGU – Guia de Transparência e Proteção de Dados Pessoais

Apresentamos a seguir as nossas sugestões de contribuições à Consulta Pública sobre o Guia de Transparência e Proteção de Dados Pessoais ([aqui](#)), promovida pela Agência Nacional de Proteção de Dados (ANPD) e pela Controladoria-Geral da União (CGU).

Considerações Gerais

O Einstein Hospital Israelita (“Einstein”), entidade que atua em assistência, ensino, pesquisa, inovação e saúde digital, e que mantém colaboração com políticas públicas e com o Poder Público, apoia a iniciativa da CGU e da ANPD e reconhece a relevância do Guia para harmonizar a transparência pública e a proteção de dados pessoais. A contribuição busca aprimorar a clareza, a segurança jurídica e a aplicabilidade prática do documento, especialmente em contextos de saúde, pesquisa, inovação e tratamento de dados pessoais sensíveis. Parte-se das premissas de que a publicidade é a regra, de que a LGPD não cria sigilo e de que eventuais restrições se fundamentam na LAI.

Capítulo 1 — Direito de acesso à informação e seus limites

Sugerimos que o rol exemplificativo de sigilos legais (art. 22 da LAI) do capítulo 1.2 mencione expressamente o sigilo profissional, em especial o sigilo médico, por sua elevada relevância para a Administração Pública que custodia informações de saúde (redes públicas, perícias, programas e parcerias com instituições de saúde). Trata-se de sigilo legal típico, preservado pela LAI, que não se confunde com a (inexistente) criação de sigilo pela LGPD e que convive com o regime do art. 31. Sugere-se acrescentar:

“Sigilo profissional, inclusive o sigilo médico, protege informações confiadas em razão do exercício de profissão regulamentada, amparado, entre outros, no art. 154 do Código Penal, na Lei nº 12.842/2013 (exercício da medicina) e, quanto à guarda e confidencialidade de prontuários, na Lei nº 13.787/2018, constituindo exceção legítima ao acesso preservada pelo art. 22 da LAI.”

Capítulo 2 — Proteção de dados pessoais nos termos da LGPD

Apoiamos integralmente a afirmação de que a LGPD não cria hipóteses de sigilo, nem altera o rol de informações restritas. Sugerimos apenas reforçar, na parte final, que a complementaridade entre LAI e LGPD impõe, no tratamento para fins de transparência, a observância dos princípios da finalidade, necessidade, adequação, segurança e prestação de contas, o que é particularmente sensível quando há dados de saúde sob guarda pública ou compartilhados em parcerias.

Capítulo 3 — Proteção de dados pessoais prevista na LAI

Sugerimos a inclusão de um box específico sobre dados de saúde, reconhecendo que: (i) dados de saúde são dados sensíveis (art. 5º, II, e art. 11 da LGPD) e estão abarcados pela proteção da intimidade (art. 31 da LAI); (ii) prontuários e registros assistenciais sujeitam-se a sigilo profissional, que é sigilo legal preservado pelo art. 22 da LAI; e (iii) quando a identificação individual não for indispensável ao interesse público, deve-se preferir a divulgação agregada, anonimizada ou pseudonimizada. Quanto à pesquisa (item 3.3, alínea “d”), apoiamos o entendimento da ANPD de que a anonimização não é condição para o compartilhamento, mas sugerimos ressalva sobre o risco de reidentificação em bases clínicas, genômicas, biométricas, de doenças raras ou de alta granularidade, com remissão à governança ética da pesquisa (CEP/CONEP).

Box sugerido no Capítulo 3 ou no Capítulo 5:

“Dados de saúde são dados pessoais sensíveis (art. 5º, II, e art. 11 da LGPD) e estão abrangidos pela proteção da intimidade e da vida privada de que trata o art. 31 da LAI. Prontuários e registros assistenciais sujeitam-se, ainda, ao sigilo profissional, que constitui sigilo legal preservado pelo art. 22 da LAI. A presença de dados de saúde em documentos sob guarda pública ou em informações decorrentes de parcerias não impõe sigilo automático, mas exige análise reforçada de risco e a preferência, sempre que a identificação individual não for indispensável ao interesse público preponderante, pela divulgação agregada, anonimizada ou pseudonimizada. Indicadores agregados de produção, qualidade, cobertura e resultados assistenciais e de pesquisa devem ser divulgados; dados individuais de pacientes, acompanhantes, familiares e participantes de pesquisa, em regra, devem ser protegidos.”

Adicionalmente, sugerimos acrescentar, após o parágrafo que acolhe o entendimento da ANPD sobre anonimização:

“Em bases de alta granularidade, como dados clínicos detalhados, genômicos, biométricos, de imagens médicas, de doenças raras ou de coortes reduzidas, há risco concreto de reidentificação mesmo após pseudonimização. Nesses casos, recomenda-se análise reforçada de risco, a adoção de salvaguardas adicionais (controle de acesso, ambiente seguro, Termo de Responsabilidade e, quando cabível, dados sintéticos ou agregados) e a observância da governança ética da pesquisa, inclusive a aprovação pelo sistema CEP/CONEP, quando aplicável. A divulgação de resultados deve preferir formatos agregados que preservem o conteúdo científico sem expor titulares.”

Capítulo 4 — Garantindo a transparência com proteção dos dados pessoais

No Teste de Interesse Público (item 4.2, passo 3), sugerimos a inclusão de matriz orientativa de risco (probabilidade × impacto), com graduação em baixo, médio e alto, e de tipologia de danos a considerar: discriminação, estigmatização, fraude, constrangimento, reidentificação, dano reputacional, exposição indevida de condição de saúde e abalo da confiança no serviço público. A matriz é meramente orientativa e não substitui a análise qualitativa e casuística. Sugerimos, ainda, que o Guia trate expressamente dos pedidos de acesso relativos a sistemas de inteligência artificial, algoritmos e decisões automatizadas do Poder Público, privilegiando a transparência sobre finalidade, lógica geral, governança, métricas de desempenho, riscos e medidas de mitigação, sem expor dados pessoais, segredos legais, propriedade intelectual ou vulnerabilidades de segurança. Na transparência por desenho (item 4.3), sugerimos estender as boas práticas às entidades parceiras, mediante cláusulas de segregação prévia entre informação pública e protegida, metadados e trilhas de auditoria.

Sugerimos, adicionalmente, acrescentar à tabela de técnicas menos invasivas exemplos do setor de saúde:

- Agregação por faixa etária, sexo, município/região e período, para indicadores epidemiológicos e de produção assistencial, sem identificação dos titulares.
- Descaracterização de CPF (***.999.999-**) e tarjamento de identificadores diretos em documentos de parcerias e prestações de contas.
- Divulgação de quantitativos de atendimentos, procedimentos e beneficiários por unidade ou programa, em vez de listas nominais de pacientes.
- Uso de pseudonimização com chave controlada para acompanhamento de coortes em estudos, dispensando a identificação direta.

Capítulo 5 — Entendimentos sobre a publicidade de dados pessoais

Sugerimos a inclusão de subseção sobre dados de saúde em contratos, convênios e parcerias com o Poder Público, diferenciando claramente as informações públicas (objeto, valores, metas, entregas, execução financeira e indicadores agregados de produção, qualidade, ensino e pesquisa) dos dados individuais protegidos (pacientes, acompanhantes, familiares, participantes de pesquisa e, com ressalvas, profissionais). Sugerimos, também, consolidar diretriz geral sobre titulares vulneráveis — crianças, adolescentes, idosos, pessoas com deficiência, pacientes em vulnerabilidade clínica, vítimas de violência e portadores de doenças estigmatizantes — com presunção reforçada de proteção e análise caso a caso do melhor interesse, em especial de crianças e adolescentes (art. 227 da CF, ECA e art. 14 da LGPD). Sugestões abaixo:

“Nos instrumentos celebrados entre o Poder Público e instituições de saúde, a publicidade incide amplamente sobre objeto, valores, metas, entregas, prazos, execução financeira e resultados agregados. Tais informações não se confundem com os dados individuais de pacientes, acompanhantes, familiares e participantes de pesquisa, que, em regra, devem ser protegidos, salvo interesse público preponderante na identificação. Incluem-se nesse contexto, ainda, dados de natureza administrativa que possam permitir inferências sobre o estado de saúde dos titulares, como registros de controle de acesso a unidades assistenciais (por exemplo, listas de visitantes), os quais, em razão do contexto, demandam tratamento com salvaguardas equivalentes às aplicáveis a dados pessoais sensíveis. Sempre que a finalidade de controle social puder ser atendida por indicadores agregados, esta deve ser a forma preferencial de divulgação.

Adicionalmente, o tratamento e a eventual divulgação de dados de pessoas em situação de vulnerabilidade (crianças e adolescentes, idosos, pessoas com deficiência, pacientes em vulnerabilidade clínica, vítimas de violência e portadores de doenças estigmatizantes) exigem cautela reforçada. No caso de crianças e adolescentes, observa-se o melhor interesse (art. 227 da CF, ECA e art. 14 da LGPD), com presunção reforçada de proteção e divulgação preferencialmente agregada ou anonimizada. A identificação nominal só deve ocorrer quando indispensável e amparada em interesse público preponderante, devidamente motivado, e nunca quando puder gerar risco à vida, à segurança, à integridade ou à dignidade do titular.”

Contribuição 111543 - 11/06/2026

É importante reforçar nessa seção que o regime de tratamento de dados pessoais da LGPD não abrange pessoas jurídicas. Essa confusão é bastante comum, tanto dentro quanto fora da Administração Pública.

Contribuição 111550 - 11/06/2026

Além disso, também é importante inserir um adendo informando a ressalva que a LGPD possui com relação a dados de pessoas mortas, tendo em vista que a eles não é aplicável a referida legislação.

Contribuição 113654 - 12/06/2026

Primeiro, a simples remoção de nome ou CPF não garante anonimato, diversos estudos internacionais demonstram que conjuntos de dados supostamente anônimos podem ser reidentificados mediante o cruzamento com outras informações disponíveis. O risco é particularmente elevado em municípios pequenos.

Segundo, recomendo substituir o entendimento de que não há risco adicional quando a informação já está disponível em outra fonte pública por redação semelhante.

Pois existência prévia de determinada informação em fontes públicas não elimina automaticamente os riscos decorrentes de sua nova divulgação, devendo ser analisados fatores como facilidade de acesso, indexação por mecanismos de busca, agregação de dados e potencial de correlação com outras bases.

Uma informação dispersa em documentos físicos ou sistemas pouco acessíveis possui impacto distinto de uma publicação estruturada em portal oficial. A republicação pode ampliar significativamente a exposição do titular

Contribuição 113762 - 12/06/2026

Pesquisas revelam que identificar uma pessoa com dados “não sensíveis” é factível. Por exemplo, CEP + data de nascimento + sexo identifica 87% dos americanos. Em conjuntos de dados brasileiros, atributos como nome, cidade, cargo ou salário já possibilitaram identificação fácil (teste prático: cruzando redes sociais ou bases vazadas). Em geral, “identificadores” (nome, CPF, RG etc.) ou “quase-identificadores” (CEP, idade, cidade) em conjunto aumentam muito a probabilidade de reidentificação. Assim, mesmo informação sem classificação sensível pode, em conjunto, revelar dados íntimos (religião, saúde, condições financeiras).

Isso significa que mascarar parcialmente CPF ou RG, sem mais, não garante privacidade se outros atributos o identificarem.

Recomenda-se tratar essas mudanças como urgentes. A simples classificação “não sensível” desses dados contraria o cenário de segurança atual e pode ensejar danos graves.

Contribuição 113765 - 12/06/2026

Publique apenas os atributos essenciais ao interesse público. Evite combinar campos desnecessariamente. Por exemplo, divulgue “faixa etária” em vez de data exata de nascimento; cidade em vez de endereço completo; ou apenas ano de concessão de benefício, não mês/dia.

Ex.: substituir CEP completo por apenas os dois primeiros dígitos; agrupar rendimentos em faixas; converter idades em décadas.

Se decidir incluir identificadores como CPF ou RG (mesmo mascarados), documente que isso

não torna os dados anônimos. Como ressalta CNIL, dados pseudonimizados permanecem pessoais se houver possibilidade de reidentificação. Em geral, prefira usar tokens irreversíveis ou simplesmente omita esses campos nas divulgações.

Incentive a consulta individual bem formulada em lugar de dumping de dados em massa; ofereça alternativas (sumários estatísticos) que atendam ao interesse público sem expor indivíduos.

Contribuição 114747 - 14/06/2026

Contribuições em relação ao capítulo 4.

Contribuição 115300 - 17/06/2026

Excelente as contribuições do antecessor. Vale, ainda, complementação. Até porque esse capítulo é o principal do Guia, orientar sobre o tratamento (e não sobre a divulgação), ainda que em parte se refira às decisões do tratamento visando a divulgação. Discordo veemente que a divulgação do Nome e CPF de beneficiário de política assistencial (Bolsa Família) tenha interesse público preponderante e baixo risco de estigmatização social devido à exposição de condição socioeconômica. A divulgação do nome completo e CPF, ainda que mascarado, é uma divulgação identificada que garante a composição de uma chave única da pessoa, que em outras divulgações que usem do mesmo binômio permitem ir montando uma perfilização dessas pessoas. É importante observar que § 2º, do artigo 12 da LGPD já trata esse risco alto. A divulgação do cpf (agora documento de identidade) mascarado junto com o nome da pessoa não é um recurso de pseudonimização, mas de identificação precisa do indivíduo.

Contribuição 115302 - 17/06/2026

O guia mistura demais divulgação com acesso. Há várias referências que abordam essas ações como distintas. Deve ser cuidadosamente revisto, porque as orientações deveriam ser em relação ao acesso e não à divulgação. Trata-se de um guia orientar o tratamento de dados pessoais por órgãos públicos em relação à compatibilização da das exigências legais vigentes, incluindo a LAI e a LGPD, mas não apenas essas (o próprio guia cita outras legislações). A divulgação de dados pessoal e o acesso devem assegurar os preceitos legais estabelecidos, finalidade, minimização, adequação, propriedade, entre tantos outros. A divulgação, por ser uma ação mais ampla e cuja consequência não se pode mensurar corretamente, considerando as condições tecnológicas atuais, deve ser ainda mais cuidadoso e cercado de recomendações bastante conservadoras e/ou comprovadas tecnicamente quanto à sua capacidade de preservação dos direitos do titular.

