

GUIA DE TRANSPARÊNCIA E PROTEÇÃO DE DADOS PESSOAIS

NO ÂMBITO DO PODER EXECUTIVO FEDERAL

Controladoria-Geral da União (CGU)
Agência Nacional de Proteção de Dados (ANPD)
Novembro de 2026

CONTROLADORIA-GERAL DA UNIÃO - CGU
Setor de Autarquias Sul (SAUS),
Quadra 5, Bloco A
Ed. Multibrasil, Brasília/DF - CEP: 70.070-050
cgu@cgu.gov.br

VINICIUS MARQUES DE CARVALHO
Ministro da Controladoria-Geral da União

EVELINE MARTINS BRITO
Secretária-Executiva

RONALD DA SILVA BALBE
Secretário Federal de Controle Interno

FERNANDA ALVARES DA ROCHA
Corregedora-Geral da União

VALDIRENE PAES DE MEDEIROS
Ouvidora-Geral da União

MARCELO PONTES VIANNA
Secretário de Integridade Privada

PATRICIA ALVARES DE AZEVEDO OLIVEIRA
Secretária de Integridade Pública

LIVIA OLIVEIRA SOBOTA
Secretária Nacional de Transparência e Acesso à Informação

EQUIPE TÉCNICA RESPONSÁVEL
CIBELLE CESAR DO AMARAL BRASIL
Diretora de Articulação, Supervisão e Monitoramento do Acesso à Informação

TAMARA FIGUEIROA BAKUZIS;
CAMILA AUGUSTO MARTINS ALVES.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS
Setor Comercial Norte (SCN),
Quadra 6, Conjunto A
Edifício Venâncio 3000, Bloco A, 9° andar
Brasília - DF / CEP: 70716-900

IAGÊ ZENDRON MIOLA
Diretor-Presidente Interino

LORENA GIUBERTI COUTINHO
Diretora

MIRIAM WIMMER
Diretora

EQUIPE TÉCNICA RESPONSÁVEL
LUCAS BORGES DE CARVALHO
Superintendente de Regulação

CAROLINE CHUCRE KAPPEL
Coordenadora-Geral de Governança e Regulação Setorial

CRISTIANE MIRANDA ARAÚJO
Coordenadora de Padrões e Conformidade

BRUNA ARMONAS COLOMBO
Coordenadora de Governança e Regulação Setorial

ANA KARLA DE SOUSA SEVERO;
DÉBORA DE ALBUQUERQUE E SILVA;
RENATA PIRES DE ALMEIDA SILVA;
PAULO CESAR DOS SANTOS.

Copyright (c) 2026 Controladoria-Geral da União e Agência Nacional de Proteção de Dados.
Permitida a reprodução desta obra, de forma parcial ou total, sem fins lucrativos, desde que citada a fonte ou endereço da internet no qual pode ser acessada integralmente em sua versão digital.

CONTEÚDO

Contextualização 4

1. Direito de acesso à informação e seus limites 6

1.1. A transparência é a regra e o sigilo é a exceção 6

1.2. Exceções à transparência 6

2. Direito à proteção de dados pessoais na LGPD 11

2.1. Princípios e hipóteses legais aplicáveis ao tratamento de dados pessoais pelo Poder Público 12

2.2. Regime jurídico do tratamento de dados pessoais pela Administração Pública 14

2.3. LGPD e LAI: compatibilidade e complementaridade 14

3. A proteção das informações relativas à intimidade, vida privada, honra e imagem das pessoas prevista na LAI 16

3.1. Informação pessoal de acesso restrito 17

3.2. Acesso pelo titular à própria informação pessoal 20

3.3. Acesso por terceiros à informação pessoal relativa à intimidade, vida privada, honra e imagem 21

3.4. Responsabilidades vinculadas ao uso de informações pessoais de terceiros 27

4. Conciliando a transparência pública e a intimidade, a vida privada, a imagem e a honra das pessoas 29

4.1. Análise da possibilidade de divulgação de informação pessoal 29

4.2. Identificando o evidente interesse público 31

4.3. Transparência por desenho 44

5. Entendimentos sobre a publicidade de dados pessoais 47

Divulgação de CPF em resposta a pedidos de acesso à informação ou para cumprimento de obrigações de transparência ativa 47

Dados pessoais de agentes públicos 48

Dados pessoais constantes de processos seletivos e dados de formação e experiência de servidores e empregados públicos 50

Dados pessoais em processos administrativos disciplinares 51

Dados pessoais em listas de controle de acesso a prédios públicos 53

Dados pessoais em processos licitatórios e contratos administrativos 55

Dados pessoais em processos administrativos de auditoria, fiscalização, controle, licenciamentos e outorgas 57

Dados pessoais sobre beneficiários de programas sociais 58

Dados de estudantes beneficiários de bolsas e ações afirmativas 60

CONTEXTUALIZAÇÃO

O acesso à informação é reconhecido como direito fundamental na Constituição Federal. Este direito é essencial para a consolidação da democracia e para a proteção de direitos humanos. O fortalecimento da transparência na Administração Pública brasileira tem se intensificado nas últimas décadas, acompanhando o amadurecimento das instituições democráticas e a consolidação de uma cultura de controle social.

A promulgação da Lei de Acesso à Informação (Lei nº 12.527/2011 – LAI), em 2011, representou um marco nesse processo de fortalecimento da transparência, ao estabelecer regras e procedimentos claros para o acesso e a divulgação de informações públicas e de interesse coletivo. É importante destacar que a LAI também estabeleceu a proteção de dados relativos à intimidade, vida privada, honra e imagem das pessoas, quando estiverem sob guarda de órgãos da Administração Pública.

Em 2018, foi promulgada a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), que estabelece as regras para o tratamento de dados pessoais. Vale destacar que a LAI já determinava, em seu art. 31, que o tratamento das informações pessoais fosse feito de forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais, remetendo a regulamento os procedimentos aplicáveis (art. 31, § 5º), hoje disciplinados pelo Decreto nº 7.724/2012. Em 2022, a proteção de dados pessoais foi alçada à categoria de direito fundamental autônomo pela Emenda Constitucional nº 115/2022, reforçando seu caráter independente, embora correlato, ao direito à intimidade e à vida privada.

Diante deste contexto, o debate em torno do acesso à informação adquiriu novas dimensões, gerando dúvidas quanto ao cumprimento das duas leis, considerando a obrigação de promover o acesso à informação, bem como garantir o tratamento legítimo dos dados pessoais.

É importante frisar que LAI e LGPD são leis complementares, que tutelam direitos fundamentais distintos. A LAI garante o direito de acesso à informação produzida e custodiada pelo Estado, assegurando a transparência como princípio basilar da democracia e da boa governança. A LGPD, por sua vez, regula o tratamento de dados pessoais tanto no setor público quanto no privado, inclusive quanto ao tratamento de dados em ambientes digitais. O seu objetivo não é restringir o acesso à informação, mas prevenir abusos e assegurar que o tratamento de dados ocorra de forma legítima e segura. Juntas, as duas leis oferecem instrumentos para que a atuação estatal seja transparente e responsável.

Vale ressaltar que a LGPD não estabelece sigilo, nem autoriza a negativa de acesso com fundamento na proteção de dados pessoais coletados, produzidos ou custodiados pelo poder público. Enquanto a LGPD disciplina o tratamento dos dados, a LAI estabelece as hipóteses de restrição de acesso a informações pessoais. Assim, eventuais negativas de acesso a dados pessoais devem se basear na LAI e cumprir os requisitos estabelecidos por essa Lei.

No contexto do setor público, o desafio consiste em equilibrar a transparência necessária para o atendimento ao interesse público com a proteção da intimidade e vida privada dos titulares dos dados. O interesse público constitui uma finalidade legítima que

justifica a divulgação de determinadas informações, contudo, essa divulgação deve ser conduzida dentro dos limites da razoabilidade e da proporcionalidade.

A divulgação de informações pessoais é uma forma de tratamento de dados pessoais e está sujeita, portanto, tanto à LAI quanto à LGPD. Sendo assim, vários questionamentos surgem: como garantir acesso à informação sem expor indevidamente a intimidade, a vida privada, a honra e a imagem das pessoas? Até que ponto é possível divulgar dados pessoais em nome da transparência? Como responder a pedidos de informação que envolvem dados pessoais? Em que situações o respeito aos direitos à intimidade, à vida privada, à honra e à imagem deve limitar a divulgação de informações, e quando isso se transforma em uma barreira indevida à transparência?

Este guia foi elaborado para apoiar agentes públicos no âmbito do Poder Executivo federal nessa tarefa, oferecendo orientações práticas para conciliar transparência e responsabilidade com os dados pessoais, e fortalecendo uma cultura administrativa que respeite os cidadãos e promova a confiança na gestão pública.

1. DIREITO DE ACESSO À INFORMAÇÃO E SEUS LIMITES

O direito de acesso à informação garante a toda pessoa o acesso a dados e informações produzidas ou custodiadas por órgãos ou entidades públicas. Esse direito existe porque o Estado administra informações em nome da sociedade. Por isso, toda informação sob gestão estatal deve ser acessível a todos, salvo quando houver justificativa legal e legítima para que este acesso seja negado.

1.1. A TRANSPARÊNCIA É A REGRA E O SIGILO É A EXCEÇÃO

Assim como outros direitos fundamentais, o acesso à informação não é absoluto. Deve-se garanti-lo na maior medida possível, de acordo com o princípio da máxima divulgação, expressamente previsto no artigo 3º, inciso I, da Lei de Acesso à Informação (Lei nº 12.527/2011 – LAI):

> *Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:*
>
> *I - observância da publicidade como preceito geral e do sigilo como exceção;*

Para que o princípio da máxima divulgação seja efetivo, é essencial que qualquer restrição de acesso à informação tenha uma base legal clara e legítima. Toda negativa de acesso deve ser devidamente fundamentada, indicando os motivos da restrição e a hipótese legal aplicável, de modo a assegurar a transparência da decisão administrativa e permitir o controle e a revisão pelos interessados.

1.2. EXCEÇÕES À TRANSPARÊNCIA

Informações classificadas

A Constituição Federal, em seu art. 5º, inciso XXXIII, garante o direito de acesso à informação, mas admite restrições excepcionais quando a divulgação puder comprometer a segurança da sociedade e do Estado.

Nesses casos, aplica-se, nos termos do art. 23 da LAI, a classificação da informação, que consiste no ato formal de limitar temporariamente o acesso a documentos ou dados públicos classificados.

Nos termos do art. 24, § 1º, da LAI, os prazos máximos de restrição de acesso à informação classificada variam conforme o grau de classificação atribuído:

- **Ultrassecreta** – até 25 anos, renovável uma única vez;
- **Secreta** – até 15 anos;
- **Reservada** – até 5 anos.

O prazo tem início na data de produção do documento. Ao fim do prazo ou do evento que justificou o sigilo, a informação torna-se automaticamente pública. A classificação deve sempre adotar o grau menos restritivo possível, considerando o interesse público.

A LAI (arts. 23 e 24) estabelece nove hipóteses taxativas para a classificação de informações, de modo que apenas aquelas informações nelas enquadradas podem ser formalmente classificadas.

Hipóteses de Classificação (Rol Taxativo)

1. Risco à defesa e soberania nacionais ou à integridade do território.
2. Prejuízo às relações internacionais do Brasil ou quebra de sigilo de informações recebidas de outros Estados/organismos internacionais.
3. Risco à vida, segurança ou saúde da população.
4. Ameaça à estabilidade financeira, econômica ou monetária do País.
5. Prejuízo a planos ou operações estratégicos das Forças Armadas.
6. Risco a pesquisas, sistemas, instalações ou áreas de interesse estratégico nacional.
7. Ameaça à segurança de instituições ou de altas autoridades, nacionais ou estrangeiras, e de seus familiares.
8. Comprometimento de atividades de inteligência, investigação ou fiscalização em andamento.
9. Risco à segurança do Presidente e Vice-Presidente da República e de seus familiares.

Encerrado o prazo ou evento que motivou a classificação, a informação torna-se passível de acesso público. Cabe ao órgão ou à entidade, no entanto, avaliar se há partes que devem permanecer protegidas por outras hipóteses de restrição previstas na legislação. Isso porque as 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.

Sigilos legais específicos

A LAI, em seu artigo 22, preserva os sigilos já existentes na legislação brasileira, pois reconhece que há exceções legítimas ao acesso à informação previstas em outras leis.

As hipóteses de sigilo apresentadas neste Guia são exemplificativas e não esgotam as

restrições de acesso previstas no ordenamento jurídico. Cabe aos órgãos e entidades observar, em cada caso concreto, a legislação específica aplicável, ainda que a respectiva hipótese de sigilo não esteja expressamente mencionada neste Guia.

São exemplos:

- **Sigilo bancário** – previsto na Lei Complementar nº 105/2001 - protege informações financeiras.
- **Sigilo fiscal** – previsto no art. 198 do Código Tributário Nacional (Lei nº 5.172/1966), resguarda dados tributários de pessoas e empresas.
- **Segredo de justiça** – previsto no art. 189 do Código de Processo Civil (Lei nº 13.105/2015) e em leis específicas, como o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) e o Código Penal (Decreto-Lei nº 2.848/1940), assegura confidencialidade de processos sensíveis, como aqueles nos quais constam dados protegidos pelo direito constitucional à intimidade, os que tratam de interesses de crianças ou adolescentes ou que envolvem crimes contra a dignidade sexual.
- **Sigilo industrial** – previsto na Lei da Propriedade Industrial (Lei nº 9.279/1996), protege informações estratégicas de empresas.

IMPORTANTE

Apenas leis ou normas com status equivalentes ou superiores podem estabelecer sigilos. Decretos, portarias, ou quaisquer outros atos infralegais não têm esse poder.

Documentos preparatórios

A possibilidade de restrição temporária a documentos preparatórios está prevista na 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.

A restrição pode ocorrer apenas quando necessária para a proteção do processo decisório em curso, evitando prejulgamentos ou interferências que comprometam a decisão. Nesses casos, o acesso é garantido após a edição do ato final que utilizou esses documentos como fundamento, ressalvadas outras hipóteses legais de restrição eventualmente aplicáveis ao conteúdo.

Exemplos:

- Documentos que subsidiam a proposição de medidas provisórias ou projetos de lei: enquanto ainda estão em discussão interna, o acesso pode ser restrito para preservar o espaço deliberativo.
- Documentos dos processos administrativos disciplinares (PAD): são restritos antes da conclusão do processo, evitando prejuízo e garantindo a eficácia da apuração.

Uma vez tomada a decisão, por exemplo, o envio da proposta ao Congresso ou conclusão do PAD, os documentos que embasaram o ato podem ser disponibilizados à sociedade, em respeito à transparência e ao controle social.

Dados pessoais

A LAI (art. 31) também estabelece proteção específica às informações pessoais, em consonância com a Constituição Federal (arts. 5º, X, e 37, § 3º, II). São de acesso restrito as informações relativas à intimidade, à vida privada, à honra e à imagem das pessoas.

Esse é um tema de grande relevância prática, sobretudo porque a Administração Pública lida diariamente com informações pessoais de cidadãos em políticas sociais, previdenciárias, de saúde, de educação e de segurança. A proteção às informações acima mencionadas será detalhada no capítulo 3 deste Guia.

Fundamentos administrativos para negativa de informação

Existem hipóteses em que os pedidos de acesso à informação não podem ser atendidos por órgãos ou entidades públicas devido à impossibilidade operacional. Nesse caso, não se trata da restrição da informação em si.

No Poder Executivo federal, essas hipóteses estão previstas no art. 13 do Decreto nº 7.724/2012, que estabelece que o pedido poderá ser negado quando for:

- **Genérico**: quando o solicitante não descreve com clareza ou especificidade a informação desejada, dificultando ou impossibilitando sua localização.

  Exemplo: "Quero todos os documentos sobre o que o órgão fez em 2024".

- **Desproporcional**: quando exige da Administração esforço excessivo de triagem, tratamento ou consolidação de dados, prejudicando o funcionamento regular do órgão e a prestação de serviços públicos. Trata-se de análise de natureza quantitativa.

  Exemplo: "Quero cópia de todos os documentos registrados no Sistema Eletrônico de Informações (SEI) em 2023".

  Nesse caso, seria necessário analisar todos os documentos para verificar a existência de informações pessoais de acesso restrito ou outras informações sigilosas.

- **Desarrazoado**: quando pode ser identificada incompatibilidade intrínseca entre o objeto da demanda e a razão pública dirigida ao bem comum. Trata-se de análise de natureza qualitativa.

  Exemplo: "Quero informações sobre a segurança do Presidente da República: quantidade de seguranças, escala de trabalho, tipos de armamentos ou outros equipamentos utilizados".

- **Trabalho adicional de 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 a atividade de localizar, organizar e fazer explicação textual sobre a informação sob sua guarda. Ou seja, localizar documentos, organizar as informações e montar uma

resposta textual explicativa não pode ser considerado trabalho de produção de informação.

Exemplo: "Quero que o órgão faça o cruzamento dos dados da base A, B e C, consolidando o resultado de todos os contratos dos últimos dez anos, separados por: fornecedor, valor, data, setor econômico, tipo de contrato, renúncia fiscal".

IMPORTANTE

A motivação do cidadão não pode ser usada como critério para considerar um pedido como desarrazoado (art. 10, §3° da LAI).

Em qualquer dessas situações, a negativa deve ser fundamentada de forma clara e objetiva, indicando as razões da impossibilidade de atendimento e, sempre que possível, sugerindo meios alternativos de acesso à informação.

Por fim, destaca-se 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, tramitação, uso, organização, arquivamento, preservação e disponibilização das informações públicas, conforme determinam a Constituição Federal e a LAI. Nesse sentido, 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.

2. DIREITO À PROTEÇÃO DE DADOS PESSOAIS NA LGPD

A Lei Geral de Proteção de Dados (LGPD) dispõe sobre princípios, direitos e deveres que devem ser observados sempre que houver tratamento de dados pessoais, por pessoa natural ou jurídica de direito público ou privado. Tudo o que se faz com o dado pessoal - coletar, guardar, compartilhar, utilizar, acessar, distribuir etc. - é considerado tratamento. Aqueles que realizam essas ações são os agentes de tratamento.

Dados pessoais são quaisquer informações relacionadas a uma pessoa natural identificada ou identificável. Isso inclui, por exemplo: nome, filiação, endereço, CPF, local de nascimento, data de nascimento, estado civil, matrícula funcional, informações de saúde, histórico escolar, vínculos trabalhistas, entre outros. A LGPD aplica-se a dados de pessoas naturais - ou seja, pessoas vivas, uma vez que a existência da pessoa natural termina com a sua morte (art. 6º, Lei nº 10.406, de 10 de janeiro de 2002 – Código Civil). Não abrange, portanto, dados relacionados a pessoas falecidas ou pessoas jurídicas.