Contribuição 115303 - 17/06/2026

O mascaramento do CPF não é uma solução pseudonimização para permitir a divulgação, ainda mais quando se trata de uma máscara estática, isso é bastante frágil. Como já comentado, se associado com outra informação pessoal, há uma redução da efetividade, na verdade a viabilização da identificação. A pseudonimização, pela própria definição legal, envolveria um código específico do controlador e não a supressão de alguns números de um documento público. Portanto, uma máscara do CPF poderia ser entendida como suficiente para caracterizar um indivíduo, a chance matemática de um mesmo indivíduo compartilhar o mesmo CPF mascarado é 1:1.000, na prática é algo em torno de 1:300. Considerando que a chave traz um algarismo que identifica a região de emissão do CPF, essa única divulgação da forma como está hoje já permite associar, agora que o documento é emitido no

nascimento, uma área em que o indivíduo nasceu, especialmente crianças já que a adoção dessa sistemática de emissão é recente.

Contribuição 115304 - 17/06/2026

Voltando ainda a conclusão que o risco de estigmatização social devido à exposição de condição socioeconômica de beneficiários de programas sociais é baixo. Sugiro uma revisão contundente, apenas considerando a veiculação recente em cadeia nacional por formador de opinião dessa estigmatização, como sendo algo generalizado. Além disso, vale considerar as contribuições já existentes na consulta, não se trata apenas de um risco único (estigmatização), mas de um risco difícil de ser mensurado quando por exemplo já reconhece o uso dessas informações para a construção de perfis pessoais (perfilização da população).

Contribuição 115572 - 18/06/2026

Os prazos de resposta às solicitações de informações devem ser normatizados, se na LGPD o prazo inicial é de três dias úteis, a LAI deve entrar em consonância, bem como os prazos de respostas e justificativas às decisões tomadas.

Outro ponto importante é em relação ao "teste de dano", o RIPD da legislação de proteção de dados deve ser levado em consideração como documento para que o agente público possa referendar formalmente suas decisões de acesso aos dados, hoje não há transparência da negativa do agente público à solicitações realizadas; em suma, não há privacy by design se o solicitante não têm transparência ao racional utilizado para porventura suas solicitações de acesso à informações sejam negadas.

Contribuição 115627 - 18/06/2026

Recomendo complementar o capítulo com referência expressa ao princípio constitucional da proporcionalidade e da concordância prática entre direitos fundamentais, reconhecendo que a transparência pública e a proteção de dados pessoais constituem valores constitucionais igualmente relevantes, devendo ser harmonizados mediante análise contextualizada e motivada. Nesse sentido, é oportuno mencionar que a Emenda Constitucional nº 115/2022 elevou a proteção de dados pessoais à categoria de direito fundamental autônomo (art. 5º, LXXIX, da Constituição Federal), reforçando a necessidade de adoção de critérios objetivos para a ponderação entre publicidade e privacidade. Também é recomendável incorporar referências aos arts. 6º, 46 e 50 da Lei nº 13.709/2018 (LGPD), evidenciando que a divulgação de informações deve observar os princípios da finalidade, necessidade, adequação, prevenção, segurança e responsabilização, bem como a implementação de programas de governança em privacidade e proteção

Contribuição 115761 - 19/06/2026

Sugiro que o guia aborde a boa prática de descaracterizar a matrícula funcional do servidor, de forma semelhante ao CPF, pois a sua publicização pode ensejar riscos aos servidores, especialmente financeiros, pois ao dispor do seu nome e de sua matrícula, é possível, por exemplo, fraudar contratação de empréstimos consignados em seu nome, sem o seu aval. A tarja parcial da matrícula como ocorre no Portal Transparência do Governo Federal parece a solução adequada, uma vez que permite a identificação de eventuais homônimos, mas protege os titulares dos cargos de eventuais fraudes e situações correlatas. Tal situação já foi objeto de jurisprudência administrativa da CGU, nos pareceres nº 21900.000470/2015-94 e 23480.009656/2014-4.

Contribuição 115804 - 19/06/2026

Com relação a identificação de risco ao titular do dado, avaliação da probabilidade de ocorrência e gravidade do dano, entendo que deve seguir a metodologia de gestão de riscos de cada órgão. Não podemos ter mais de uma matriz de riscos e nem fazer avaliação aleatoriamente, sem critérios e método, principalmente se for qualitativo. Assim, o sistema deveria ter opção de inclusão de riscos para o titular para registro da tomada de decisão do órgão. Se é um critério para análise da demanda tem que haver um local de registro para a motivação do ato.

Contribuição 115809 - 19/06/2026

Contribuições em nome da [REDACTED]

Teste de Interesse Público

A [REDACTED] considera o Teste de Interesse Público um dos pontos mais relevantes do Guia, pois oferece metodologia prática para ponderar transparência, proteção de dados e riscos ao titular. Recomenda-se, entretanto, que o Guia detalhe melhor a aplicação do teste em situações que envolvam pessoas jurídicas e dados pessoais presentes em documentos empresariais.

A divulgação de informações deve considerar não apenas a existência de interesse público abstrato, mas o benefício coletivo concreto, a necessidade da informação para atingir esse benefício, a existência de meios menos invasivos e os riscos decorrentes da divulgação. O interesse público não deve ser confundido com curiosidade pública, conveniência genérica ou exposição ampla de documentos sem triagem prévia.

Contribuição 115810 - 19/06/2026

[REDACTED]

Teste de Interesse Público

A [REDACTED] recomenda incluir expressamente que o Teste de Interesse Público considere riscos de segurança institucional, fraudes, engenharia social, ataques cibernéticos, exposição de dados de empregados, fornecedores e representantes, bem como riscos concorrenciais e de violação de segredo industrial quando documentos empresariais estiverem envolvidos.

Sugestão de inclusão:

“Na aplicação do Teste de Interesse Público a documentos apresentados por pessoas jurídicas de direito privado à Administração Pública, a avaliação deverá considerar o benefício coletivo concreto da divulgação, a necessidade dos dados para a finalidade pretendida, a existência de meios menos invasivos, a possibilidade de divulgação parcial, anonimização, pseudonimização ou descaracterização, bem como riscos à privacidade de indivíduos, à segurança da informação, à prevenção de fraudes, à concorrência, ao segredo industrial e à proteção de informações estratégicas.”

Contribuição 115811 - 19/06/2026

Contribuições em nome da [REDACTED]

Transparência por desenho

A [REDACTED] considera positiva a inclusão do conceito de transparência por desenho. A adoção desse princípio pode reduzir retrabalho, diminuir riscos de exposição indevida de dados, padronizar procedimentos e permitir que informações públicas sejam disponibilizadas de forma segura desde a origem.

Sugere-se, contudo, que o Guia avance em recomendações práticas para os órgãos públicos. Em especial, recomenda-se prever que sistemas de protocolo, contratação, fiscalização, regulação, ouvidoria e gestão documental sejam estruturados com campos

segregados para informações públicas, informações pessoais, informações sensíveis, documentos sigilosos e informações empresariais protegidas.

Contribuição 115812 - 19/06/2026

Contribuições em nome da [REDACTED]

Transparência por desenho

A ausência dessa segregação gera insegurança para a Administração e para o setor privado, pois documentos inteiros podem acabar sendo restringidos ou divulgados indevidamente por falta de classificação adequada dos campos de informação.

Sugestão de inclusão:

“Os órgãos e entidades públicas devem, sempre que possível, estruturar seus sistemas, formulários, processos eletrônicos e bases documentais com segregação entre campos de informação pública, dados pessoais, dados pessoais sensíveis, informações protegidas por sigilo legal e informações empresariais estratégicas. Essa organização favorece a transparência ativa, reduz o risco de exposição indevida e permite respostas mais céleres e proporcionais a pedidos de acesso à informação.”

Contribuição 115961 - 19/06/2026

vide item 4 - documento anexo

Contribuição 116188 - 21/06/2026

A transparência prevista na Lei de Acesso à Informação (LAI) deve ser exercida em harmonia com os princípios da Lei Geral de Proteção de Dados (LGPD). Em ambientes de amplo acesso público, a divulgação de dados em excesso pode ultrapassar a finalidade legítima do controle social, especialmente diante da atual capacidade de cruzamento de informações por meios digitais. Dessa forma, a publicidade dos atos administrativos deve se limitar aos dados estritamente necessários para garantir a fiscalização e a transparência, evitando a exposição desnecessária de informações identificáveis. A adoção de medidas como a supressão ou o mascaramento de dados não essenciais preserva o acesso à informação sem comprometer a proteção de dados pessoais, conciliando os objetivos da LAI, da LGPD e o controle social. O controle social se dá de forma ativa pela sociedade e não de forma passiva com a simples exposição.

Contribuição 116228 - 21/06/2026

Em anexo, contribuição para o subitem 4.3 Transparência por desenho, com respeito à coleta de dados (através) de terceiros.

Contribuição 116253 - 21/06/2026

Inclusão: incluir o pesquisador como nova categoria na Tabela de Titulares: “• Tipo de titular: pesquisador / colaborador científico. • Proximidade com o Estado: média. • Expectativa de privacidade: média. • O que pode ser publicado? (em tese): nome completo; instituição de vínculo; número de identificação acadêmica; título do projeto de pesquisa financiado ou apoiado por infraestrutura pública.”

Justificativa: refletir a realidade do Sistema Nacional de CT&I. As categorias atuais limitam-se a relações administrativas ou assistenciais. O pesquisador que utiliza infraestruturas públicas possui uma relação diferenciada com o Estado. Nesse sentido, a explicitação deste titular

auxiliará as instituições de ensino e os órgãos de fomento a calibrarem corretamente o Teste de Interesse Público, que servirá como apoio necessário para ponderar, no caso concreto, se o direito de acesso à informação e o benefício coletivo superam o direito à privacidade e proteção de dados do titular.

Contribuição 116254 - 21/06/2026

Inclusão: inserir ao roteiro do Teste de Interesse Público mecanismo de tipificação de hipóteses para dispensa de avaliação caso a caso: “Para otimização do fluxo de trabalho e eficiência administrativa, os órgãos e entidades poderão adotar matrizes internas de decisão consolidada (presunções operacionais) para situações recorrentes e de baixa complexidade. Essas matrizes dispensam a reaplicação integral do Teste de Interesse Público, observados os seguintes parâmetros: a) consolidação prévia das hipóteses em que há evidente presunção de interesse público na divulgação (ex: dados vinculados a desembolsos financeiros públicos); e b) consolidação prévia das hipóteses em que há evidente presunção de restrição de acesso (ex: dados de saúde, vulnerabilidade social ou outros dados sensíveis).” ++

Contribuição 116255 - 21/06/2026

'++ Justificativa: otimizar a gestão administrativa e garantir a eficiência no atendimento à LAI pelas instituições de ensino, pesquisa e inovação. A aplicação individualizada do Teste de Interesse Público para cada pedido de acesso a informações pessoais impõe um ônus operacional às entidades. Nesse sentido, a criação de “presunções operacionais” padroniza os cenários mais comuns e cotidianos, preservando a análise detalhada apenas para os casos complexos ou que apresentem riscos evidentes à privacidade e proteção de dados pessoais.

Contribuição 116271 - 22/06/2026

Excluir o parágrafo que in:

"Se o órgão usa do Sistema Eletrônico de Informações (SEI) como plataforma digital de gestão de documentos e processos administrativos, pode-se criar dois processos relacionados. O processo principal ..."

O Guia não pode orientar operacional de sistemas específicos, mas sim boas práticas. Por exemplo, evitar repetição de dados de qualificação de Interessado do processo administrativo em cada documento, deixando a qualificação detalhada na instauração do processo. A prática disposta no parágrafo a ser retirado não é considerada adequada, onerando muito o operacional da instrução processual e duplicando informações desnecessariamente. Geração de cópia com tarjamento deve ser meio para atendimento de pedido de vistas. É mais importante orientar que os processos administrativos sejam instruídos orientados à publicidade, evitando inserção de informações restritas desnecessariamente que venha a tornar o documento restrito.

Contribuição 123337 - 18/07/2026

Contribuição ao Capítulo 4 — Itens 4.1 e 4.2

A ausência de critérios operacionais alimenta o "escudo argumentativo": uso da LGPD como barreira genérica à transparência (caso INEP; Acórdão TCU 96/2024). Proponho três ajustes

à minuta: (i) inverter os Passos 4 e 5 — necessidade/minimização antes do sopesamento; (ii) incluir o RIPD como registro formal da negativa complexa (Res. CD/ANPD nº 2/2022, art. 41 LGPD); (iii) acoplar os Passos 1–3 ao e-SIC como filtros automáticos, reservando a análise humana para conflitos genuínos.

Protótipo funcional (HTML/JS, 100% local, sem nuvem) e Manual Didático anexados.

Contribuição completa com fundamentação ABNT no PDF em anexo.

Contribuição 123339 - 18/07/2026

Contribuição à Consulta CGU/ANPD — Guia LAI×LGPD, Itens 4.1 e 4.2

Submeto subsídio técnico-acadêmico desenvolvido no âmbito

. Apresento o

. A ferramenta roda integralmente no navegador, sem envio de dados a servidores externos.

O subsídio escrito, a ferramenta e o tutorial de uso estão disponíveis em:

Contribuição 123732 - 22/07/2026

O roteiro do "Teste de Interesse Público" (item 4.2) guarda grande semelhança estrutural com o teste de balanceamento (Legitimate Interest Assessment, ou LIA) já consolidado pela ANPD para as hipóteses do art. 7º, IX, e art. 11, II, "g", da LGPD.

Ambos exigem identificação do dado, mapeamento de benefícios, avaliação de risco ao titular, ponderação e registro motivado da decisão.

Sugere-se que o Guia faça remissão expressa a essa metodologia já testada e utilizada, indicando que os órgãos públicos podem se valer da mesma estrutura documental (e, quando possível, dos mesmos templates internos de LIA) para o registro exigido no item 6 do roteiro. Isso evitaria a criação de dois fluxos documentais paralelos para uma análise essencialmente equivalente, reduzindo retrabalho e uniformizando o padrão.