A LGPD também traz o conceito de dado pessoal sensível e estabelece regras mais rigorosas para o tratamento desse tipo de dado, devido ao seu maior potencial discriminatório em caso de acesso indevido. São considerados dados pessoais sensíveis, conforme o art. 5º, II, da LGPD, aqueles que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organizações de caráter religioso, filosófico ou político, além de dados referentes à saúde, à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

É importante esclarecer que a proteção de dados pessoais, nos termos da LGPD, alcança, em regra, todo e qualquer dado de caráter pessoal, de modo que seu âmbito de proteção é mais abrangente do que a LAI, que protege especificamente informações pessoais que guardam relação com a intimidade, vida privada, honra e imagem das pessoas. A LGPD estabelece critérios para o tratamento de dados pessoais, não com o intuito de restringir o acesso a dados pessoais, mas de estabelecer as balizas para que todo tratamento ocorra em respeito aos direitos fundamentais, à autodeterminação informativa e ao livre desenvolvimento da personalidade da pessoa natural.

Entendendo o escopo ampliado de incidência da LGPD, cabe explicitar a diferença entre proteção de dados pessoais e a proteção à intimidade, à vida privada, à honra e à imagem.

	Proteção de dados pessoais	Proteção das informações pessoais relativas à intimidade, vida privada, honra e imagem
Lei incidente	LGPD	LAI
O que é?	Refere-se às regras que orientam como os dados pessoais devem ser tratados, ou seja, coletados, utilizados, compartilhados, etc.	Refere-se a informações pessoais relacionadas aos direitos de cada pessoa de preservar sua intimidade, vida privada, honra e à imagem.
Para que serve?	Busca garantir que o tratamento de dados pessoais seja realizado de forma adequada, necessária, segura e compatível com os direitos dos titulares.	Busca evitar exposições indevidas ou interferências injustificadas na vida do indivíduo.
Quais as obrigações dos agentes públicos?	Adotarem medidas ativas para garantir o tratamento de dados em conformidade com a lei, prevenir a ocorrência de danos, e garantir o exercício de direitos pelo titular, entre outras.	Adotarem medidas para proteger as informações pessoais relativas à intimidade, à vida privada, à honra e à imagem de acesso indevido, salvo se houver previsão legal.

Dessa forma, conclui-se que a LAI e a LGPD são regimes jurídicos complementares, que tutelam direitos fundamentais distintos e igualmente relevantes, cuja aplicação deve ser harmonizada. A LGPD, introduziu critérios, princípios e salvaguardas para o tratamento de dados pessoais de modo a evitar tratamento desnecessário, desproporcional ou dissociado da finalidade pública que o justifica. Nesse contexto, a LGPD nem afasta, nem relativiza o princípio da publicidade que rege a Administração Pública, e tampouco cria hipótese de sigilo.

2.1. PRINCÍPIOS E HIPÓTESES LEGAIS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

A LGPD estabelece regras e princípios para orientar o tratamento de dados pessoais pelo Poder Público. Destacam-se, em especial:

- **Finalidade**: o tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular. No âmbito do setor público, o tratamento de dados pessoais deve atender a uma finalidade pública.
- **Adequação**: os dados tratados devem ser compatíveis com as finalidades informadas e com o contexto do tratamento.
- **Necessidade**: o tratamento deve se limitar ao mínimo de dados pessoais indispensáveis para a consecução da finalidade pública, evitando coletas, usos ou divulgações excessivas.
- **Transparência**: os titulares devem ter acesso a informações claras, precisas e acessíveis sobre o tratamento de seus dados. Esse princípio impõe obrigações de cunho geral e que demandam uma postura ativa do agente de tratamento. No setor público, esse princípio é reforçado, visto que o art. 23, I da LGPD prevê o dever de informação das hipóteses de tratamento de dados pessoais realizados

pelo Poder Público em veículos de fácil acesso pelas pessoas jurídicas de direito público responsáveis pelas operações de tratamento.

- **Segurança**: devem ser adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, vazamentos, perdas ou usos indevidos.
- **Prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
- **Responsabilização e prestação de contas**: o órgão público deve demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Esses princípios orientam quaisquer operações de tratamento de dados pessoais pela Administração Pública, o que inclui a sua divulgação para cumprimento de obrigações de transparência, seja para o atendimento a pedidos formulados com base na LAI ou para publicação em transparência ativa.

Além de observar os princípios apresentados acima, o tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais.

No setor público, o tratamento de dados pessoais é, em regra, fundamentado nas hipóteses de cumprimento de obrigação legal ou regulatória e de execução de políticas públicas[1]. É o que acontece quando o Poder Público divulga informações pessoais para o cumprimento da LAI, da Lei de Governo Digital, e de outras legislações que tratam de transparência. Nessas situações, o tratamento é autorizado para atender determinações legais expressas com a finalidade de persecução do interesse público (LGPD art. 7º, II, III; art. 11, II, 'a' e 'b'; e art. 23 e 24). Ademais, a publicização de dados pessoais deve atender às regras estabelecidas por essas leis.

É importante destacar também que, quando o tratamento envolver dados pessoais de crianças e adolescentes, ele deve observar, ainda, o princípio do melhor interesse e as regras específicas previstas no art. 14 da LGPD.[2] Nesses casos, compete ao controlador demonstrar que foram adotadas as medidas de segurança apropriadas, considerando a especial vulnerabilidade desse público.

1 Para mais informações sobre as hipóteses legais previstas na LGPD para o tratamento de dados pessoais por entidades e órgãos públicos, ver o "Guia Orientativo – Tratamento de Dados Pessoais pelo Poder Público". ANPD, Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf/@@display-file/file.

2 Conforme o Enunciado CD/ANPD nº 1, de 22 de maio de 2023, "o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei."

2.2. REGIME JURÍDICO DO TRATAMENTO DE DADOS PESSOAIS PELA ADMINISTRAÇÃO PÚBLICA

No Capítulo IV, a LGPD estabelece um regime jurídico específico para o tratamento de dados pessoais pelo Poder Público, distinto daquele aplicável às relações privadas. Esse regime especial, embora amparado no interesse público, não autoriza o tratamento irrestrito de dados pessoais. Ao contrário, impõe à Administração Pública o dever de tratar dados de forma proporcional, finalística e compatível com suas competências institucionais, devendo ser realizado para o atendimento da finalidade pública, na persecução do interesse público. 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.

2.3. LGPD E LAI: COMPATIBILIDADE E COMPLEMENTARIDADE

É fundamental reforçar que a LGPD não institui, por si só, hipótese geral de sigilo para informações pessoais, nem altera o rol de informações de acesso restrito previsto na legislação aplicável, sem prejuízo da observância das limitações, requisitos e salvaguardas incidentes sobre o tratamento e a divulgação de dados pessoais previstos na própria LGPD e em legislação específica. No que concerne ao regime jurídico do acesso à informação pública, seu papel é complementar à LAI, oferecendo critérios para o tratamento responsável de dados pessoais ao longo do ciclo informacional do Estado.

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.

A adequada articulação entre LAI e LGPD exige dos órgãos públicos uma postura ativa de planejamento, ponderação e fundamentação das decisões administrativas, assegurando simultaneamente o direito de acesso à informação, os direitos à intimidade, à vida privada, à honra, à imagem e à proteção de dados pessoais. Nesse sentido, a proteção de dados deve ser compreendida como elemento estruturante da boa governança, da transparência responsável e do fortalecimento da legitimidade da atuação estatal.

IMPORTANTE

Considerando o escopo de proteção da LGPD, importa destacar que não existem dados pessoais irrelevantes e que, no ambiente digital contemporâneo, identificadores, como nome completo e CPF, podem funcionar como elementos de conexão entre diferentes bases de dados, públicas ou privadas, ainda que tais bases de dados tenham sido anonimizadas, podendo viabilizar a reidentificação e a construção de perfis detalhados dos titulares por meio de técnicas de correlação e mineração de dados. Esse risco de reidentificação, assim como eventuais outros riscos a que possam ser expostos os titulares, deve ser considerado pelos agentes públicos na aplicação do princípio da prevenção (art. 6°, VIII, da LGPD), que requer a adoção de medidas de mitigação de riscos para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Tais medidas devem ser proporcionais à finalidade legítima de divulgação do dado pessoal, priorizando a descaracterização (anonimização/pseudonimização) sempre que possível. Vale ressaltar, no entanto, que a anonimização ou a pseudonimização não foram definidas pela LGPD como condições técnicas para a divulgação pública ou para o compartilhamento de dados pessoais por entidades e órgãos públicos. Por esta razão, a eventual identificação dos titulares ou a admissão de algum grau de risco de sua identificação, quando necessárias, por exemplo, para atender determinações legais, o interesse público ou o direito de acesso à informação, são compatíveis com a LGPD.

Eventualmente, essas medidas podem ser descritas em relatório de impacto à proteção de dados pessoais, documento 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" (art. 5°, XVII, e art. 38, parágrafo único, ambos da LGPD).