Contribuição 124156 - 23/07/2026

Pág. 26: "Tabela de exemplos – divulgação de CPF descaracterizado"

O fornecimento de CPF, ainda que descaracterizado, não encontra respaldo legal, além de poder servir de parâmetro para a identificação do CPF completo.

Pág. 27: "Tabela de exemplos de aplicação do teste de interesse público"

Não há obrigação legal de realizar o teste de interesse público. A previsão no guia pode levar o leitor a entender pela obrigatoriedade e, inclusive, ser fazer com que ocorra mais um pedido de acesso à informação (acesso ao teste).

Contribuição 124372 - 24/07/2026

Segue em anexo relatório de pesquisa conduzida sobre o tema citado na contribuição enviada.

Contribuição 124389 - 24/07/2026

O Capítulo 4, ao trazer uma ótima ferramenta de avaliação de interesse público, poderia torná-la mais abrangente, sendo útil também para a classificação de documentos quanto ao nível de sigilo. Até onde foi a pesquisa conduzida por mim no Lab GGPP (ver <https://doi.org/10.1590/2317-6172202415>), não há, ao menos nas Forças Armadas, baremas claros para fazer esse teste de interesse público no processo e no ato de classificar documentos. Particularmente, a figura do item 4.2 poderia ser facilmente adaptada para toda a sorte de informações que, de alguma forma, possam vir a ser condicionalmente restritas aos olhos dos cidadãos, apenas retirando a menção a dados pessoais e incluindo uma redação mais genérica relativa a informações ou dados. Não sendo possível fazê-lo neste guia, sugere-se a criação de outro guia específico para tal.

Contribuição 124392 - 24/07/2026

Segue em anexo contribuição

Contribuição 124393 - 24/07/2026

Contribuições técnicas ao Capítulo 4 do Guia de Transparência e Proteção de Dados Pessoais, fundamentadas em evidências, dados e boas práticas internacionais. As sugestões buscam aprimorar o texto-base, tornando suas orientações mais claras, objetivas, previsíveis e adequadas aos diferentes contextos da Administração Pública relacionados ao tratamento e à divulgação de informações.

Contribuição 124450 - 24/07/2026

Devido à extensão das contribuições, [REDACTED]

encaminharam-nas ao e-mail dasai@cgu.gov.br em 24/07, por meio do endereço eletrônico [REDACTED]

Contribuição 113203 - 12/06/2026

1 - Deixar claro e exposto num parágrafo que independem de classificação pelo órgão/entidade informações submetidas a outras hipóteses de sigilo previstas na legislação, como fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial, segredo de justiça e dados pessoais. O órgão/entidade deve realizar a classificação EXCLUSIVAMENTE das informações previstas no art. 23 da LAI e legislação complementar do ente federado.

2 - Entre os sigilos legais que foram listados, sugiro incluir sigilo de atividades de pesquisa e criação desenvolvidas por instituições científicas, tecnológicas e de inovação (ICTs), cfe. Lei federal nº 10.973, de 2004 (Lei de Inovação) (art. 12).

3 - Entre os sigilos legais, incluir também o segredo de justiça dos processos criminais, que não constou a fundamentação: Lei federal nº 13.105, de 2015 (Código de Processo Civil) (arts. 11 e 189) e Decreto-Lei nº 3.689, de 1941 (Código de Processo Penal) (art. 201, § 6º).

Contribuição 113572 - 12/06/2026

O Guia não considera a realidade brasileira de vazamentos massivos, rsrs.

Sugestão: Inserir referência expressa à evolução tecnológica e aos riscos futuros de tratamento automatizado.

Sugestão: Inserir orientação para que a análise de divulgação considere a possibilidade de

correlação com bases já expostas em incidentes de segurança.

Contribuição 114664 - 13/06/2026

Embora o Guia apresente as hipóteses legais de restrição de acesso à informação, não estabelece metodologia para orientar decisões em situações nas quais coexistam interesse público na divulgação e riscos à privacidade dos titulares. Recomenda-se a adoção de procedimento inspirado no GDPR (arts. 5º, 25 e 35; Recitals 47, 75 e 76), prevendo que o órgão registre formalmente: (i) o interesse público da divulgação; (ii) a necessidade dos dados pessoais para atingir a finalidade pretendida; (iii) a existência de alternativas menos invasivas, como anonimização ou divulgação parcial; (iv) os riscos aos titulares; e (v) a justificativa da decisão adotada. Tal medida fortalece os princípios da necessidade e da responsabilização previstos na LGPD, promovendo maior segurança jurídica, uniformidade de entendimento e proteção dos direitos fundamentais.

Contribuição 114744 - 14/06/2026

Contribuições em anexo.

Contribuição 114751 - 15/06/2026

Contribuições ao Capítulo 1 em anexo.

Contribuição 114969 - 15/06/2026

Relativamente ao trecho "É importante destacar que a motivação do cidadão não pode ser usada como critério para considerar um pedido como desarrazoado (art. 10, §3º da LAI - São vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público)." , talvez precise ser feita uma distinção entre motivação do cidadão e finalidade do tratamento. Muitas vezes o gestor quer negar o fornecimento apelando à LGPD porque o solicitante não forneceu a finalidade, confundindo a finalidade do tratamento com a finalidade que cidadão pretende dar às informações obtidas.

Contribuição 115248 - 17/06/2026

Em relação aos exemplos de sigilo, dever-se-ia estar objetivamente relacionado o dever de sigilo profissional, uma vez que várias profissões, para o seu exercício, necessitam de tratar dados pessoais, várias delas prestados por serviços públicos, como o sigilo da fonte para jornalistas, o sigilo de informações e prontuários médico/saúde, o sigilo no tratamento de informações pessoais entre advogados e clientes. O quadro em destaque que aponta que apenas Lei pode estabelecer hipótese de sigilo carece de referência legal. Há situações em que áreas de atividades econômicas e profissionais, em que a atuação é regulada, estabelecem regulamentos de proteção da informação que devem ser observados pelos operadores.

Contribuição 115252 - 17/06/2026

Não entendi a razão de fazer parte do guia de transparência e tratamento de dados pessoais a seção sobre fundamentos administrativos para negativa de informação, sem que entre eles esteja relacionado um principal, altamente correlacionado com a temática, que seria a

solicitação de dado pessoal por terceiro para uso que divirja da finalidade inicial que ensejou o tratamento de dados pessoais do titular pela administração pública. Esse é um ponto que merece tratamento objetivo em um guia como esse, extremamente relevante e que foi, inclusive, objetivo de ADI e julgamento do STF, tendo consequências práticas para a adequação do decreto de compartilhamento de dados na Administração Pública Federal, estabelecendo um conjunto de salvaguardas ao cidadão que não está mencionado nesse guia (e deveria estar).

Contribuição 115445 - 17/06/2026

Contribuição em anexo.

Contribuição 115619 - 18/06/2026

Recomendo inserir referência expressa ao direito fundamental à proteção de dados pessoais, introduzido pela Emenda Constitucional nº 115/2022, que incluiu o inciso LXXIX ao art. 5º da Constituição Federal, bem como reforçar a necessidade de observância do princípio da harmonização entre transparência e proteção de dados previsto no art. 6º, inciso III, da Lei nº 13.709/2018 (LGPD). Também é recomendável explicitar que a negativa de acesso à informação deve observar os princípios da motivação e da proporcionalidade, previstos no art. 50 da Lei nº 9.784/1999, sendo vedadas restrições genéricas ou sem fundamento legal. Além disso, convém destacar que o tratamento e a divulgação de informações públicas devem observar as diretrizes de governança e compartilhamento de dados estabelecidas pelo Decreto Federal nº 10.046/2019, bem como os entendimentos consolidados da Controladoria-Geral da União (CGU) e da Autoridade Nacional de Proteção de Dados (ANPD) anonimização ou pseudonimização.

Contribuição 115624 - 18/06/2026

Encaminhamos anexa a contribuição.

Contribuição 115629 - 18/06/2026

Segue anexa a contribuição.

Contribuição 115788 - 19/06/2026

Concorda-se com a premissa de que a transparência deve ser a regra e o sigilo a exceção. Contudo, recomenda-se que o Guia reforce, de maneira mais explícita, que as exceções à transparência não se limitam às hipóteses de classificação da informação, abrangendo também sigilos legais específicos, proteção de dados pessoais, documentos preparatórios, segredo industrial, sigilo comercial, sigilo fiscal, sigilo bancário, propriedade intelectual e informações cuja divulgação possa afetar a segurança institucional, econômica ou competitiva de agentes privados. Sugere-se aprimorar o texto para evitar interpretações segundo as quais todo documento apresentado por empresa à Administração Pública, pelo simples fato de estar sob custódia estatal, passaria automaticamente a ser público em sua integralidade.

Contribuição 115789 - 19/06/2026

Recomenda-se que o Guia destaque a necessidade de análise concreta, motivada e proporcional antes da divulgação de documentos empresariais que contenham dados pessoais ou informações protegidas por sigilo legal, segredo industrial, sigilo comercial ou legítimo interesse concorrencial.

Sugestão de inclusão:

“Nos casos em que documentos custodiados pela Administração Pública contenham informações fornecidas por pessoas jurídicas de direito privado, especialmente em processos de contratação, fiscalização, regulação, fomento, inovação, certificação ou habilitação técnica, a análise de acesso deverá considerar, além do interesse público na divulgação, a eventual incidência de sigilos legais, segredo industrial, propriedade intelectual, informações concorrencialmente relevantes, dados pessoais de representantes, empregados ou terceiros, bem como riscos à segurança, à concorrência e à competitividade”.

Contribuição 115820 - 19/06/2026

Anexamos arquivo compilado com todas as contribuições a esta consulta pública.

Contribuição 115929 - 19/06/2026

Proposta de aprimoramento: incluir orientação específica para empresas estatais, sociedades de economia mista e demais entidades controladas pelo Poder Público que atuem em ambiente concorrencial e regulado, especialmente quando desenvolvam atividade econômica em competição com agentes privados.

Fundamentação: nesses casos, a aplicação harmônica da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados Pessoais (LGPD) exige parâmetros interpretativos mais claros, capazes de compatibilizar a transparência pública e o controle social com a proteção de dados pessoais e com o resguardo de informações estratégicas, comerciais, negociais, concorrenciais ou submetidas a regimes legais, regulatórios ou contratuais de confidencialidade.

Contribuição 115949 - 19/06/2026

Capítulo 1 — Direito de acesso à informação e seus limites

Sugerimos que o rol exemplificativo de sigilos legais (art. 22 da LAI) do capítulo 1.2 mencione expressamente o sigilo profissional, em especial o sigilo médico, por sua elevada relevância para a Administração Pública que custodia informações de saúde (redes públicas, perícias, programas e parcerias com instituições de saúde). Trata-se de sigilo legal típico, preservado pela LAI, que não se confunde com a (inexistente) criação de sigilo pela LGPD e que convive com o regime do art. 31. Sugere-se acrescentar:

“Sigilo profissional, inclusive o sigilo médico, protege informações confiadas em razão do exercício de profissão regulamentada, amparado, entre outros, no art. 154 do Código Penal, na Lei nº 12.842/2013 (exercício da medicina) e, quanto à guarda e confidencialidade de prontuários, na Lei nº 13.787/2018, constituindo exceção legítima ao acesso preservada pelo art. 22 da LAI.”

Contribuição 115950 - 19/06/2026

Capítulo 1 — Direito de acesso à informação e seus limites

Sugerimos que o rol exemplificativo de sigilos legais (art. 22 da LAI) do capítulo 1.2 mencione expressamente o sigilo profissional, em especial o sigilo médico, por sua elevada relevância para a Administração Pública que custodia informações de saúde (redes públicas, perícias, programas e parcerias com instituições de saúde). Trata-se de sigilo legal típico, preservado

pela LAI, que não se confunde com a (inexistente) criação de sigilo pela LGPD e que convive com o regime do art. 31. Sugere-se acrescentar:

“Sigilo profissional, inclusive o sigilo médico, protege informações confiadas em razão do exercício de profissão regulamentada, amparado, entre outros, no art. 154 do Código Penal, na Lei nº 12.842/2013 (exercício da medicina) e, quanto à guarda e confidencialidade de prontuários, na Lei nº 13.787/2018, constituindo exceção legítima ao acesso preservada pelo art. 22 da LAI.”

Contribuição 116118 - 20/06/2026

Sugerimos incluir orientação específica para sociedades de economia mista que atuam em ambiente concorrencial e regulado, reconhecendo a necessidade de compatibilizar transparência pública com a proteção de informações estratégicas, negociais, empresariais e outros sigilos legais a quais essas empresas estejam sujeitas.

Contribuição 116119 - 20/06/2026

Propomos diferenciar com maior clareza o direito de acesso à informação pública, regido pela LAI, dos pedidos que deveriam ser tratados por outros canais de atendimento direcionados ao cidadão, cliente ou consumidor, como as demandas de consultas individuais personalíssimas ou de interesse apenas de um indivíduo, evitando desvio de finalidade da LAI.

Contribuição 116244 - 21/06/2026

As contribuições apresentadas possuem caráter colaborativo e foram elaboradas com o objetivo de auxiliar no aprimoramento didático, interpretativo e operacional do Guia, especialmente para apoiar a atuação prática dos agentes públicos na aplicação conjunta da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados Pessoais (LGPD).

Contribuição 116247 - 21/06/2026

Incluir, na lista exemplificativa de documentos preparatórios, os projetos de PD&I em andamento como exemplo expresso de restrição temporária de acesso: “Documentos relacionados a projetos de pesquisa, desenvolvimento científico e inovação tecnológica em andamento: informações que subsidiam projetos não concluídos (como protótipos, testes de conceito, especificações técnicas, rascunhos de patentes e negociações com parceiros) podem ter o acesso restrito até o encerramento da pesquisa.”

Justificativa: refletir de forma mais abrangente a realidade das entidades de ensino, pesquisa e desenvolvimento tecnológico. A explicitação desse contexto diretamente no Guia é de grande valia, pois a LAI já protege a atividade de pesquisa em diversos dispositivos. Antes da conclusão de um projeto, tramitam documentos técnicos e negociais altamente sensíveis. Adicionar este exemplo confere maior segurança jurídica para que protejam a inovação, harmonizando o guia c/ as diretrizes do Marco Legal de CT&I.

Contribuição 116248 - 21/06/2026

Esse Guia é muito relevante para diminuir a insegurança gerada por dúvidas sobre a interação da Lei de Acesso à Informação (LAI) com a Lei Geral de Proteção de Dados (LGPD), o que leva, por vezes, à redução da transparência pública. Sugere-se a inclusão de um glossário com os principais termos e conceitos utilizados nesse Guia, com as diretrizes da

linguagem simples, para facilitar a compreensão pelos usuários, reduzir dúvidas e diferentes interpretações, bem como contribuir para a aplicação das orientações por agentes públicos, ouvidorias, serviços de informação ao cidadão, encarregados pelo tratamento de dados pessoais e demais profissionais que atuam com transparência e proteção de dados. A adoção de um glossário contribuirá para padronizar a linguagem utilizada no Guia, aumentar a segurança jurídica, facilitar a compreensão dos conceitos e fortalecer a aplicação integrada da transparência pública, do acesso à informação e da proteção de dados pessoais.

Contribuição 116263 - 21/06/2026

Seguem contribuições em nome da [REDACTED], já enviadas em cada tópico, de maneira consolidada.

Contribuição 116265 - 21/06/2026

SEÇÃO 1 – Direito de acesso à informação e seus limites: Inclusão na lista exemplificativa de documentos preparatórios dos projetos de PD&I em andamento. Fundamentação legal: art. 7o, §1o e art. 23, VI da LAI. Tal inclusão proporcionará maior segurança jurídica para a proteção da inovação e a harmonia do Guia com as diretrizes do Marco Legal de CT&I (Lei no 13.243/2016).

Contribuição 116266 - 21/06/2026

Alterar o título do item 1.1 para deixar claro que o sigilo é exceção fundamentada, em consonância do inciso I do art. 3º com o art. 22 da LAI:

- "1.1. A transparência é a regra e o sigilo é exceção fundamentada"

Deixar mais claro quando mencionar classificação em grau de sigilo, informar sempre a expressão "em Grau de Sigilo":

"1.2. Exceções da transparência

Informações Classificadas em Grau de Sigilo"

Adicionar "em grau de sigilo" e "conforme a imprescindibilidade da informação para a segurança da sociedade e do Estado (grau de risco)":

"Nesses casos, aplica-se a classificação da informação, que consiste no ato formal de limitar temporariamente o acesso a documentos ou dados públicos classificados em grau de sigilo. O prazo de restrição varia conforme a imprescindibilidade da informação para a segurança da sociedade e do Estado (grau de risco):"

Contribuição 116269 - 21/06/2026

Deve apresentar uma lista mais completa das hipóteses legais já mapeadas na legislação. Ou link para um hotsite da CGU com tal lista.

- Veja lista mapeada na comunidade do SEI:

<https://docs.google.com/spreadsheets/d/e/2PACX-1vTgEpMSzvVw1yWGb2YPCfBVh4dyVyah9gYrG3cxtSVZSiWZqv25EDROkxj410XCE3YMrMcO5y0ZduEi/pubhtml>

Contribuição 116267 - 21/06/2026

Ajustar o texto abaixo para deixar claro que antes de enquadrar nos incisos é preciso atender a condição disposta no caput do art. 24 da LAI:

"A LAI (arts. 23 e 24) estabelece nove hipóteses taxativas em que a classificação em grau de sigilo pode ser aplicada. Assim, se estiver diante de informações imprescindíveis à

segurança da sociedade ou do Estado (condição do caput do art. 24 da LAI) deve enquadrar a classificação em uma dessas hipóteses legais e, portanto, podem ser formalmente classificadas."

Contribuição 116268 - 21/06/2026

SEÇÃO 1 – Direito de acesso à informação e seus limites: Inclusão dos projetos de PD&I, em andamento, na lista exemplificativa de documentos preparatórios. Fundamentação legal: art. 7º, §1º e art. 23, VI da LAI. Tal inclusão proporcionará maior segurança jurídica para a proteção da inovação e a harmonia do Guia com as diretrizes do Marco Legal de CT&I (Lei nº 13.243/2016).

Contribuição 124150 - 23/07/2026

Segue a contribuição para o primeiro item, para colaborar a visão de uma empresa estatal que atua em ambiente concorrencial, considerando as peculiaridades das sociedades de economia mista que lidam com informações estratégicas, negociais e comerciais, além de dados funcionais.

Contribuição 124378 - 24/07/2026

Esta é a primeira de uma série de contribuições do [REDACTED]

Observado

o guia, verificou-se que ele, acertadamente, vai além da análise de pedidos de informação que envolvam dados pessoais. Seu texto sistematiza todas as hipóteses de exceção à transparência e ainda apresenta modelos, parâmetros e roteiros, como o teste de interesse público e a transparência por desenho. Para refletir esse alcance, sugere-se, na "contextualização", deslocar o último parágrafo para que seja o primeiro e alterar seu texto para: «Este Guia traz orientações, parâmetros, critérios e roteiros para apoiar agentes públicos na análise e decisão sobre a concessão ou restrição do acesso à informação, pessoais ou não, em transparência ativa ou passiva, bem como no registro de processos e documentos em sistemas, como o SEI, no compartilhamento de dados e em outras medidas de tratamento.»

Contribuição 124379 - 24/07/2026

Na subseção "informações classificadas", para facilitar a compreensão das hipóteses, autoridades competentes e prazos, sugere-se manter o primeiro parágrafo, alterar a ordem do quarto para que passe a ser o segundo seguido do quadro rol taxativo, com o seguinte texto:

«As informações não devem ser passíveis de quaisquer restrições tão somente por tratarem ou terem sido produzidas por órgãos ou entidades dos setores de defesa, segurança, relações internacionais ou outros ligados às demais categorias previstas no Anexo II do Decreto nº 7.845, de 2012. A LAI (arts. 23 e 24) estabelece nove hipóteses taxativas em que a classificação pode ser aplicada. Assim, apenas informações enquadradas nessas hipóteses podem ser formalmente classificadas.»

Contribuição 124380 - 24/07/2026

Após o parágrafo da contribuição Contribuição [REDACTED] pelos mesmos motivos apresentados naquela contribuição, incluir o parágrafo abaixo:

«A decisão de classificação, que consiste no ato formal de limitar temporariamente o acesso a documentos ou dados, é privativa das seguintes autoridades, conforme os graus e prazos indicados:

- no grau ultrassecreto – até 25 anos, renovável uma única vez: Presidente e Vice-Presidente da República, Ministros de Estado, Comandantes das Forças Armadas e Chefes de Missões Diplomáticas e Consulares permanentes no exterior;
- no grau secreto – até 15 anos: titulares de autarquias, fundações, empresas públicas e sociedades de economia mista; e
- no grau reservado – até 5 anos: cargos e funções comissionadas de nível 15 e seus equivalentes.»

Contribuição 124381 - 24/07/2026

Na sequência da Contribuição, para exclusão de conteúdos redundantes (3º e 5º parágrafos), sugere-se que a subseção “informações classificadas” seja encerrada com os parágrafos abaixo: «A classificação deve sempre adotar o grau menos restritivo possível, considerando o interesse público. O prazo conta a partir da data de produção da informação. O acesso público ocorre a partir do término desse prazo ou, alternativamente, por evento estabelecido como termo final de restrição, se consumado antes do transcurso do prazo máximo de classificação.

Encerrado esse prazo ou evento, a informação torna-se acessível, devendo o órgão ou a entidade avaliar, contudo, se há partes que permanecem protegidas por outras hipóteses de restrição de acesso previstas na legislação. Outras restrições de acesso previstas na LAI, como informações pessoais, sigilos legais ou documentos preparatórios, não se confundem com a classificação, pois seguem regimes próprios de proteção.”

Contribuição 124382 - 24/07/2026

Na sequência da contribuição, para melhorar esclarecimento das especificidades relacionadas às informações classificadas, sugere-se que seja incluído parágrafo que indique que documentos que contenham informações classificadas não devem ser objeto de registro no SEI ou em outros sistemas de protocolo aberto, observando que seu tratamento é tratado por regulamentação específica, como o Decreto 7.845, de 2012, a IN CGU 33, de 2024, e a Resolução CMRI 7, de 2024.

Contribuição 124383 - 24/07/2026

Na subseção “documentos preparatórios”, o texto permite interpretação ampliada da restrição baseada nessa hipótese, com risco de banalização. Com base no Parecer da CGU sobre Despacho Presidencial de 1º de janeiro de 2023, sugere-se que início do 2º parágrafo seja alterada para «A restrição somente pode ser aplicada quando necessária para proteger processo decisório em curso, evitando pré julgamentos ou interferências, portanto, apenas quando a divulgação puder frustrar a própria finalidade do procedimento ao qual se encontra vinculado ou eventuais expectativas dos administrados. Nesses casos, o acesso é garantido após a edição do ato final que utilizou esses documentos como fundamento.» Quanto ao último parágrafo, sugere-se indicar a cautela de que seja verificado se dos documentos que passarão a ser franqueados não possam constar informações sobre as quais recaiam outras hipóteses de restrição.

Contribuição 124384 - 24/07/2026

Tal pedido de cautela contido na Contribuição é motivado por resultados de pesquisas

realizadas no âmbito do laboratório, segundo as quais os servidores têm se utilizado com frequência dessa classificação de informação para ocultar dados do público, sem que se enseje o processo custoso, burocrático e rastreável da classificação por níveis de sigilo, mas não é claro que, nas atividades de inteligência, todo e qualquer documento gerado esteja ligado a uma decisão ou processo decisório.

Contribuição 124385 - 24/07/2026

Sugere-se que a subseção “dados pessoais” tenha o título alterado para “informações pessoais relativas à intimidade, vida privada, honra e imagem”. Essa contribuição é importante para evitar a banalização da aplicação de restrição a dados pessoais sem qualquer análise, como preceituado pela LGPD. Sugere-se ainda, pelo mesmo motivo, que o segundo parágrafo da página 12 seja incluído entre o primeiro e o terceiro parágrafo da subseção sob comento.

«A LAI não protege todo dado pessoal, as informações protegidas pelo art. 31 são aquelas relacionadas com a intimidade, vida privada, honra e imagem das pessoas.»

Contribuição 124390 - 24/07/2026

Contribuições técnicas ao Capítulo 1 do Guia de Transparência e Proteção de Dados Pessoais, fundamentadas em evidências, dados e boas práticas internacionais. As sugestões buscam aprimorar o texto-base, tornando suas orientações mais claras, objetivas, previsíveis e adequadas aos diferentes contextos da Administração Pública relacionados ao tratamento e à divulgação de informações.

Contribuição 124447 - 24/07/2026

Devido à extensão das contribuições, a [REDACTED] encaminham-nas ao e-mail dasai@cgu.gov.br em 24/07, por meio do endereço eletrônico [REDACTED].

Contribuição 124480 - 24/07/2026

No que tange à gestão de documentos (gestão documental) é importante enfatizar o ciclo de vida que o conjunto de operações que formam a gestão documental abarca: produção, tramitação, uso, avaliação e arquivamento, conforme a Lei nº 8.159, de 8 de janeiro de 1991. Sugestão:

Por fim, é importante destacar que o pleno exercício do direito de acesso à informação depende do constante aprimoramento da gestão documental, com políticas, sistemas e processos que viabilizem a adequada produção, tramitação, uso, organização, avaliação, arquivamento e preservação objetivando a disponibilização das informações públicas, conforme determinam a Constituição Federal e a LAI. Ou seja, um órgão não pode se eximir indefinidamente de atender um pedido de informação por dificuldades operacionais; ele tem o dever de melhorar seus processos e sistemas para garantir que a sociedade tenha acesso às informações públicas, cumprindo os princípios da transparência, eficiência e interesse coletivo.

Contribuição 124481 - 24/07/2026

Na qualidade de Analista de xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx,
encaminho, em anexo, as contribuições da organização para a consulta pública do Guia de
Transparência e Proteção de Dados Pessoais.

Contribuição 124492 - 24/07/2026

Na qualidade de representante da [REDACTED] encaminho contribuição à Consulta Pública assinado e apoiado por 37 entidades e 56 especialistas. Descrição e fundamentos em anexo.

Contribuição 113411 - 12/06/2026

O inc. II do § 3º do art. 31 da LAI afasta o uso do consentimento quando:

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; Portanto, o uso de informações pessoais relacionadas à intimidade, vida privada ... é vedado nesse contexto de uso e sem o consentimento. A atual redação do guia poderá gerar equívocos, agravados pela menção à LGPD (sem considerar "Lex specialis derogat generali").

Em geral, a busca por uma redação mais determinística e exemplificativa poderá provocar incidentes em organizações públicas, ao desconsiderar contextos e exceções. Exemplo: Dado pessoal sensível não é obrigatoriamente um dado de acesso restrito, ou seja, há dado pessoal sensível sujeito ao controle social e à transparência pública, como aqueles divulgados em resultados de processos seletivos com modalidades de ingresso por ação afirmativa (ex.: Lei de Cotas).

Contribuição 113625 - 12/06/2026

Sistemas modernos conseguem inferir informações altamente sensíveis a partir de dados aparentemente comuns.

A avaliação de divulgação deverá considerar que informações não classificadas como sensíveis podem, quando analisadas isoladamente ou em conjunto com outras bases de dados, permitir inferências sobre aspectos protegidos pela LGPD.

A análise de divulgação de dados pessoais deve considerar não apenas riscos presentes, mas também riscos futuros decorrentes da evolução tecnológica, incluindo novas capacidades de correlação, inferência e processamento automatizado.

O princípio da precaução recomenda que decisões atuais considerem impactos futuros razoavelmente previsíveis.

Contribuição 114682 - 13/06/2026

Sugiro a inclusão de diretriz específica para avaliação de risco aos titulares antes da divulgação de informações pessoais com fundamento no interesse público e geral preponderante. Embora o Guia determine a realização de ponderação entre transparência e privacidade, seria recomendado que essa análise considere, de forma expressa e documentada, a probabilidade e a gravidade dos impactos decorrentes da divulgação, tais como discriminação, fraude, danos reputacionais, riscos à segurança ou exposição indevida da vida privada. A proposta inspira-se nos Recitals 75 e 76 e no Art. 35 do GDPR, que exigem avaliação dos riscos aos direitos e liberdades das pessoas antes de tratamentos potencialmente impactantes. A adoção desse critério fortalecerá a fundamentação das decisões, aumentará a uniformidade entre órgãos públicos e promoverá maior segurança jurídica na aplicação conjunta da LAI e da LGPD.