3. A PROTEÇÃO DAS INFORMAÇÕES RELATIVAS À INTIMIDADE, VIDA PRIVADA, HONRA E IMAGEM DAS PESSOAS PREVISTA NA LAI

A LAI estabelece que as informações pessoais relativas à intimidade, vida privada, honra e imagem têm regime de proteção próprio. Dessa forma, a LAI restringe o acesso de terceiros a essas informações, autorizando-o apenas em hipóteses específicas (art. 31). No âmbito da Administração Pública, portanto, é a LAI que estabelece o escopo de restrição de acesso à informação pessoal coletada, produzida ou armazenada, e não a LGPD.

Quando se trata de divulgar informações pessoais, seja em resposta a pedidos de acesso à informação, ou para cumprimento de obrigações de transparência ativa, deve-se levar em consideração as determinações da LAI relativas à proteção da intimidade, da vida privada, da honra e da imagem das pessoas.

A LAI é norma específica que rege essa matéria, enquanto a LGPD é aplicada de maneira complementar de modo a garantir que o tratamento de dados observe princípios como finalidade, necessidade, transparência, segurança e prevenção. Nesse sentido, destaca-se o Enunciado CGU nº 4, de 10 de março de 2022.

Enunciado CGU nº 4/2022

Nos pedidos de acesso à informação e respectivos recursos, as decisões que tratam da publicidade de dados de pessoas naturais devem ser fundamentadas nos arts. 3º e 31 da Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), vez que:

A LAI, por ser mais específica, é a norma de regência processual e material a ser aplicada no processamento desta espécie de processo administrativo; e

A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos.

A tabela a seguir resume as características centrais de cada legislação, e serve de apoio para compreensão da distinção entre elas:

Característica	Lei de Acesso à Informação (LAI)	Lei Geral de Proteção de Dados (LGPD)
Escopo Principal	Regulamenta o direito de acesso à informação pública, seja por meio de publicação proativa de informação ou em resposta a demandas específicas	Regulamenta o tratamento de dados pessoais (coleta, uso, processamento, acesso, transmissão, eliminação etc.).
Alcance da lei	Todos os órgãos e entidades do poder público.	Qualquer agente de tratamento, seja pessoa natural ou jurídica, de direito público ou privado.
Hipótese de restrição de acesso à informação pessoal	Apresenta hipóteses de restrição de acesso a informações pessoais relativas à intimidade, vida privada, honra e imagem das pessoas (art. 31). A LAI também elenca as situações excepcionais em que terceiros podem acessar informações pessoais relativas à intimidade, vida privada, honra e imagem.	Não apresenta hipóteses adicionais de restrição de acesso a informações pessoais no âmbito do poder público.

3.1. INFORMAÇÃO PESSOAL DE ACESSO RESTRITO

Como visto no capítulo anterior, dados pessoais correspondem a todas as informações relacionadas a uma pessoa natural identificada ou identificável, incluindo, entre outros, dados cadastrais e informações vinculadas à sua vida pessoal ou profissional.

IMPORTANTE

É importante destacar que o Estado não é o titular do dado pessoal, mesmo quando a informação está sob sua guarda. O dado pessoal tem um titular: a pessoa natural identificada ou identificável a que se refere.

A LAI não restringe acesso a todo dado pessoal: as informações protegidas pelo art. 31 são aquelas relacionadas à intimidade, à vida privada, à honra e à imagem das pessoas.

O termo “informação pessoal de acesso restrito” será utilizado nesse Guia para se referir a esse subconjunto de informações.

A LAI protege várias esferas da vida pessoal do indivíduo, as quais estão detalhadas a seguir:

Categoria	O que é	Importância da restrição	Exemplos (informações protegidas, em tese)
Intimidade	Esfera mais íntima da pessoa, cuja divulgação pode comprometer o livre desenvolvimento da sua personalidade ou sujeitá-la a atos discriminatórios.	Evitar, entre outros aspectos, constrangimento, discriminação ou violação direta da vida íntima da pessoa.	• Informações de saúde (atestados, diagnósticos). • Origem étnica ou racial. • Convicções religiosas, políticas ou filosóficas. • Dados sobre orientação sexual.
Vida Privada	Abrange relações familiares, sociais e profissionais do indivíduo. É uma esfera mais ampla que a intimidade.	Evitar intromissões indevidas na rotina, vínculo e nas relações pessoais, preservando a segurança e o direito ao resguardo.	• Endereço e telefone pessoal. • Dados sobre dependentes e familiares. • Vínculos afetivos. • Informações sobre rotina, deslocamentos ou hábitos pessoais.
Honra	Relaciona-se a informações que se referem ao valor social e moral da pessoa. Trata-se do que a pessoa sente sobre si mesma e do que a sociedade pensa sobre ela.	Evitar que sejam divulgadas ofensas, difamações ou falsidades que possam gerar danos à reputação, prejuízos morais ou abalar a imagem de alguém perante si mesmo ou perante os outros.	• Reputação perante a sociedade.
Imagem	Dados que revelam a fisionomia e retrato da pessoa, ou seja, sua imagem-retrato como uma expressão externa do indivíduo. Há também a imagem-atributo da pessoa, que está relacionada com um conjunto de características que podem ser associadas a um indivíduo em sua representação no meio social, como a reputação ou o prestígio.	A exposição não autorizada pode gerar riscos, constrangimentos e uso indevido da imagem da pessoa. Busca-se preservar não apenas o aspecto físico, mas também o contexto em que a imagem pode ser exibida.	• Fotos ou vídeos identificando pessoas em contextos da vida privada. • Filmagens de câmeras de segurança. • Imagens obtidas em fiscalizações que exponham indivíduos.

IMPORTANTE

A LGPD confere maior rigor no tratamento dos dados pessoais sensíveis, os quais também se enquadram no escopo de proteção estabelecido pela LAI. Contudo, a proteção conferida pela LAI alcança também dados pessoais não sensíveis, incluindo, por exemplo, endereço, filiação e dados pessoais de contato, desde que relativos à intimidade, vida privada, honra e imagem.

No entanto, **não se deve confundir a categorização dos dados como "sensíveis" e "não sensíveis", com a obrigação de publicizar ou restringir o acesso**. A decisão quanto à possibilidade de divulgação de dados pessoais deve sempre decorrer de análise da situação específica, desde que observados os critérios previstos na LAI e as orientações indicadas neste Guia.

Conforme já mencionado no capítulo anterior, existe a categoria dos dados pessoais sensíveis, criada pela LGPD. Em razão de seu potencial de discriminação ilícita ou abusiva, esses dados estão sujeitos a um regime de proteção mais rigoroso, abrangendo dados sobre origem racial ou étnica, crenças religiosas, opiniões políticas, filiação a entidades, bem como informações relativas à saúde, à vida sexual e a características genéticas ou biométricas.

O acesso a informação pessoal referente à intimidade, vida privada, honra ou imagem pode ocorrer por diferentes vias, tais como: pedido de acesso à informação por meio da LAI; cumprimento de ordem judicial; obrigação legal; ou para a proteção da vida ou da saúde de pessoas.

A restrição de acesso a esse tipo de informação pessoal é de, no máximo, 100 anos, contados a partir da data de produção do documento, conforme o art. 55 do Decreto nº 7.724/2012. Ou seja, não se trata de um sigilo de 100 anos a ser aplicado de forma automática a todos os casos, mas do prazo máximo que pode ser aplicado para a proteção de uma informação para assegurar o direito à intimidade, vida privada, honra e imagem das pessoas.

Visando limitar o uso excessivo do prazo máximo de 100 anos, foi publicado o Enunciado CGU nº 1/2024, que estabeleceu diretrizes para a aplicação do prazo de restrição de acesso a dados pessoais.

> *Enunciado CGU nº 1/2024 - Prazo de Restrição Padrão*
>
> ***Na ausência de indicação expressa quanto ao prazo de sigilo da informação pessoal, não se pode presumir a aplicação do prazo máximo previsto no art. 31, §1º, da Lei nº 12.527, de 18 de novembro de 2011. Nesses casos, deve-se adotar a presunção de restrição de 15 (quinze) anos ou, quando possível, até o evento que permita determinar seu termo final. Decorrido esse prazo, a Administração, mediante requerimento, deverá realizar nova análise da situação específica da informação. Este enunciado não gera qualquer prejuízo ao direito de solicitação de acesso à informação a qualquer tempo, nem ao exercício da autotutela administrativa.***

Em outras palavras, os órgãos devem indicar o prazo de restrição de acesso levando em consideração o risco concreto da sua divulgação antecipada. Se não houver indicação expressa de prazo, aplica-se, como regra, o prazo de 15 anos (ou até evento que defina seu término). Não se pode, portanto, presumir o prazo máximo da LAI quando indeferido o acesso à informação. Ressalta-se que, após esse período, a restrição será reavaliada, caso o órgão receba nova solicitação de acesso.

O Enunciado foi publicado a partir do entendimento de que o período de restrição deve ser definido de forma proporcional à natureza dos dados pessoais demandados no caso concreto. Isso exige avaliar tanto o interesse público e geral existente no acesso à informação sob análise, quanto o risco concreto ao titular dos dados a partir da divulgação. Dessa forma, o prazo de restrição deve se limitar ao período efetivamente necessário à proteção do titular, evitando-se restrições prolongadas quando não houver justificativa suficiente para afastar, por período tão extenso, o exercício do direito fundamental de acesso à informação.