Contribuição 114746 - 14/06/2026

Contribuições em relação ao capítulo 3.

Contribuição 115283 - 17/06/2026

Acredito ser fundamental para um guia o uso de linguagem adequada e apropriada. Na seção 3 e subseção 3.3 o título aborda adequadamente o termo acesso. Contudo o texto que se segue trata de "fornecimento" como se algo fosse ser entregue a outro. Vale lembrar que a própria LAI e outros normativos vigentes apontam que o acesso não tem uma forma única, como o "fornecimento", pode incluí-lo mas não deve ser a ele limitado. Sugestão: trocar todos os termos "fornecimento" por "acesso". A escolha da forma do acesso é uma prerrogativa do controlador do dado, inclusive quando precisa decidir por exemplo o acesso a uma documentação, mas a oposição de informação detalhada do titular no próprio documento, quando essa representa uma violação aos seus direitos.

Contribuição 115292 - 17/06/2026

Acerca da seção 3.4:

A dispensa do Termo de Responsabilidade fragiliza mecanismos de responsabilização no tratamento de dados pessoais. Ainda que o acesso seja legítimo, inclusive para controle social ou por interesse público preponderante, tais fundamentos não afastam a necessidade de garantir o uso adequado, seguro e proporcional das informações após o seu compartilhamento. Dessa forma, sugerimos a seguinte alteração:

Onde se lê:

“A assinatura de termo de responsabilidade pode ser dispensada quando: (...) for comprovado o interesse público e geral preponderante que justifique o acesso;”

Leia-se:

“A assinatura de Termo de Responsabilidade não será dispensada nos casos de acesso a dados pessoais, inclusive quando houver interesse público e geral preponderante, devendo ser adotado Termo de Responsabilidade, ainda que em modelo simplificado, como medida de responsabilização, vinculação à finalidade e prevenção de uso indevido, sem prejuízo do direito de acesso à informação.

Contribuição 115295 - 17/06/2026

Ainda na linha do cuidado com a linguagem, o guia parece misturar alguns conceitos, tratando-os como "sinônimos" quando não são. Divulgação não me parece ser a mesma coisa que acesso. O acesso pode ser controlado e específico. Divulgação é o ato ou efeito de tornar algo público, difundindo ou propagando uma informação, produto ou ideia para um grande número de pessoas. Da mesma forma que o cuidado com o termo "fornecimento", especialmente o item "i" da subseção 3.3 merece um cuidado em relação à divulgação, que seria mais apropriado o termo acesso. Isso é importante, por exemplo, na própria prerrogativa do tratamento de dado pessoal sem o consentimento para a realização de pesquisa não faria sentido se o objetivo da pesquisa for divulgar a informação pessoal acessada, na verdade o acesso pressupõe que a informação será utilizada para a construção do conhecimento sobre fenômenos de aplicação geral, esse é o fundamento do método científico.

Contribuição 115296 - 17/06/2026

Especialmente no que diz respeito à seção 3.4 é importante recuperar e apresentar formal e

objetivamente, uma vez que o guia apresenta desta forma as hipóteses que dispensariam o termo de responsabilidade quando do uso por terceiro de informação pessoal, é importante apresentar as exigências a serem observadas pelo "segundo" que obteve do titular ("o primeiro") quando tratou o dado pessoal para uma finalidade específica, especialmente o que dispõem os § 3º, § 4º, § 5º, § 6º e § 7º, que não o desobrigam (o segundo) de observar as disposições existentes (previstos na legislação vigente não exclusivamente na LGPD), os fundamentos e os princípios gerais, os direitos dos titulares e as disposições para o tratamento de dados pessoais estabelecidos na LGPD.

Contribuição 115297 - 17/06/2026

Em relação ao item h, da Subseção 3.3 é importante (já tratada em outra contribuição) apresentar as condições estabelecidas pelo Supremo Tribunal Federal em relação ao compartilhamento de dados na Administração Pública, resultantes das ADI 6649 e ADPF 695, que ensejaram a adequação do Decreto nº 10.046/2019.

Contribuição 115299 - 17/06/2026

Seção 3.4, bullet sobre interesse público

Onde se lê: "for comprovado o interesse público e geral preponderante que justifique o acesso. A informação concedida, nesse caso, deve atender ao princípio da necessidade e poderá ser compartilhada com terceiros;"

Leia-se: "for comprovado o interesse público e geral preponderante que justifique o acesso. Nesse caso, o Termo de Responsabilidade deve ser mantido em formato digital simplificado, vinculando o requerente ao uso dos dados exclusivamente para a finalidade declarada;"

Justificativa: A dispensa cria lacuna de accountability. O Termo não restringe acesso — documenta finalidade e responsabiliza por uso indevido, compatibilizando LAI e LGPD (art. 6º, VIII).

Contribuição 115626 - 18/06/2026

Recomendo complementar o texto com referência expressa à Emenda Constitucional nº 115/2022, que elevou a proteção de dados pessoais à condição de direito fundamental autônomo (art. 5º, LXXIX, da Constituição Federal), reforçando que a tutela das informações pessoais previstas no art. 31 da Lei nº 12.527/2011 (LAI) deve ser interpretada à luz desse novo status constitucional. Também é pertinente destacar que a restrição de acesso a informações pessoais exige motivação individualizada, observando os princípios da proporcionalidade, razoabilidade e da máxima divulgação, previstos nos arts. 3º e 31 da LAI, bem como o dever de motivação estabelecido pelo art. 50 da Lei nº 9.784/1999, sendo vedadas negativas genéricas ou fundamentadas exclusivamente na invocação abstrata da LGPD. Convém, ainda, incorporar referência aos princípios da finalidade, necessidade, adequação e responsabilização previstos no art. 6º da Lei nº 13.709/2018 (LGPD).

Contribuição 115793 - 19/06/2026

Contribuições em nome da [REDACTED]

A [REDACTED] concorda com a distinção entre dado pessoal em sentido amplo, nos termos da LGPD, e informação pessoal protegida pela LAI, relacionada à intimidade, vida privada, honra e imagem. Essa diferenciação é importante para evitar o uso indevido da LGPD como barreira automática à transparência.

Contudo, recomenda-se que o Guia explicita que dados pessoais de representantes, sócios, empregados, responsáveis técnicos, procuradores, consultores ou prepostos de empresas

privadas não devem ser tratados, de forma automática, como dados de interesse público irrestrito. A existência de vínculo entre uma empresa e o Poder Público não elimina a necessidade de proteção dos dados pessoais de indivíduos vinculados à pessoa jurídica.

Contribuição 115794 - 19/06/2026

Em processos administrativos, contratações, convênios, termos de cooperação, procedimentos fiscalizatórios e interações regulatórias, é comum que documentos contenham assinaturas, documentos de identificação, endereços pessoais, telefones, e-mails pessoais, procurações, currículos, informações profissionais, dados bancários e outros pessoais. A publicidade do ato adm. pode ser preservada sem que haja exposição excessiva desses dados.

Sugestão de inclusão:

“A publicidade de atos administrativos envolvendo pessoas jurídicas de direito privado não implica, por si só, autorização para divulgação irrestrita de dados pessoais de sócios, administradores, empregados, representantes legais, responsáveis técnicos, procuradores ou terceiros vinculados à empresa. Sempre que possível, devem ser preservadas as informações necessárias ao controle social do ato, com supressão, descaracterização ou restrição de dados pessoais excessivos ou desvinculados da finalidade pública da divulgação.”

Contribuição 115933 - 19/06/2026

Sugestões da

Proposta de aprimoramento: explicitar a distinção entre pedidos de acesso à informação, formulados com fundamento na LAI, e demandas típicas de atendimento ao usuário, consumidor ou titular de dados pessoais, as quais possuem canais próprios de tratamento. Recomenda-se, ainda, a inclusão de exemplos objetivos de situações que não se enquadram no escopo da LAI.

Fundamentação: Essa diferenciação tende a ampliar a segurança jurídica, qualificar a orientação prestada ao cidadão e evitar a utilização inadequada da LAI para reclamações, regularizações cadastrais ou contratuais, solicitações operacionais, exercício de direitos de titular previstos na LGPD ou tratamento de casos individuais, hipóteses que devem ser direcionadas aos canais próprios, como SAC, ouvidoria, encarregado pelo tratamento de dados pessoais ou serviços específicos disponibilizados pela entidade.

Contribuição 115952 - 19/06/2026

Contribuições

Capítulo 3 — Proteção de dados pessoais prevista na LAI

Sugerimos a inclusão de um box específico sobre dados de saúde, reconhecendo que: (i) dados de saúde são dados sensíveis (art. 5º, II, e art. 11 da LGPD) e estão abarcados pela proteção da intimidade (art. 31 da LAI); (ii) prontuários e registros assistenciais sujeitam-se a sigilo profissional, que é sigilo legal preservado pelo art. 22 da LAI; e (iii) quando a identificação individual não for indispensável ao interesse público, deve-se preferir a divulgação agregada, anonimizada ou pseudonimizada.

Quanto à pesquisa (item 3.3, alínea “d”), apoiamos o entendimento da ANPD de que a anonimização não é condição para o compartilhamento, mas sugerimos ressalva sobre o risco de reidentificação em bases clínicas, genômicas, biométricas, de doenças raras ou de alta granularidade, com remissão à governança ética da pesquisa (CEP/CONEP).

Contribuição 115955 - 19/06/2026

Contribuições

vide item 3 - documento anexo

Contribuição 116121 - 20/06/2026

Sugerimos que o guia esclareça que o acesso aos próprios dados pessoais é um dos direitos previstos pela LGPD, que deve ser assegurado pelos agentes de tratamento. Nesse contexto, a orientação deve ser no sentido de direcionar o exercício do direito ao canal específico na instituição/órgão, no qual seja disponibilizado também o exercício dos demais direitos previstos na LGPD.

Contribuição 116136 - 20/06/2026

Em anexo, segue contribuição a respeito do item 3.1, detalhando problemas no quadro intitulado "IMPORTANTE" e no conceito de Intimidade. Há, também, sugestão quanto ao item 3.2, tendo em vista a necessidade de harmonização na forma de entrega de dados pessoais, quando solicitado pelo titular. Por fim, há uma exposição sobre o tópico da letra "D" (Estatísticas e Pesquisas), cujo conteúdo me pareceu não menos que desastroso.

Contribuição 116250 - 21/06/2026

Inclusão: complementar a tabela resumo do Guia com disposição expressa sobre o alcance da LAI às entidades privadas sem fins lucrativos (art. 2º da LAI): "Alcance da lei: todas as órgãos e entidades do poder público e, no que couber, as entidades privadas sem fins lucrativos que recebam recursos públicos, hipótese em que a publicidade se restringe à parcela dos recursos públicos recebidos e à sua destinação (art. 2º da LAI)."

Justificativa: refletir de forma integral o dispositivo previsto no art. 2º, parágrafo único, da LAI. Haja vista que a legislação também se aplica a entidades privadas sem fins lucrativos que executam ações de interesse público, como é o caso da RNP, a explicitação desse limite diretamente na tabela resumo do Guia confere maior clareza e precisão à aplicabilidade da Lei, auxiliando de forma mais didática tanto os cidadãos requerentes quanto os gestores dessas instituições.

Contribuição 116251 - 21/06/2026

Inclusão: acrescentar ao final da alínea "d" parágrafo que firme a presunção de interesse público para o tratamento de dados, sem consentimento, por órgãos de pesquisa:

"Presume-se atendido o requisito de evidente interesse público ou geral quando a demanda for formulada por órgão de pesquisa (art. 5º, XVIII, da LGPD) e a finalidade for pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico."

Justificativa: a LAI e a LGPD autorizam o tratamento e o compartilhamento de dados pessoais para fins de pesquisa independentemente do consentimento do titular, desde que presente o evidente interesse público ou geral. Na prática, porém, a exigência de que seja avaliado subjetivamente o mérito e o interesse público de cada projeto pode gerar insegurança jurídica: na dúvida sobre se o requisito está atendido, o gestor tende a exigir o consentimento, muitas vezes inviável em bases de pesquisa, ou simplesmente a negar o acesso, paralisando a pesquisa científica. ++

Contribuição 116252 - 21/06/2026

'++ A fixação de uma presunção de interesse público para as demandas de órgãos de pesquisa esclarece que, nessas hipóteses, a dispensa de consentimento já decorre da lei, deslocando o foco da análise do julgamento subjetivo sobre a relevância do estudo para a verificação da regularidade institucional.

Contribuição 123731 - 22/07/2026

O item "d" acerta ao afastar a anonimização/pseudonimização como condição técnica obrigatória para pesquisa (alinhado ao entendimento da ANPD).

Seria interessante, porém, que o Guia esclareça o tratamento aplicável quando a "pessoa jurídica de direito privado sem fins lucrativos" (art. 5º, XVIII, LGPD) atua em parceria com empresa privada com fins lucrativos no mesmo projeto de pesquisa (arranjo comum em estudos com financiamento privado). Nesses casos, é recorrente a dúvida sobre até que ponto os dados podem circular dentro do consórcio de pesquisa sem descaracterizar a hipótese legal aplicada, e se o Termo de Responsabilidade deve ser assinado por todos os integrantes do consórcio ou apenas pela entidade de pesquisa formalmente demandante.

Contribuição 124154 - 23/07/2026

Segue a contribuição da [REDACTED] para o terceiro item, para colaborar a visão de uma empresa estatal que atua em ambiente concorrencial, considerando as peculiaridades das sociedades de economia mista que lidam com informações estratégicas, negociais e comerciais, além de dados funcionais.

Pág. 13: "Seção 3.2 Acesso pelo titular à própria informação pessoal"

A fim de evitar controvérsias e orientar melhor os titulares dos dados, sugere-se incluir orientação expressa para que a solicitação de documentos pessoais, com base no inciso II, do art. 18 da LGPD, seja realizada por meio dos canais da LAI.