3.2. ACESSO PELO TITULAR À PRÓPRIA INFORMAÇÃO PESSOAL

O titular do dado pessoal pode utilizar a LAI para solicitar ao Estado acesso às suas próprias informações pessoais. Nesses casos, aplicam-se os procedimentos e prazos previstos na LAI para o atendimento do pedido, que, 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.

USO DE CANAIS ESPECÍFICOS PARA ACESSO À INFORMAÇÃO PESSOAL

Muitos órgãos e entidades públicas dispõem de canais ou sistemas próprios destinados especificamente ao atendimento de demandas de acesso à informação pessoal pelo titular (canais de atendimento relativo à gestão de pessoas, sistemas de acompanhamento de benefícios previdenciários ou centrais de atendimento setoriais).

Nesses casos, aplica-se o entendimento consolidado pela Comissão Mista de Reavaliação de Informações (CMRI), por meio da Súmula CMRI nº 1/2015, de que o órgão ou a entidade deve orientar o interessado a buscar a informação por intermédio do canal ou procedimento específico, indicando os prazos e as condições para sua utilização, sendo o pedido considerado atendido.

Essa indicação só é válida quando o canal específico for efetivo. Caso o cidadão demonstre, no próprio pedido LAI ou em fase recursal, que o canal indicado não funcionou ou não permitiu o acesso à informação, o órgão deve responder à demanda normalmente pela via da LAI.

Cabe diferenciar o direito do titular, assegurado pela LGPD, de conhecer o tratamento realizado com seus dados pessoais e de ter acesso aos dados que são objeto desse tratamento, nos termos dos arts. 9º e 18, inciso II. Esse direito não se confunde com o direito de acesso à informação previsto na LAI. No exercício dos direitos previstos na LGPD, o titular busca saber quais de seus dados pessoais são tratados pelo órgão e obter informações sobre as condições em que esse tratamento ocorre, como sua finalidade, forma e duração. Já em um pedido formulado com fundamento na LAI, o interessado pode requerer acesso ao conteúdo de documentos ou processos administrativos que contenham informações a seu respeito, isto é, aos registros documentais produzidos ou mantidos pelo Poder Público, e não apenas aos dados pessoais neles contidos.

3.3. ACESSO POR TERCEIROS À INFORMAÇÃO PESSOAL RELATIVA À INTIMIDADE, VIDA PRIVADA, HONRA E IMAGEM

A LAI estabelece as situações específicas em que a informação pessoal relativa à intimidade, vida privada, honra e imagem pode ser acessada por terceiros. As hipóteses são apresentadas a seguir, com explicação e orientações práticas para os órgãos e entidades públicas, e correspondem às finalidades que autorizam o acesso.

A indicação da finalidade no momento da demanda, que relaciona a solicitação às hipóteses autorizativas, não se confunde, portanto, com a necessidade de motivação do pedido de acesso à informação geral produzida ou custodiada por órgãos e entidades públicas (art. 10, § 3º da LAI). Como já mencionado, o Estado não é o titular da informação pessoal, e a própria LAI estabelece procedimentos distintos para esse tipo de demanda.

a) Consentimento expresso para divulgação do dado, por meio de procuração

Uma das possibilidades de acesso à informação pessoal por terceiros, nos termos do art. 60, parágrafo único, inciso I, do Decreto nº 7.724/2012, é mediante a apresentação de procuração. Trata-se de consentimento específico para a divulgação de dados pessoais, em resposta a pedidos de informação pessoal.

Contudo, em todas as outras hipóteses em que a LAI permite a divulgação a terceiros, a autorização por meio de procuração não é necessária. Essa hipótese está alinhada à LGPD, que prevê diferentes hipóteses legais para o tratamento de dados pessoais, sem estabelecer hierarquia entre elas.

b) Previsão legal

O acesso também pode ocorrer quando uma lei específica determina a divulgação do dado ou autoriza o seu fornecimento a terceiros, especialmente para uso por agentes públicos no exercício de sua função.

O acesso para essa finalidade pode ser necessário, inclusive, para processos de apuração de irregularidades. A LAI é expressa ao indicar que a restrição de acesso a dados relativos à intimidade, vida privada, honra e imagem das pessoas não pode ser usada como obstáculo à condução de tais processos, quando o titular dos dados estiver envolvido (LAI, art. 31, § 4º).

Ressalta-se, também, que compartilhamento de dados pessoais para atender a demandas de instituições públicas no exercício de suas competências legais submete-se, geralmente, a normas e legislações próprias. Assim, nesses casos, a concessão do acesso não ocorrerá por meio de resposta a um pedido de acesso nos termos da LAI.

c) Prevenção e diagnóstico médico

A LAI permite o acesso a informações pessoais quando necessário para prevenção ou diagnóstico médico de pessoas incapazes. Essa hipótese é aplicada, por exemplo, no âmbito administrativo, a equipes e profissionais de saúde no tratamento dos pacientes. Nesses casos, a concessão do acesso não ocorrerá por meio de resposta a um pedido de acesso nos termos da LAI.

d) Estatísticas e pesquisas

A LAI autoriza os órgãos e entidades públicas a fornecerem informações pessoais para realização de estatísticas ou pesquisa científica, com a condição de que as pessoas a que eles se referem não sejam identificadas e de que a pesquisa tenha objetivos de evidente interesse público ou geral, previstos em lei (art. 31, § 3º, II, da LAI). Essa hipótese constitui exceção específica à exigência de consentimento e deve observar integralmente os requisitos estabelecidos pela LAI.

A LGPD, por sua vez, prevê hipótese legal específica para o tratamento de dados pessoais por órgãos de pesquisa, devendo, sempre que possível, promover sua anonimização (art. 7º, inciso IV, art. 11, inciso II, alínea "c", e art. 16, inciso II da LGPD). Dito isso, a lei se resume às obrigações de órgãos de pesquisa, na condição de controladores, no tratamento desses dados, mas não sobre as formas de acesso a eles.

A concessão de acesso a dados pessoais que permitam a identificação não contraria a LGPD, conforme o "Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas" da ANPD, que esclarece que 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[3]. Como a ANPD reconhece no referido Guia, em alguns casos, a identificação dos titulares pode ser imprescindível para os objetivos da pesquisa.

No caso de dados pessoais que passaram por pseudonimização ou anonimização, alguns pontos merecem ser esclarecidos. A pseudonimização é o tratamento pelo qual os dados pessoais deixam de ser atribuídos a um titular específico, salvo mediante o uso de informações adicionais mantidas separadamente pelo controlador. Como essa associação continua possível, os dados não perdem sua natureza pessoal e, portanto, permanecem sujeitos à LGPD. A anonimização, por sua vez, consiste em processo que descaracteriza o dado como pessoal, desde que a reidentificação do titular não seja possível mediante meios técnicos razoáveis e disponíveis no momento do tratamento.

O acesso não será, contudo, automático, permanecendo sujeito aos procedimentos da LAI e às demais restrições legais aplicáveis.

No que se refere à avaliação sobre o evidente interesse público ou geral da pesquisa a ser realizada, trata-se de uma exigência prevista no art. 31, § 3º, II, da LAI, e no Decreto nº 7.724/2012. Por isso, as solicitações devem fornecer elementos que possibilitem que o órgão avalie esse requisito. Assim, é necessária a demonstração do interesse público ou geral para subsidiar a análise do órgão.

3 ANPD. Guia Orientativo – Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas. Brasília, 2023, p. 41. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf/@@display-file/file

Como anteriormente citado, o pedido de acesso à informação pessoal para essa finalidade não se confunde com o pedido de acesso a demais informações produzidas ou custodiadas pelo Poder Público, que não exige que o cidadão motive a sua demanda (art. 10, § 3º da LAI). Como já esclarecido anteriormente, o dado pessoal não é do Estado, tem um titular. Por isso, para o pleno cumprimento da LAI e da LGPD, exige-se tratamento diferenciado para esse tipo de informação.

ORIENTAÇÕES PARA FORNECER INFORMAÇÕES PESSOAIS PARA PESQUISA COMPATIBILIZANDO AS DISPOSIÇÕES DA LAI E DA LGPD:

Dados pessoais identificados

As informações pessoais podem ser fornecidas para pesquisa, preferencialmente de forma anonimizada ou pseudonimizada (art. 7º, inciso IV da LGPD e art. 31, § 3º, inciso II da LAI). Se for necessário fornecer o dado sem a devida anonimização ou pseudonimização, é importante garantir os requisitos a seguir:

- A demanda deve ser apresentada por representante de órgão de pesquisa. Como anteriormente citado, 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 indicar quais são os dados pessoais requeridos, além de informações mínimas necessárias à avaliação do interesse público ou geral da pesquisa ou estudo (art. 31, § 3º, inciso II da LAI).
- Não cabe aos órgãos que concedem acesso à informação avaliar a metodologia, o mérito técnico ou o 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 (art. 61 do Decreto nº 7.724/2012).
- Para pesquisas em saúde pública, os dados fornecidos serão tratados exclusivamente dentro do órgão de pesquisa, mantidos em ambiente controlado e seguro, conforme práticas de segurança apropriadas, 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 qual-

quer excerto do estudo ou da pesquisa em nenhuma hipótese poderá revelar dados pessoais (art. 13 da LGPD).