Contribuição 124371 - 24/07/2026

Segue em anexo contribuição da [REDACTED] sobre o tema

Contribuição 124391 - 24/07/2026

A Softex apresenta contribuições técnicas ao Capítulo 3 do Guia de Transparência e Proteção de Dados Pessoais, fundamentadas em evidências, dados e boas práticas internacionais. As sugestões buscam aprimorar o texto-base, tornando suas orientações mais claras, objetivas, previsíveis e adequadas aos diferentes contextos da Administração Pública relacionados ao tratamento e à divulgação de informações.

Contribuição 124449 - 24/07/2026

Devido à extensão das contribuições, a [REDACTED] encaminharam-nas ao e-mail dasai@cgu.gov.br em 24/07, por meio do endereço eletrônico [REDACTED]

Contribuição 112269 - 12/06/2026

LGPD é uma farsa, é política feita apenas para punir empresas, quando o principal vazador

de dados pessoais é o próprio Estado, e contra o Estado nada acontece, ninguém nunca é responsabilizado pelo vazamento de dados feito pelo Estado! Empresas devem sim ser responsabilizadas e ser punidas pelo vazamento de dados das pessoas, mas o Estado tb deveria, não só ser responsabilizado, como tb ser punido com indenizações para os afetados, além de punir os responsáveis pelo vazamento de dados, sejam eles quais forem, tanto de pessoas q't de empresas!

Contribuição 113594 - 12/06/2026

A LGPD estabelece uma classificação jurídica dos dados, mas essa classificação não necessariamente reflete o risco tecnológico moderno.

Atualmente, um CPF ou nome completo pode servir como chave para agregação de informações oriundas de múltiplas fontes públicas e privadas, permitindo a construção de perfis altamente detalhados.

Ferramentas de inteligência artificial, sistemas de mineração de dados e técnicas de correlação automatizada ampliam significativamente esse risco.

Sugestão

Adicionar o conceito de dados de elevado potencial identificador são dados que, embora não classificados como sensíveis pela LGPD, permitem a identificação inequívoca do titular ou funcionam como elementos de conexão entre diferentes bases de dados, aumentando significativamente os riscos de reidentificação, perfilamento e fraude.

Exemplos:

Nome completo;

CPF;

endereço residencial.

Contribuição 114672 - 13/06/2026

Sugere-se a inclusão de diretriz expressa sobre os princípios de “Proteção de Dados desde a Concepção” (Privacy by Design) e “Proteção de Dados por Padrão” (Privacy by Default), previstos no Art. 25 do GDPR. Embora o Guia destaque a necessidade de observância dos princípios da LGPD e mencione medidas como anonimização e pseudonimização, recomenda-se reforçar que sistemas, processos, portais de transparência e procedimentos de atendimento à LAI sejam concebidos desde sua origem para minimizar a exposição de dados pessoais. Além disso, as configurações padrão devem privilegiar a divulgação apenas dos dados estritamente necessários ao atendimento da finalidade pública, reduzindo riscos aos titulares e fortalecendo os princípios da necessidade, segurança e responsabilização previstos na LGPD. Tal medida contribuirá para uma transparência mais segura, preventiva e alinhada às melhores práticas internacionais de governança de dados.

Contribuição 114745 - 14/06/2026

Contribuições em relação ao capítulo 2.

Contribuição 115256 - 17/06/2026

Importantíssimo constar dessa seção do Guia (2.2), de forma objetiva e expressa, os requisitos emanados do STF na ADI 6649) e ADPF 695 em relação ao compartilhamento de dados na Administração Pública. Se o que se pretende com o guia é orientar o uso adequado, essa seção não pode ser tão sintética. Importantíssimo que se esclareça a sociedade sobre o uso para finalidade diversa da inicial. Da forma apresentada no guia, especialmente no último parágrafo do tópico 2.1 e todo o tópico 2.3, parece que a orientação

é de que uma solicitação de acesso a dados pessoais dos beneficiários de um programa, por exemplo, com base na LAI deveria ser, por princípio atendido. A finalidade da transparência não é (e não deve ser) a inicial que ensejou o tratamento de dados pessoais pelo poder público, normalmente a finalidade está associada à prestação de um serviço público e individualizado, com prazo determinado (início da relação e término dessa relação).

Contribuição 115277 - 17/06/2026

Em relação à Seção 2.3. é preciso esclarecer que embora a LGPD não crie hipóteses de sigilo no âmbito da Administração Pública, ela estabelece objetivamente a forma como a Administração Pública deverá tratar os dados pessoais, inclusive em seção específica. Assim o tratamento estabelecido (Capítulo IV) dispõem um conjunto de condições a ser observado com impactos práticos em relação às decisões que devem ser observadas pela Administração no tratamento de dados pessoais, o que inclui difusão, acesso, distribuição, comunicação, como os princípios arrolados no Artigo 6º e os fundamentos dispostos no Artigo 2º. Por exemplo, e não esgotando as referências, o Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

Contribuição 115279 - 17/06/2026

Ainda como um Guia, especificamente orientado à Administração Pública, é necessário que se oriente mais claramente em relação ao Art. 26 da LGPD, pois a decisão do que publicar (inciso III do §1º desse artigo) é uma condição de exceção à vedação da administração pública compartilhar dados com a iniciativa privada. Portanto, a publicação de informação que não observa os requisitos estabelecidos em lei para proteção do dado pessoal, pode ensejar uma apropriação privada da informação que consta de bases públicas e que foram tratadas para uma finalidade específica, primária, e não a transparência como finalidade em relação à divulgação de informação pessoal (do contrário não haveria qualquer informação pessoal protegida).

Contribuição 115622 - 18/06/2026

Recomendo incluir referência expressa ao reconhecimento da proteção de dados pessoais como direito fundamental autônomo, conferido pela Emenda Constitucional nº 115/2022, que acrescentou o inciso LXXIX ao art. 5º da Constituição Federal, reforçando que a proteção da privacidade e dos dados pessoais constitui garantia constitucional independente, embora correlata ao direito à intimidade e à vida privada. Também é pertinente destacar que a interpretação e a aplicação da LGPD no setor público devem observar os princípios da Administração Pública previstos no art. 37 da Constituição Federal, especialmente os princípios da legalidade, publicidade, eficiência e impessoalidade, bem como os princípios da prevenção e da prevenção de danos decorrentes do tratamento inadequado de dados pessoais. Recomenda-se, ainda, mencionar os deveres de governança e boas práticas previstos nos arts. 46, 49 e 50 da LGPD, incluindo a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais

Contribuição 115791 - 19/06/2026

A [REDACTED] considera positiva a afirmação de que LAI e LGPD são normas compatíveis e complementares. No entanto, recomenda-se que o Guia esclareça com maior objetividade que a compatibilização entre transparência e proteção de dados deve observar, de forma

cumulativa, os princípios da finalidade, adequação, necessidade, segurança, prevenção, transparência e responsabilização.

É importante que o Guia evite uma interpretação excessivamente centrada na divulgação, sem incorporar de forma equivalente a lógica de governança do tratamento de dados. A divulgação de dados pessoais pela Administração Pública é também uma operação de tratamento e, portanto, deve estar submetida a critérios mínimos de necessidade, proporcionalidade, segurança e prestação de contas.

Contribuição 115792 - 19/06/2026

A [REDACTED] sugere que o Guia reforce que os órgãos públicos devem manter registros decisórios, critérios objetivos e mecanismos de controle interno para justificar a divulgação integral, a divulgação parcial ou a restrição de acesso. Isso é especialmente importante para reduzir decisões contraditórias entre órgãos públicos e evitar insegurança jurídica para cidadãos e empresas.

Sugestão de inclusão:

“A divulgação de dados pessoais pela Administração Pública, seja em transparência ativa ou em resposta a pedidos de acesso à informação, constitui operação de tratamento de dados pessoais e deve observar os princípios da LGPD, em especial finalidade, adequação, necessidade, segurança, prevenção e responsabilização. A decisão pela divulgação integral, divulgação parcial ou restrição de acesso deve ser motivada, registrada e compatível com a finalidade pública pretendida.”

Contribuição 115904 - 19/06/2026

Em atenção à comunicação acerca da abertura de consulta pública conjunta da CGU e da ANPD sobre o Guia de Transparência e Proteção de Dados Pessoais, informamos que realizamos análise técnica do documento.

De forma geral, o Guia apresenta importante avanço ao consolidar diretrizes para harmonização entre a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD), com destaque para o modelo de tomada de decisão baseado na ponderação entre transparência e proteção de dados.

Contudo ... vide arquivo em anexo.

Contribuição 115951 - 19/06/2026

Contribuições [REDACTED]

Capítulo 2 — Proteção de dados pessoais nos termos da LGPD

Apoiamos integralmente a afirmação de que a LGPD não cria hipóteses de sigilo, nem altera o rol de informações restritas. Sugerimos apenas reforçar, na parte final, que a complementaridade entre LAI e LGPD impõe, no tratamento para fins de transparência, a observância dos princípios da finalidade, necessidade, adequação, segurança e prestação de contas, o que é particularmente sensível quando há dados de saúde sob guarda pública ou compartilhados em parcerias.

Contribuição 116030 - 19/06/2026

Anexo em PDF a contribuição relacionada ao Tema nº 2, devido ao excesso de caracteres (3.104). Nela, sugiro maior destaque ao tópico da COLETA nos itens 2.1 e 2.2, com vistas a impedir a coleta excessiva e/ou abusiva de dados, orientando os órgãos e as entidades de governo a não coletarem dados que não sejam pertinentes à sua natureza pública.

Contribuição 116227 - 21/06/2026

Segue contribuição. Cumprimentos pelo trabalho e oportunidade.

Contribuição 116270 - 21/06/2026

Adicionar nessa seção destaque de que o § 3º do art. 7º da LGPD "reconhece a existência de dados pessoais públicos", o que reforça a separação do escopo da LAI e da LGPD, sendo a LAI a norma de regência sobre acesso a informações na Administração Pública.

Nesse sentido, cabe destacar previsão expressa no § 3º do art. 7º da LGPD da existência de dados pessoais públicos:

"Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

[...]

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização."

Contribuição 124153 - 23/07/2026

Segue a contribuição da [REDACTED] para o segundo item, para colaborar a visão de uma empresa estatal que atua em ambiente concorrencial, considerando as peculiaridades das sociedades de economia mista que lidam com informações estratégicas, negociais e comerciais, além de dados funcionais.

P'ág. 8: Item do princípio da Transparência ("acesso" aos dados pessoais)

Sugerimos utilizar o termo 'tratamento' no lugar de acesso, por ser mais amplo.

Contribuição 124448 - 24/07/2026

Devido à extensão das contribuições, a [REDACTED]

[REDACTED] encaminharam-nas ao e-mail dasai@cgu.gov.br em 24/07, por meio do endereço eletrônico [REDACTED]

Contribuição 111040 - 11/06/2026

Eu sou a favor da vigilância de órgãos de fiscalização no que se referem dados pessoais de pessoas.

Contribuição 112283 - 12/06/2026

Discordo do [REDACTED] o Estado não deve utilizar órgãos de fiscalização em dados pessoais, exceto em casos onde possa haver algum tipo de crime e seja necessário uma investigação da pessoa!

Contribuição 112865 - 12/06/2026

A fiscaliz dos bancos de dados dos brasileiros não deveria ficar a cargo do governo. O mais adequado seria a criação de uma comissão independente, composta pela OAB e por servidores de carreira do MPF, da ABIN e da PF — profissionais com expertise técnica e, sobretudo, com garantias institucionais que os blindam de pressões políticas. Nessa estrutura, os dados de agentes públicos e de seus familiares deveriam ter acesso restrito,

disponível apenas ao próprio órgão fiscalizador. Já as informações relativas a beneficiários de programas assistenciais do governo precisam ser transparentes e de acesso público, como forma de garantir controle social sobre o uso dos recursos. Deixar essa responsabilidade nas mãos do Exec representa um risco real. Num país marcado por disputas políticas acirradas, concentrar esse poder no governo de plantão abre espaço para uso seletivo e politizado das informações — algo incompatível com qualquer projeto sério de proteção de dados e de Estado Democrático de D

Contribuição 114748 - 14/06/2026

Contribuições em relação ao capítulo 5.

Contribuição 114836 - 15/06/2026

Discordo do entendimento de que dados pessoais de um servidor público federal possam ser divulgados abertamente como acontece hoje.

Qualquer tipo de dado que possa identificar uma pessoa, incluindo seu nome, função, etc., é dado pessoal e, portanto, deve estar protegido pela LGPD. O Estado tem acesso a estes dados pessoais e o dever de os guardar.

Quando vejo a proposta de que dados como nome, cargo e, inclusive, remuneração continuem sendo divulgados abertamente, como ocorre hoje, realmente me parece um retrocesso e totalmente oposto ao objetivo da LGPD. É inadmissível termos estes dados pessoais divulgados hoje no website do Governo Federal. E a proposta de continuar divulgando-os não faz o mínimo sentido se estivermos tratando a proteção de dados pessoais com seriedade. Existem mecanismos previstos para requisição de dados pessoais de agentes públicos, e podíamos explorar este tipo de abordagem. Divulgar dados pessoais com a bandeira da "Transparência" beira o insensato.

Contribuição 114866 - 15/06/2026

Contribuição em anexo.

Contribuição 114945 - 15/06/2026

3.1 Prazos e articulação com a LAI

O guia está confuso quanto aos prazos, especialmente na relação entre LAI e LGPD. Não fica claro quando se aplica o prazo da LAI ou se há alterações por análise de dados pessoais/sigilo.

Sugestão: incluir fluxograma ou exemplos práticos deixando essa diferenciação objetiva.

3.2 Uso do FalaBR (anexos)

Não está claro se documentos anexados via FalaBR são suficientes para instruir pedidos.

Sugestão: explicitar a validade dos anexos e eventuais exigências complementares.

3.3 Governança

O guia é positivo, mas a decisão não deveria ficar restrita a instâncias burocráticas.

Sugestão: prever participação multistakeholder (academia, sociedade civil, especialistas), aumentando legitimidade e qualidade das decisões.

Contribuição 115280 - 17/06/2026

A divulgação de registro de frequência com o detalhe do horário de entrada e saída do servidor refere-se a informação sobre rotina, deslocamentos ou localização habitual que

expõem o servidor a riscos de integridade física e também toda a sua família, não havendo respaldo na Lei para que essa informação seja disponibilizada. Afronta diretamente os princípios da Necessidade, Segurança e Prevenção da LGPD. O interesse público preponderante não prevalece quando a divulgação criar risco razoável e demonstrável à integridade física ou moral do servidor.