Dados anonimizados

Quando existe a possibilidade de entrega dos dados pessoais de forma efetivamente anonimizada, aplicam-se as seguintes regras:

- Qualquer solicitante pode demandar as informações, ou seja, não é necessário estar associado a um órgão de pesquisa.
- A demanda deve indicar quais são os dados pessoais requeridos, além de informações mínimas necessárias à avaliação do interesse público ou geral da pesquisa ou estudo (art. 31, § 3º, inciso II da LAI).
- A assinatura de termo de responsabilidade é dispensada nesses casos.

e) Cumprimento de ordem judicial

O órgão deve fornecer a informação pessoal quando houver ordem judicial expressa. Ressalta-se, como mencionado anteriormente, que o compartilhamento de dados pessoais para atender a demandas de instituições públicas no exercício de suas competências legais submete-se, geralmente, a normas e legislações próprias. Assim, nesses casos, a concessão do acesso não ocorrerá por meio de resposta a um pedido de acesso nos termos da LAI.

f) Defesa dos direitos humanos

A LAI permite a divulgação de informações pessoais, sem consentimento do titular, para defesa de direitos humanos. Trata-se de hipótese aplicada quando a manutenção da restrição de acesso representar risco à proteção da pessoa ou grupo envolvido. O acesso à informação pessoal para essa finalidade tem alguns requisitos específicos.

Não foi à toa que a LAI estabeleceu hipótese específica de acesso à informação por terceiros para a proteção de direitos humanos. As violações também podem ser praticadas por agentes públicos, e a análise deve buscar privilegiar o acesso de modo a proteger os direitos humanos.

Primeiramente, deve-se avaliar se a informação demandada é necessária para defesa do direito humano ameaçado ou violado. Tal análise deve considerar as informações constantes na própria demanda. Trata-se de exigência da LAI (art. 31, § 3º, inciso IV) e do Decreto nº 7.724/2012 (art. 60, parágrafo único, inciso IV). Segundo as normas, o acesso à informação para esse fim é permitido caso haja demonstração da efetiva necessidade dos dados para a defesa de direitos humanos pretendida.

Disso decorre a importância de o solicitante demonstrar a necessidade de acesso à informação. Ressalta-se que isso não configura um descumprimento do art. 10, § 3º da LAI, que veda que os órgãos questionem a motivação da demanda. Como já citado anteriormente, o acesso a dados pessoais submete-se a parâmetros diferenciados, em cumprimento à LAI e à LGPD.

g) Recuperação de fatos históricos

A LAI prevê, ainda, situação especial que permite a divulgação de dados pessoais para recuperação de fatos históricos de maior relevância, sem necessidade de consentimento do titular. Essa exceção é um instrumento importante para evitar que documentos cruciais para a história do país permaneçam inacessíveis, assegurando que o interesse coletivo na memória histórica seja atendido de forma responsável e criteriosa.

No Poder Executivo federal, o reconhecimento formal de que um conjunto documental é essencial para a história administrativa, coletiva, social ou institucional do país é de competência do dirigente máximo do órgão detentor da informação.

Esse reconhecimento não é automático e deve seguir os seguintes passos:

- **Fundamentação**: A decisão precisa ser devidamente fundamentada, explicando por que aqueles registros são relevantes e por que o acesso é necessário para a preservação histórica;
- **Apoio técnico (opcional)**: Para garantir a segurança e objetividade da decisão, o órgão pode solicitar apoio técnico de universidades, centros de pesquisa ou instituições com experiência em história e arquivologia;
- **Transparência sobre abertura**: Antes de liberar o acesso irrestrito, o órgão deve publicar, com pelo menos trinta dias de antecedência, um extrato com a descrição resumida dos documentos envolvidos (assunto, origem e período), garantindo transparência sobre os dados que serão divulgados, permitindo manifestações de interessados;
- **Acesso público**: Após a decisão fundamentada e o decurso do prazo, o conjunto documental passa a ser de acesso público, não exigindo mais análise caso a caso (art. 59, § 3º do Decreto nº 7.724/2012).

Reforça-se que, como anteriormente citado, o pedido de acesso à informação pessoal para essa finalidade não se confunde com o pedido de acesso a demais informações produzidas ou custodiadas pelo Poder Público, que não exige que o cidadão motive a sua demanda (art. 10, § 3º da LAI). Segundo as normas, o acesso à informação para esse fim é permitido caso haja demonstração da efetiva necessidade dos dados para a recuperação de fatos históricos relevantes.

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

PRESERVAÇÃO DA HISTÓRIA E DO BEM COLETIVO

A Resolução nº 54/2023 do Conselho Nacional de Arquivos (CONArq) estabelece que os dados de pessoas falecidas recolhidos a arquivos permanentes não se sujeitam à LGPD. Segundo a norma, esse entendimento se estende aos dados de pessoas ausentes, nos casos em que a lei autoriza a abertura de sucessão definitiva.

Quando um indivíduo falece, a necessidade de proteger sua privacidade direta diminui diante do interesse de toda a sociedade. Com o passar do tempo, os documentos guardados em arquivos permanentes ganham um novo valor e se transformam em fontes essenciais de teor histórico, científico e de pesquisa, fundamentais para a compreensão do passado.

Assim, essas informações pessoais passam a integrar o patrimônio documental do país, protegidas por leis específicas que garantem o direito à memória coletiva e permitem que as futuras gerações conheçam sua própria história.

h) Interesse público e geral preponderante

A LAI prevê a possibilidade de divulgação de informações pessoais relativas à intimidade, vida privada, honra e imagem quando necessário para o atendimento ao interesse público e geral preponderante. Nesse caso, o órgão público precisa realizar uma análise cuidadosa, caso a caso. Na avaliação, é necessário fazer uma ponderação entre o direito de acesso à informação e os direitos à intimidade, à vida privada, à honra, à imagem e à proteção de dados do titular.

Disso decorre a importância de o solicitante demonstrar a necessidade de acesso à informação. Ressalta-se que não se trata de descumprimento do art. 10, § 3º da LAI, que veda que os órgãos questionem a motivação da demanda. Como já citado anteriormente, o acesso a dados pessoais submete-se a parâmetros diferenciados, em cumprimento à LAI e à LGPD.

O Enunciado CGU nº 12/2023 tratou sobre o assunto, estabelecendo que a proteção de dados pessoais deve ser compatibilizada com o direito de acesso à informação e que, por isso, pode ser flexibilizada quando, na situação concreta, prevalecer o interesse público geral e preponderante.

> *Enunciado CGU nº 12/2023 - Informação pessoal*
>
> *O fundamento "informações pessoais" não pode ser utilizado de forma geral e abstrata para se negar pedidos de acesso a documentos ou processos que contenham dados pessoais, uma vez que esses podem ser tratados (tarjados, excluídos, omitidos, descaracterizados etc.) para que, devidamente protegidos, o restante dos documentos ou processos solicitados sejam fornecidos, conforme preceitua o § 2º do art. 7º da Lei nº 12.527, de 18 de novembro de 2011, assegurando-se o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo. Além disso, a proteção de dados pessoais deve ser compatibilizada com a garantia do direito de acesso à informação, podendo aquela ser flexibiliza-*

da quando, no caso concreto, a proteção do interesse público geral e preponderante se impuser, nos termos do art. 31, § 3º, inciso V da Lei n. 12.527, de 2011, e dos arts. 7º, § 3º, e 23, caput, da Lei nº 13.709, de 14 de agosto de 2018.

Para identificar o interesse público e geral preponderante, o órgão deve avaliar se a informação é crucial para, por exemplo:

- Análise de uso adequado de recursos públicos;
- Controle social da política ou serviço público;
- Avaliação de integridade dos processos administrativos (licitações, processos seletivos);
- Controle social do exercício de função pública;
- Verificação de probidade administrativa (avaliação de enriquecimento ilícito, danos ao erário, violação aos princípios da Administração Pública).

As informações pessoais liberadas para atender ao interesse público e geral preponderante são consideradas fundamentais para permitir o controle social. Por essa razão, essas informações poderão ser utilizadas para divulgação ampla, em transparência ativa, pois beneficiam toda a sociedade. Dispensa-se, nesse caso, a assinatura de termo de responsabilidade.

3.4. RESPONSABILIDADES VINCULADAS AO USO DE INFORMAÇÕES PESSOAIS DE TERCEIROS

O acesso à informação pessoal por terceiros está condicionado à assinatura de um termo de responsabilidade com a hipótese que autorizou a divulgação, sendo vedada a destinação diversa ao que foi autorizado (Decreto nº 7.724/2012, art. 61). Sendo assim, o uso da informação pessoal pelo requerente se vincula expressamente à hipótese autorizativa, dentre as citadas anteriormente:

- Consentimento expresso, por meio de procuração;
- Previsão legal;
- Prevenção e diagnóstico médico;
- Estatísticas e pesquisas;
- Cumprimento de ordem judicial;
- Defesa dos direitos humanos;
- Recuperação de fatos históricos;
- Interesse público e geral preponderante.

A assinatura de termo de responsabilidade para fins de atendimento a pedido de acesso à informação pode ser dispensada quando:

- há autorização expressa do titular, por meio de procuração;

- a informação é concedida para recuperação de fatos históricos de maior relevância, já que, após a divulgação, a informação é considerada de acesso irrestrito ao público (art. 59, § 3º do Decreto nº 7.724/2012);
- for comprovado o interesse público e geral preponderante que justifique o acesso.

Independentemente da assinatura de termo de responsabilidade, a LAI é expressa ao indicar que quem obtiver acesso às informações pessoais de terceiros será responsabilizado por seu uso indevido (art. 61, §2º do Decreto nº 7.724/2012).

IMPORTANTE

- O termo de responsabilidade é previsto no art. 61 do Decreto nº 7.724/2012, como um dos requisitos para o acesso à informação pessoal de terceiros.
- A assinatura do termo de responsabilidade somente é necessária quando se tratar de dados pessoais. Não se aplica, portanto, quando forem anonimizados. Nesta hipótese, não há propriamente divulgação de informação de natureza pessoal, de modo que os riscos ao titular estão mitigados ou eliminados, pois a pessoa não é mais identificável.
- A gestão dos termos de responsabilidade, incluindo seu armazenamento e arquivamento, cabe a cada órgão, considerando suas necessidades operacionais e as normas aplicáveis.

4. CONCILIANDO A TRANSPARÊNCIA PÚBLICA E A INTIMIDADE, A VIDA PRIVADA, A IMAGEM E A HONRA DAS PESSOAS

Garantir a transparência em conjunto com a intimidade, a vida privada, a imagem e a honra das pessoas é um desafio no âmbito da Administração Pública. Nem toda informação produzida ou guardada pelo poder público é automaticamente passível de acesso, nem todo dado pessoal demandado deve permanecer inacessível sem uma avaliação criteriosa.

Vale relembrar que as informações pessoais podem ser acessadas tanto pelo próprio titular do dado quanto por terceiros, observadas as hipóteses tratadas no capítulo anterior. O caminho para avaliar se um dado pessoal pode ou não ser divulgado a terceiros deve considerar diversos fatores. A seguir, é apresentado um roteiro para apoiar o agente público na tomada de decisão para identificar se a informação pessoal pode ser divulgada ou se deve ter seu acesso restrito.

4.1. ANÁLISE DA POSSIBILIDADE DE DIVULGAÇÃO DE INFORMAÇÃO PESSOAL

Apresenta-se a seguir um esquema visual de perguntas que se deve fazer ao avaliar a possibilidade de divulgação do dado pessoal, especificamente para resposta a pedido de acesso à informação ou para o cumprimento de obrigações de transparência ativa. O escopo de análise em questão não inclui, portanto, todas as hipóteses de acesso à informação pessoal por terceiros descritas no capítulo anterior.



A. A demanda é apresentada pelo titular ou por representante autorizado?

- Se a informação pessoal é relacionada ao próprio solicitante, deve-se conceder acesso ao titular, condicionada à comprovação de sua identidade.
- Se quem demanda a informação é um representante do titular, deve-se solicitar a apresentação de procuração e validar a identidade do terceiro. Nesse caso, a decisão é pela concessão do acesso.

A identidade pode ser comprovada presencialmente, com apresentação de documentos de identificação, ou mediante acesso a sistemas governamentais com Selo de Confiabilidade Gov.br Ouro/Prata.

B. Se a demanda não é do próprio titular ou de representante autorizado, deve-se verificar se a informação demandada é relacionada à intimidade, vida privada, honra ou imagem

- Se a informação não for relativa à intimidade, vida privada, honra e imagem: a decisão é pela concessão do acesso.
- Ainda que a informação pessoal seja de acesso restrito, caso haja enunciados ou orientações da CGU, súmulas da CMRI ou precedentes do Supremo Tribunal Federal (STF) que abordem os mesmos tipos de informações pessoais demandadas, e em contexto semelhante, o acesso à informação poderá ser concedido.
- Caso as situações acima não se confirmem, será necessário avaliar o enquadramento em hipóteses específicas de acesso à informação por terceiros, em que a informação é de evidente interesse público.

C. Verificar se a demanda se enquadra em alguma das hipóteses que autorizam o acesso por terceiros quando comprovado o evidente interesse público

Para cumprimento das normas de transparência pública, informações pessoais podem ser acessadas por terceiros para:

- a realização de pesquisas e estatísticas científicas de evidente interesse público ou geral;
- a defesa de direitos humanos de terceiros;
- o cumprimento de decisão judicial;
- a prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização exclusivamente para o tratamento;
- a recuperação de fatos históricos de maior relevância; ou
- a proteção do interesse público geral e preponderante.

Essas hipóteses requerem a ponderação entre o direito de acesso à informação e o direito à proteção da intimidade, vida privada, honra e imagem. Se comprovado o evidente interesse público na informação, quando o benefício da divulgação da informação superar os eventuais riscos à privacidade das pessoas, a decisão será pela concessão do acesso.

Conforme a Lei de Acesso à Informação e o Decreto nº 7.724/2012, o acesso a dados pessoais de terceiros, nas hipóteses acima, depende da demonstração de interesse público evidente e legítimo. Cabe ao solicitante esclarecer essa finalidade no momento do pedido. A ausência dessa justificativa, porém, não impede a análise: nesse caso, o próprio agente público avalia o benefício potencial da divulgação e faz a ponderação necessária.

Especificamente para o acesso a dados pessoais para recuperação de fatos históricos, cabe destacar que o art. 59 do Decreto nº 7.724/2012 prevê rito específico para a análise. Aqui, o teste de interesse público é ferramenta importante, mas o dirigente máximo do órgão ou entidade pode solicitar apoio técnico de universidades, centros de pesquisa ou instituições com experiência em história e arquivologia, para garantir a segurança e objetividade da decisão.

4.2. IDENTIFICANDO O EVIDENTE INTERESSE PÚBLICO

O evidente interesse público é aquele que fundamenta, em situações específicas, a concessão de acesso a informações pessoais relativas à intimidade, vida privada, honra ou imagem que sejam importantes e necessárias para:

- fortalecer a participação democrática e o controle social;
- assegurar a prestação de contas do Estado;
- proteger direitos humanos;
- assegurar o direito à memória coletiva, permitindo que futuras gerações conheçam sua própria história; ou
- realizar estatísticas e pesquisas cujo resultado esperado apresente relevância que transcenda o interesse particular do pesquisador.

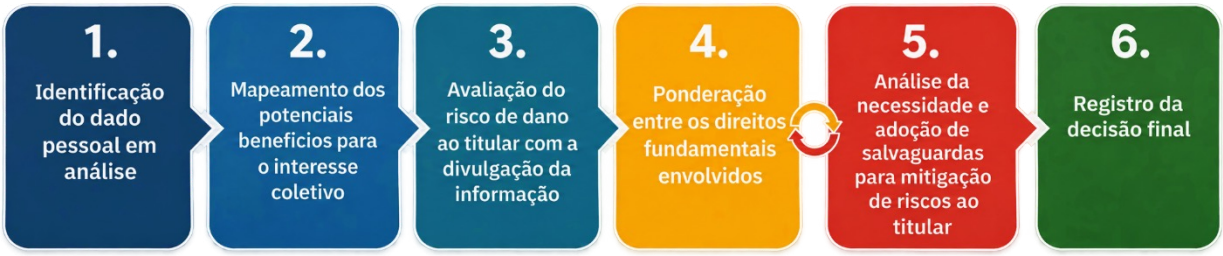
Nesse contexto, decidir se o acesso a um dado pessoal pode ou não ser concedido para atender ao interesse público requer uma análise criteriosa, por se tratar de uma situação que envolve direitos fundamentais garantidos pela Constituição Federal. De um lado, tem-se o direito de acesso à informação produzida ou guardada por instituições públicas. Do outro, os direitos à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Para decidir de forma segura, deve-se realizar o Teste de Interesse Público, levando em consideração as circunstâncias específicas de cada caso. Recomenda-se a aplicação do Teste sempre que se identificar eventual conflito entre os direitos de acesso à informação e de inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. O teste é aplicável especialmente nas hipóteses de divulgação de dados pessoais para a realização de pesquisas e estatísticas; a defesa de direitos humanos; a recuperação de fatos históricos de maior relevância; ou a proteção do interesse público e geral.

A seguir, apresenta-se o roteiro decisório para orientar a realização do Teste de Interesse Público para avaliação da possibilidade de divulgação de informações relativas à intimidade, da vida privada, da honra e da imagem das pessoas. Objetiva-se auxiliar a tomada de decisões equilibradas e responsáveis, fortalecendo a transparência e o controle social e sem exposição excessiva ou desproporcional de dados pessoais, em respeito ao princípio da necessidade consagrado pelo art. 6º, III da LGPD.

Ressalta-se que a complexidade do caso pode requerer a atuação coordenada de diferentes áreas do órgão, de acordo com suas competências, incluindo as áreas técnicas que produzem as informações demandadas, os responsáveis pela transparência e acesso à informação, e o/a encarregado/a de dados. A atuação conjunta pode contribuir para a tomada de decisão e para a definição da forma adequada de divulgação, quando for o caso.

Teste de Interesse Público: roteiro decisório



1. Identificação do dado pessoal em análise

Inicialmente, o agente público deve identificar quais dados pessoais são solicitados e analisar sua natureza, considerando, entre outros aspectos:

- É possível identificar claramente os dados pessoais em análise?
- Quais os tipos de dados demandados? Por exemplo: dados de identificação, dados acadêmicos, dados profissionais, dados funcionais, dados biométricos, dados financeiros, dados relacionados à saúde, à origem racial, a convicções religiosas, à vida privada etc.
- Trata-se de dados pessoais sensíveis ou não sensíveis?

Nesse momento, a intenção ainda não é fazer julgamento, mas sim identificar qual tipo de dado está sendo solicitado.