Sugere-se a restrição da divulgação pública de registros de frequência ao cumprimento da carga horária, sem detalhamento de horários específicos de entrada e saída.

Dessa forma, pedimos avaliar a modificação do quadro que trata de "Dados Pessoais de agentes públicos" (Seção 5), da seguinte forma:

Onde se lê: Registro de frequência;

Leia-se: Registro de frequência sem detalhamento de horários específicos de entrada e saída.

Contribuição 115301 - 17/06/2026

Capítulo 5, subseção de agentes públicos (novo item sobre teletrabalho)

Incluir: "No contexto do teletrabalho e do trabalho remoto, a publicidade deve recair sobre metas e resultados institucionais. São vedadas a divulgação de: endereço de IP residencial; telefone celular pessoal; informações de localização física do servidor em regime remoto; e dados da infraestrutura tecnológica privada utilizada em sua residência. O controle deve ser feito por indicadores agregados, sem exposição de dados da esfera privada do servidor."

Justificativa: O Guia já veda endereço e telefone pessoal (Cap. 5). O IP residencial e a infraestrutura doméstica têm a mesma natureza de "vida privada" (LAI, art. 31, §1º). O Princípio da Necessidade (LGPD, art. 6º, III) impede sua exposição quando o controle é atingível por indicadores institucionais.

Contribuição 115310 - 17/06/2026

A seção 5 precisa de uma revisão cuidadosa. Apresentar informações contraditórias ou em desacordo com outras da própria seção e da seção 4. De maneira geral, ambas as seções parecem desconsiderar um ponto bastante importante previsto em lei. O caráter relativo das medidas de proteção dos dados pessoais, considerando as condições tecnológicas (conhecimento, conhecimento aplicação e recursos computacionais) e a necessidade de que as medidas sejam sistematicamente avaliadas e reavaliadas. Cria-se, aqui, uma expectativa de preservação de uma condição anterior frente novas situações. A própria questão da divulgação dos rendimentos do servidores público, com base na justificativa do controle social, precisa ser reavaliada quanto à forma.

Contribuição 115312 - 17/06/2026

Apresento minhas considerações para contribuir com o aprimoramento técnico do Guia, especialmente quanto à distinção entre LAI, LGPD, sigilo e proteção de dados pessoais. Sugiro reforçar que dado pessoal não é, por si só, informação sigilosa, e que a LGPD não cria hipótese autônoma de restrição de acesso. A LAI deve permanecer como norma de regência dos pedidos de informação, cabendo à LGPD orientar o tratamento responsável, proporcional e seguro dos dados, sempre privilegiando, quando possível, o acesso parcial por meio de tarjamento, anonimização, certidão, extrato ou versão pública.

Segue anexo

Contribuição 115313 - 17/06/2026

Diferentes seções e referências utilizadas, por exemplo, trazem orientações diferentes para,

por exemplo, a "divulgação do nome da pessoa". Para beneficiários de programas sociais "pode ser divulgado", mas se esse beneficiários forem estudantes, a "regra" é que o nome é uma informação pública. A própria referência feita à decisão do STF no MS 3.902/SP aponta que dados como remuneração, cargos, funções e órgão de lotação constituem informações de interesse coletivo ou geral e não violam a intimidade ou a vida privada, por estarem diretamente vinculados ao exercício da função pública. Portanto poderia compor uma divulgação, por exemplo, associada ao número da matrícula, minimizando a exposição de dados pessoais e, ainda assim, assegurando o controle social. Vale destacar que, no conjunto, as decisões diferentes pode resultar em divulgações que podem ser combinadas e integradas, reduzindo a efetividade da decisão de um órgão. Há a necessidade de um tratamento mais profundo da questão.

Contribuição 115323 - 17/06/2026

Importante considerar que o CPF é um documento público e, portanto, acessível em qualquer relação administrativa/contratual do indivíduo com um terceiro (seja agente público ou privado). De posse das informações pessoais e dados públicos disponíveis, qualquer contratante, empregador, interessado, perseguidor, empresa de composição de perfis comportamentais e marketing, podem compor bases que além poder ser enriquecidas em decorrências de vulnerabilidades, mas também podem ser exclusivamente construídas, mantidas e enriquecidas a partir da divulgação pública, orientada a um "controle social", que não observa o que a lei dispõe sobre a necessidade de considerar meios técnicos razoáveis disponíveis no momento de tratamento, que podem alimentar estratégias não apenas de estigmatização, mas concretas de segregação, discriminação, predileção, etc.

Contribuição 115628 - 18/06/2026

Recomendo complementar o capítulo com referências mais explícitas aos fundamentos constitucionais da publicidade, moralidade, eficiência e accountability previstos no art. 37 da Constituição Federal, reforçando que a divulgação de dados pessoais relacionados ao exercício de funções públicas, à aplicação de recursos públicos e à execução de políticas públicas decorre da prevalência do interesse coletivo e da necessidade de assegurar o controle social. Também é recomendável mencionar a Emenda Constitucional nº 115/2022, que conferiu status de direito fundamental autônomo à proteção de dados pessoais (art. 5º, LXXIX), evidenciando que a publicidade de dados pessoais deve ser orientada pela harmonização entre direitos fundamentais e não por uma lógica de prevalência automática da privacidade ou da transparência. Convém, ainda, associar os entendimentos práticos apresentados aos princípios da finalidade, necessidade, adequação e minimização previstos no art. 6º da Lei nº 13.709/2018 (LGPD).

Contribuição 115713 - 19/06/2026

Sugere-se que o Guia de Transparência e Proteção de Dados Pessoais inclua orientações específicas para o tratamento, compartilhamento e divulgação de dados pessoais sensíveis em saúde, considerando os desafios decorrentes da digitalização dos serviços públicos e da interoperabilidade entre sistemas. Recomenda-se a definição de critérios mais claros para anonimização, avaliação de riscos de reidentificação e adoção de salvaguardas proporcionais à sensibilidade dos dados, especialmente em atividades de pesquisa, vigilância em saúde e uso de tecnologias digitais. Além disso, é importante que o Guia incorpore uma perspectiva de equidade, prevenindo a exposição, discriminação ou estigmatização de indivíduos e grupos vulnerabilizados, de forma a conciliar adequadamente os princípios da transparência pública, da proteção de dados pessoais e dos direitos fundamentais.

Contribuição 115763 - 19/06/2026

Sugiro que o guia aborde a boa prática de descaracterizar a matrícula funcional do servidor, de forma semelhante ao CPF, pois a sua publicização pode ensejar riscos aos servidores, especialmente financeiros, pois ao dispor do seu nome e de sua matrícula, é possível, por exemplo, fraudar contratação de empréstimos consignados em seu nome, sem o seu aval. A tarja parcial da matrícula como ocorre no Portal Transparência do Governo Federal parece a solução adequada, uma vez que permite a identificação de eventuais homônimos, mas protege os titulares dos cargos de eventuais fraudes e situações correlatas. Tal situação já foi objeto de jurisprudência administrativa da CGU, nos pareceres nº 21900.000470/2015-94 e 23480.009656/2014-4.

Contribuição 115808 - 19/06/2026

Com relação a transparência de PADs quando concluídos, verificar a contradição com a PORTARIA NORMATIVA CGU Nº 27, DE 11 DE OUTUBRO DE 2022 que limita o acesso em algumas situações, aí cabe uma pergunta, pode uma norma de um órgão limitar a Lei de Acesso à Informação?

A norma da CGU fala em tratamento do dados a partir do artigo 113 e situações que não permitirá o acesso, verifiquem se há contradições ao guia. Ou seja, não há acesso irrestrito ao PAD, deve ser pontuado no Guia a previsão do normativo para negativas de acesso.

Contribuição 115819 - 19/06/2026

Contribuição em nome da [REDACTED]

Em virtude da limitação de caracteres, encaminhamos arquivo anexo com nossas contribuições sobre o Capítulo 5: Entendimentos sobre a publicidade de dados pessoais.

Contribuição 115972 - 19/06/2026

Sugiro que avaliem a inclusão de orientação específica sobre o tratamento da rubrica em documentos, dado tratado expressamente pelo Parecer CGU nº 107/2015.

A rubrica tem relevância prática na gestão documental pública e não é recomendável que seu tratamento seja inferido apenas por analogia com a assinatura manuscrita.

Contribuição 115813 - 19/06/2026

Contribuição em nome da [REDACTED]

A [REDACTED] recomenda atenção especial aos trechos do Guia que tratam de licitações, contratos, fornecedores, registros de acesso a prédios públicos, processos fiscalizatórios, auditorias e atividades regulatórias. Esses temas afetam diretamente a relação entre Administração Pública e setor produtivo.

No caso de fornecedores e contratados, é legítima a divulgação de informações necessárias ao controle social, como razão social, CNPJ, objeto contratado, valores globais, vigência, órgão contratante, situação contratual e sanções administrativas aplicadas, quando houver. Contudo, não devem ser divulgados de forma irrestrita dados pessoais de representantes, empregados, responsáveis técnicos ou terceiros, nem informações empresariais protegidas por sigilo legal, segredo industrial, propriedade intelectual ou legítimo interesse concorrencial.

Contribuição 115814 - 19/06/2026

Contribuição em nome da [REDACTED]

A divulgação de documentos empresariais deve observar análise concreta e proporcional, especialmente quando envolver metodologias proprietárias, projetos técnicos sensíveis, informações de segurança, dados de fornecedores, documentos de identificação, dados bancários, contatos pessoais, assinaturas manuscritas e informações comerciais que possam gerar risco de fraude, prejuízo concorrencial ou exposição indevida.

A [REDACTED] sugere que o Guia estabeleça exemplos mais claros de divulgação parcial em contratos e processos empresariais, com indicação de quais dados tendem a ser públicos, quais devem ser avaliados para descaracterização e quais podem justificar restrição de acesso, conforme o caso concreto.

Contribuição 115815 - 19/06/2026

Devido ao tamanho disponibilizado nesse campo às contribuições apresentadas seguem no arquivo PDF anexo.

Contribuição 115816 - 19/06/2026

Contribuição em nome da [REDACTED]

Sugestão de inclusão:

“Em processos de contratação pública, fiscalização, regulação e controle, a publicidade deve assegurar o controle social sobre o uso de recursos públicos e a atuação administrativa, sem acarretar exposição desnecessária de dados pessoais ou de informações empresariais protegidas. Como regra, podem ser divulgados razão social, CNPJ, objeto, valor global, vigência, órgão contratante, situação contratual e sanções administrativas. Devem ser avaliados para restrição, descaracterização ou divulgação parcial dados pessoais de representantes, empregados, responsáveis técnicos, procuradores e terceiros, bem como informações protegidas por segredo industrial, propriedade intelectual, sigilo comercial, segurança institucional ou risco concorrencial.”

Contribuição 115817 - 19/06/2026

[REDACTED]

Sugestão de novo item: Dados pessoais e informações empresariais em documentos de pessoas jurídicas privadas

A [REDACTED] recomenda a inclusão de item específico no Guia dedicado a documentos empresariais custodiados pelo Poder Público. A ausência de tratamento próprio para esse tema pode gerar insegurança jurídica, especialmente porque empresas privadas são frequentemente obrigadas a fornecer informações detalhadas à Administração Pública em razão de contratos, fiscalizações, políticas públicas, programas de incentivo, regulação setorial ou exigências legais.

Esse novo item poderia consolidar orientações sobre publicidade, divulgação parcial, proteção de dados pessoais de representantes e empregados, preservação de segredo industrial, tratamento de informações concorrencialmente relevantes e aplicação de técnicas como tarja, extração de certidões, elaboração de versões públicas de documentos, descaracterização de CPF, ocultação de assinaturas e supressão de dados excessivos.

Contribuição 115921 - 19/06/2026

Sugerimos a inclusão de um bloco específico dedicado às atividades e aos tipos documentais característicos das Casas Legislativas de todas as esferas. Embora existam diversas

orientações aplicáveis a documentos comuns tanto ao Poder Executivo quanto ao Legislativo, ainda são escassas as referências voltadas a documentos próprios da atividade legislativa. Encaminhamos um documento contendo sugestões de definições e classificações. Ressaltamos, contudo, que o mais importante é a existência de orientações claras e tecnicamente fundamentadas, ainda que adotem entendimentos diferentes dos aqui sugeridos.

Contribuição 115962 - 19/06/2026

Contribuições

vide item 5 - documento anexo

Contribuição 115964 - 19/06/2026

Boa tarde a todos e todas.

Eu já consultei diversas leituras e opiniões sobre a possibilidade do Estado definir com precisão os limites entre o sigilo bancário privado e o sigilo bancário de contas públicas, ao meu ver inexistente. Se são contas públicas, em tese não poderiam possuir quaisquer restrições de acesso, sejam estas da União, dos estados, dos municípios ou mesmo de quaisquer órgãos, públicos ou privados, que estejam usando recursos públicos. Usou recurso público, automaticamente deveria cair o sigilo bancário. Embora o Governo Digital seja uma realidade e os níveis de transparência tenham inegavelmente avançado, e essa plataforma gov.br, com mais de 180 milhões de usuários, é uma prova desta transparência, a abertura em tempo real das contas públicas em todas as plataformas ainda parece distante. Por exemplo que os bancos públicos possibilitem nos Caixas Eletrônicos e em seus aplicativos de celulares, acesso a todas e quaisquer contas públicas. A tecnologia já permite isso.

Contribuição 115970 - 19/06/2026

Seria interessante a inclusão no Guia de orientação sobre as modalidades de assinatura eletrônica mais utilizadas em documentos administrativos, contribuindo para maior padronização no tratamento desses dados.

Além da assinatura manuscrita, seria útil que o Guia tratasse também de outras formas de assinatura, como a assinatura eletrônica por login e senha, a assinatura digital com certificado ICP-Brasil, a assinatura pelo gov.br e a assinatura com imagem digitalizada da assinatura física.

Contribuição 115973 - 19/06/2026

Sugiro que avaliem o aprimoramento da orientação sobre divulgação de e-mail funcional individualizado de agentes públicos.

O Guia menciona a possibilidade de não divulgação do e-mail individual quando houver canal institucional, mas seria útil esclarecer melhor o alcance dessa ressalva.

Indicar, de forma mais objetiva, o que pode ser considerado canal institucional de atendimento ao cidadão, como e-mails de área, caixas compartilhadas, sistemas eletrônicos ou formulários institucionais. A ausência de balizas claras pode gerar insegurança jurídica e aplicação inconsistente.

Contribuição 115975 - 19/06/2026

Em Sigilo Legal, especificar, por meio de exemplos, os documentos protegidos pela

legislação e incluir projeto de pesquisa na parte de Direitos Autorais.

Contribuição 116058 - 20/06/2026

Para adequada interpretação das disposições relativas à transparência administrativa e à proteção de dados pessoais, recomenda-se que a norma reconheça expressamente a diferença existente entre informações pessoais constantes de documentos acessíveis mediante consulta individualizada em processos administrativos e aquelas contidas em documentos submetidos à publicação oficial de ampla divulgação.

Contribuição 116068 - 20/06/2026

Sugere-se que a norma estabeleça, como regra geral, a publicidade de procurações, atos constitutivos, documentos de representação, termos de designação e demais documentos apresentados para comprovação da qualificação das partes, representantes legais e procuradores nos processos administrativos, ressalvadas apenas as hipóteses excepcionais de restrição de acesso previstas em lei ou devidamente fundamentadas. Da mesma forma, recomenda-se que a norma esclareça expressamente que a anonimização ou o mascaramento de dados de qualificação constantes desses documentos não constitui medida necessária de forma geral quando mantidos nos autos administrativos.

Contribuição 116122 - 20/06/2026

Sugerimos explicitar a incidência de sigilos legais aplicáveis a sociedades de economia mista e instituições financeiras públicas, como sigilo bancário, empresarial e concorrencial, destacando que restrições de acesso devem ser concretas, motivadas, proporcionais e juridicamente fundamentadas.

Contribuição 116120 - 20/06/2026

Os Encarregados de Dados e as estruturas de governança em proteção de dados das Cortes de Contas acompanham com atenção a elaboração do Guia de Transparência e Proteção de Dados Pessoais (CGU/ANPD, maio de 2026) e apresentam, por meio desta contribuição técnica conjunta, posição fundamentada sobre ponto específico da minuta que impacta diretamente a efetividade do controle externo e o exercício do controle social: a diretriz de descaracterização do Número de Inscrição no Cadastro de Pessoas Físicas (CPF) nas publicações de órgãos públicos, sem ressalva para as decisões e acórdãos proferidos pelas Cortes de Contas. São signatários desta contribuição o [REDACTED]

Contribuição 116123 - 20/06/2026

Sugerimos esclarecer como deve se dar o tratamento de pedidos reiterados, repetitivos ou usados como substituição a canais institucionais específicos, quando houver desvio de finalidade, sobrecarga administrativa ou inadequação ao regime de acesso à informação pública.

Contribuição 116124 - 20/06/2026

Sugere-se incluir no Guia que solicitações envolvendo dados pessoais de ex-funcionários de

instituições financeiras, especialmente informações trabalhistas, não devem ser tratadas indistintamente pelos canais gerais de acesso à informação, em razão da natureza sensível dessas informações e dos riscos associados ao seu tratamento inadequado. Tais demandas devem ser direcionadas a canal específico, adequado ao tratamento conforme a legislação e proteção de direitos. A diretriz segue a Súmula CMRI/CGU nº 01/2015 e garante transparência com proteção de dados, reduzindo riscos e reforçando segurança jurídica.

Contribuição 116143 - 21/06/2026

A [REDACTED] apresenta contribuições ao Guia de Transparência e Proteção de Dados Pessoais da CGU e da ANPD, reafirmando o entendimento de que a LGPD fortalece a transparência pública sem impor restrições indevidas ao acesso à informação. As sugestões concentram-se em três eixos principais: (i) integração do regime arquivístico à política de acesso à informação, com referência expressa à Resolução CONARQ nº 54/2023 para documentos em fase permanente; (ii) estabelecimento de diretrizes para governança algorítmica e uso de inteligência artificial em processos de triagem e tarjamento, com rastreabilidade, auditoria e supervisão humana; e (iii) reforço da proteção de dados de crianças e adolescentes como regra de privacidade por padrão, em consonância com a Lei nº 15.211/2025 (ECA Digital). As contribuições visam aprimorar a segurança jurídica, a transparência e a proteção de direitos fundamentais.

[REDACTED]

[REDACTED]

[REDACTED]

Contribuição 116164 - 21/06/2026

Inclusão de Glossário

O Guia reúne conceitos de dois regimes jurídicos distintos: LAI e LGPD, além de expressões técnicas de anonimização, gestão documental, transparência e análise de riscos. Sem um glossário, termos próximos podem ser interpretados como equivalentes.

Contribuição 116241 - 21/06/2026

Com relação ao tópico “Dados pessoais em listas de controle de acesso a prédios públicos”, não é clara a indicação de não divulgação de Foto (Capturada ou do documento). Trata-se da imagem apenas estática? O que se orienta quanto a imagens de câmera de segurança? Há alguns anos, correligionários de um ex-presidente da República foram acusados de invadir e depredar prédios públicos em Brasília. Poucas horas depois, imagens PÚBLICAS das câmeras de segurança estavam circulando em toda a mídia, junto com nome dos envolvidos. O que ocorreu nesse caso? Como as imagens PÚBLICAS foram parar em domínio público? Isso sem falar que, durante todo o tempo, havia um processo policial em andamento, investigando a invasão/depredação. Afinal, a imagem duma pessoa em prédio público, capturada pelas câmeras de segurança, é restrita ou não? Sob quais circunstâncias? Para quais finalidades?

Contribuição 116242 - 21/06/2026

No tópico “Dados de estudantes beneficiários de bolsas e ações afirmativas”, é importante citar, ainda que brevemente, que os beneficiários de bolsas não são apenas estudantes, mas também professores. Multiplicam-se nas universidades as iniciativas de pesquisa e extensão em que o responsável, sempre um acadêmico, recebe, é claro, verba pública. A transparência nesses casos, porém, fica restrita ao aluno que integra a iniciativa. Em

universidades, sejam federais ou privadas, a regra é esconder o máximo possível informações sobre valores recebidos pelo corpo docente e fazer parecer que são os discentes apenas que recebem bolsas.

Contribuição 116243 - 21/06/2026

A respeito da divulgação de “nomes dos estudantes beneficiários de ações afirmativas (cotas raciais ou sociais)”, há que se orientar órgãos e entidades quanto aos riscos decorrentes. Em certa universidade federal do estado do RJ, por exemplo, há cota para pessoas trans. Após classificadas, essas pessoas precisam comparecer à universidade para uma entrevista. Ocorre, porém, que a tal universidade divulga em seu site uma lista não apenas com os nomes das trans, mas também com a data, a hora e endereço em que elas devem comparecer à entrevista. Ora, essa divulgação expõe pessoas trans a riscos, uma vez que qualquer um tem acesso à informação de onde essa categoria discriminada estará, tendo possibilidade de organizar e levar a cabo algum ato de violência. Como dito, é preciso cautela do poder público. Este trecho, no entanto, parece genérico demais: a divulgação deve ser do nome apenas? Porque não é o que se verifica na prática.

Contribuição 116246 - 21/06/2026

A presente contribuição de [REDACTED] apresenta sugestões de aprimoramento ao Guia de Transparência e Proteção de Dados Pessoais elaborado pela CGU e pela ANPD, com foco na aplicação das regras de acesso à informação e proteção de dados no contexto das parcerias entre a Administração Pública e as organizações da sociedade civil (OSCs). O documento identifica lacunas no tratamento dessas relações pelo Guia, propõe parâmetros para a divulgação e proteção de dados pessoais envolvidos na execução de parcerias regidas pelo Marco Regulatório das Organizações da Sociedade Civil (Lei nº 13.019/2014), analisa referências normativas nacionais e internacionais e apresenta propostas concretas de ajustes redacionais, incluindo a criação de seção específica sobre OSCs e aperfeiçoamentos no roteiro decisório do Guia. Segue anexa a contribuição detalhada para apreciação. Ficamos à disposição para aprofundar quaisquer dos temas em audiências públicas e esperamos apoiar na consolidação do Guia.

Contribuição 116249 - 21/06/2026

Apresento a seguir as minhas sugestões de contribuições à Consulta Pública sobre o Guia de Transparência e Proteção de Dados Pessoais, desenvolvida pela Agência Nacional de Proteção de Dados (ANPD) e pela Controladoria-Geral da União (CGU). [REDACTED]

[REDACTED]

Essa contribuição busca aprofundar o desenvolvimento de políticas de acesso respeitando os direitos fundamentais de acesso à informação e de proteção de dados, no contexto dos arquivos, especialmente os arquivos públicos. Ademais, respeitando aqui os princípios de transparência, sobretudo outros de governança, os princípios de integridade, de responsabilidade e prestação de contas.

Contribuição 116256 - 21/06/2026

Sugestão: reformular a orientação de divulgação nominal de beneficiários de ações

afirmativas para priorizar dados agregados: “A transparência das ações afirmativas é assegurada preferencialmente mediante a divulgação de dados agregados e estatísticos que demonstrem o cumprimento dos critérios e da reserva de vagas, sem identificação nominal individualizada da condição racial.”

Justificativa: recomendamos a alteração para alinhar a orientação ao regime legal de proteção de dados pessoais sensíveis (art. 11 da LGPD). Vincular publicamente o nome de um estudante à cota racial pode revelar, por inferência, sua origem racial ou étnica. O próprio texto do Guia alerta, na mesma seção, sobre o risco de estigmatização decorrente da exposição desse tipo de dado. Recomendamos, portanto, que seja dada preferência a dados agregados, garantindo o controle e a comprovação do preenchimento das vagas, sem expor desnecessariamente a identidade e a privacidade dos estudantes.

Contribuição 121256 - 04/07/2026

Contribuição ao Guia de Transparência e Proteção de Dados Pessoais — Acesso à Informação. Sugestão técnica para vedação de formatos que possibilitem a raspagem automatizada (scraping) de dados remuneratórios de agentes públicos.

Contribuição 122197 - 10/07/2026

Sugere-se aperfeiçoar o item para estabelecer que a divulgação de currículos de agentes públicos seja realizada de forma padronizada, atualizada e verificável, contendo formação acadêmica, experiência profissional, vínculo institucional, função exercida e data da última atualização. A publicidade deve se limitar às informações pertinentes à avaliação da capacidade técnica e da adequação ao cargo, excluindo dados pessoais sem relação com a função pública, como endereço, telefone, documentos de identificação e informações familiares. Recomenda-se, ainda, indicar a fonte de comprovação dos títulos, prever correção de informações inexatas e adotar formato acessível e pesquisável. A medida fortalece o controle social, a integridade das nomeações e a confiança pública, sem afastar os princípios da necessidade, proporcionalidade e minimização previstos na LGPD.

Contribuição 122678 - 14/07/2026

CONTRIBUIÇÕES PARA O GUIA ORIENTATIVO: LAI E LGPD NA ADMINISTRAÇÃO PÚBLICA

Apresento sugestões de aprimoramento ao texto do Guia Orientativo, com foco na pacificação de diretrizes sobre transparência ativa, gestão de pessoas e harmonização entre a LAI (Lei nº 12.527/2011) e a LGPD (Lei nº 13.709/2018):

Contribuição 122681 - 14/07/2026

CONTRIBUIÇÕES TÉCNICAS AO GUIA ORIENTATIVO: LAI E LGPD NA ADMINISTRAÇÃO PÚBLICA

Apresentam-se sugestões de aprimoramento ao texto do Guia Orientativo promovido pela Controladoria-Geral da União (CGU) e pela Autoridade Nacional de Proteção de Dados (ANPD), com foco no aperfeiçoamento da governança pública, inovação tecnológica e proteção de direitos fundamentais:

Contribuição 122688 - 14/07/2026

CONTRIBUIÇÕES TÉCNICAS AO GUIA ORIENTATIVO: LAI E LGPD NA ADMINISTRAÇÃO

PÚBLICA

Apresentam-se sugestões de aprimoramento ao texto do Guia Orientativo promovido pela Controladoria-Geral da União (CGU) e pela Autoridade Nacional de Proteção de Dados (ANPD), com foco no aperfeiçoamento da governança pública, inovação tecnológica e proteção de direitos fundamentais: Recomenda-se incluir no Guia a orientação para que os órgãos públicos e instituições de ensino/pesquisa adotem ambientes virtuais controlados de amostragem (Data Cleanrooms) e protocolos padronizados de pseudonimização. Essa medida assegura a utilidade estatística dos dados acadêmicos para o avanço da ciência e da inovação pública, garantindo pleno alinhamento aos princípios da minimização, segurança e finalidade previstos no art. 6º da LGPD.

Contribuição 123498 - 21/07/2026

Teste

Contribuição 123733 - 22/07/2026

Contribuição da [REDACTED]

Recomenda-se que o Guia esclareça a aplicação do padrão de descaracterização do CPF (***.999.999-**) especificamente em contextos de dados estruturados e sistemas de consulta (bases abertas, portais de transparência com filtros e exportação), e não apenas em documentos e certidões individuais.

Em bases estruturadas, a descaracterização parcial pode não impedir a reidentificação por cruzamento com outras bases públicas (nome + lotação + órgão, por exemplo), o que é um risco distinto do risco de exposição de um documento isolado.

Contribuição 124163 - 23/07/2026

Segue a contribuição da [REDACTED] para o quinto item, para colaborar a visão de uma empresa estatal que atua em ambiente concorrencial, considerando as peculiaridades das sociedades de economia mista que lidam com informações estratégicas, negociais e comerciais, além de dados funcionais.

Contribuição 124394 - 24/07/2026

A [REDACTED] apresenta contribuições técnicas ao Capítulo 5 do Guia de Transparência e Proteção de Dados Pessoais, fundamentadas em evidências, dados e boas práticas internacionais. As sugestões buscam aprimorar o texto-base, tornando suas orientações mais claras, objetivas, previsíveis e adequadas aos diferentes contextos da Administração Pública relacionados ao tratamento e à divulgação de informações.

Contribuição 124451 - 24/07/2026

Devido à extensão das contribuições, [REDACTED]

encaminharam-nas ao e-mail dasai@cgu.gov.br em 24/07, por meio do endereço eletrônico [REDACTED].