Ressalta-se que não se deve confundir a categorização dos dados como “sensíveis” e “não sensíveis” com a obrigação de publicizar ou restringir o acesso. A decisão quanto à possibilidade de divulgação de dados pessoais deve sempre decorrer de análise da situação específica, observados os critérios previstos na LAI e as orientações apresentadas neste Guia.

A tabela abaixo elenca exemplos de dados pessoais usualmente coletados e tratados pelos órgãos públicos para exercício de suas competências, que podem ser objeto de análise.

Dados pessoais não sensíveis		Dados pessoais sensíveis
• Nome Completo • Data de Nascimento • Local de nascimento • Gênero • Filiação • Estado Civil • Grau de escolaridade • Endereço pessoal • Email pessoal • Telefone pessoal • Número Pis/Pasep • Número do CPF • Número do RG • Número da Carteira de Trabalho • Número do Passaporte • Número do Título de Eleitor • Números identificadores do Certificado de Reservista • Data de nascimento ou casamento	• Email profissional • Telefone Profissional • Formação acadêmica • Matrícula funcional • Endereço profissional • Email profissional • Telefone Profissional • Cargo • Função • Histórico profissional • Assinatura manuscrita • Dados bancários • Dados fiscais • Dados de cartão de crédito • Endereço IP utilizado para acesso a sites e sistemas	• Origem racial ou étnica • Vida sexual • Convicção religiosa • Opinião política • Filiação a sindicato, organização religiosa, filosófica ou política • Dado de saúde • Dado genético • Dado biométrico

2. Mapeamento dos potenciais benefícios para o interesse coletivo

Para decidir se há evidente interesse público em relação ao dado pessoal em análise, o agente público deve identificar o benefício concreto que a divulgação produzirá para a coletividade.

Como explicado anteriormente, nas hipóteses em que o Teste de Interesse Público for aplicável, o solicitante deve esclarecer a finalidade pretendida e demonstrar a necessidade dos dados, o que auxiliará o órgão a identificar esse benefício. Na ausência dessa justificativa, cabe ao próprio agente público avaliá-lo.

Veja tabela exemplificativa de possíveis benefícios à coletividade:

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
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

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
Defender direitos humanos	Contribuir para a identificação e compreensão de violações de direitos humanos Permitir o reconhecimento e a reparação das vítimas, bem como a responsabilização por condutas ilícitas e a adoção de medidas destinadas a prevenir sua repetição
Permitir a recuperação de fatos históricos de maior relevância	Reconstituir acontecimentos de interesse coletivo, e preservar a memória social e institucional Compreender processos históricos que produziram efeitos no presente
Viabilizar a realização de estatísticas e pesquisas importantes para a coletividade	Contribuir para a compreensão de fenômeno social relevante, avaliação ou formulação de políticas públicas Promover conhecimento sobre a atuação estatal em áreas como saúde, educação e segurança
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 as agendas de agentes públicos em cargos decisórios para identificar vínculos de parentesco ou afinidade que possam comprometer a impessoalidade e a moralidade administrativa em nomeações e contratações.

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 serão consequências claras e diretas geradas a partir da abertura do dado analisado.

Para identificação dos benefícios concretos à coletividade, é fundamental que se analise a relação do titular do dado pessoal com o Estado. De forma geral, quanto mais próxima for a relação do titular com a Administração Pública, maior tende a ser o benefício coletivo da divulgação. Nesses casos, a publicidade do dado possibilita a verificação da regularidade da atuação funcional, do cumprimento dos deveres legais e do uso adequado de recursos públicos, contribuindo para o controle da legalidade e da moralidade administrativa.

É o que ocorre, por exemplo, com a divulgação da remuneração de agentes públicos, que apresenta benefício coletivo concreto ao permitir o controle do uso de recursos públicos e a identificação de eventuais situações de enriquecimento ilícito. Em sentido diverso, a divulgação da remuneração de particulares sem vínculo com a Administração Pública não produz, em tese, benefício público relevante, ainda que tais informações estejam sob a guarda do Estado, como ocorre com dados fiscais mantidos pela Receita Federal.

Assim, agentes públicos e particulares diretamente vinculados à Administração Pública estão sujeitos a um menor grau de preservação da intimidade, vida privada, honra e imagem em relação a informações associadas ao exercício dessas atividades. Já indivíduos para os quais a relação com o Estado é distante, indireta ou eventual apresentam maior expectativa de proteção a informações relativas a esses direitos da personalidade, devendo a divulgação de seus dados ser analisada com maior cautela.

Veja, a seguir, exemplos de dados que poderiam ser divulgados, a partir da análise da relação do titular com o Estado. Trata-se de orientação geral que pode ensejar decisão diferente dadas as particularidades do caso concreto.

Tipo de Titular	Proximidade com o Estado	Expectativa de Preservação da Intimidade, Vida Privada, Honra e Imagem	Exemplos de dados que podem ser divulgados (em tese)
Agente Público	Alta	Baixa	Nome completo Número de matrícula E-mail e endereço profissionais CPF descaracterizado, conforme padrão indicado no capítulo 5 Remuneração recebida Atos administrativos realizados Informações profissionais e acadêmicas
Fornecedor	Média alta	Média baixa	Nome completo E-mail e endereço profissionais CPF descaracterizado, conforme padrão indicado no capítulo 5
Beneficiário de recursos públicos	Média Baixa	Média alta	Nome completo CPF descaracterizado, conforme padrão indicado no capítulo 5 Se for o caso, número de cadastro na política pública (ex: NIS) Se for o caso, dado relacionado a requisito específico que enseja o recebimento do benefício
Usuário (Serviços Públicos)	Baixa	Alta	Normalmente, os dados pessoais são de acesso restrito. No entanto, pode haver situações em que o nome completo e outras informações passam ser divulgados. Por exemplo: alunos de universidades públicas, que são beneficiários das políticas de educação superior. A depender do serviço utilizado, porém, nem o nome completo pode ser divulgado. Por exemplo: serviços de saúde, segurança pública, proteção à vítima ou à testemunha.

3. Avaliação do risco de dano ao titular com a divulgação da informação

Para uma tomada de decisão responsável, o órgão deve avaliar os riscos concretos de dano ao titular decorrentes da divulgação da informação. O risco corresponde à probabilidade de ocorrência de um dano e à gravidade de suas consequências, caso esse dano venha a se concretizar.

A avaliação do risco deve considerar apenas danos plausíveis e diretamente relacionados à divulgação do dado analisado. Não se deve utilizar hipóteses abstratas ou meramente especulativas. **O dano analisado deve guardar relação direta de causa e efeito com a abertura da informação**.

A análise do risco envolve, de forma integrada, os seguintes elementos:

a) identificação do potencial dano - consiste em identificar quais efeitos adversos podem resultar da divulgação da informação, como risco à segurança do titular, estigmatização, discriminação, prejuízo financeiro ou exposição indevida da vida privada ou de dados sensíveis.

b) avaliação da probabilidade de ocorrência - após identificado o dano potencial, deve-se analisar a probabilidade de que ele se concretize efetivamente após a divulgação, considerando o tipo de dado, o contexto da solicitação, o grau de exposição. Aqui é também necessário avaliar se a informação já está acessível em outras fontes públicas oficiais como diários oficiais (da União, de estados ou municípios), em portais ou sistemas de responsabilidade de órgãos e entidades públicas. Nesse caso, a decisão pela divulgação não incorrerá em risco adicional ao titular do dado, já que as informações já estão públicas e podem ser acessadas por outros meios.

Nesta etapa, a avaliação da probabilidade de ocorrência dos riscos identificados deve considerar a forma de disponibilização da informação. Há diferença relevante entre a publicação em transparência ativa e o fornecimento de informação em resposta a um pedido de acesso pela LAI. Como a transparência ativa amplia a exposição e o alcance dos dados pessoais, sua adoção exige avaliação mais cautelosa quanto à necessidade, à adequação e à proporcionalidade da divulgação. Sempre que possível, devem ser adotadas medidas para reduzir os impactos sobre a intimidade, vida privada, honra e imagem, limitando a exposição dos dados ao estritamente necessário para viabilizar o controle social. Deve-se considerar, ainda, que os riscos à intimidade, vida privada, honra e imagem não decorrem apenas do conteúdo divulgado, mas também da forma de disponibilização da informação: quanto maior a facilidade de localização, cruzamento e reutilização dos dados, maior tende a ser o potencial de impacto sobre os titulares.

c) avaliação da gravidade do dano - caso o dano venha a ocorrer, deve-se estimar a gravidade de seus impactos sobre o titular, de forma qualitativa, podendo ser classificado, de maneira orientativa, como leve, médio ou grave, conforme seus reflexos sobre direitos fundamentais, segurança, situação econômica ou dignidade, por exemplo.

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. Essa avaliação pode ser compreendida como uma relação entre probabilidade e impacto. Não se trata, no entanto, de uma operação matemática ou automática, e sim de uma análise qualitativa, que deve ser realizada caso a caso.

4. Ponderação entre o direito de acesso à informação e a proteção à intimidade, vida privada, honra e imagem das pessoas



Concluídas as etapas anteriores, o agente público deve realizar a ponderação entre o direito de acesso à informação, tendo como base os benefícios coletivos levantados, e o direito à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas e à proteção de dados pessoais, nos termos da LAI e da LGPD.

Essa ponderação é base para a decisão final quanto à possibilidade de divulgação do dado pessoal, isto é, define se a informação poderá ou não ser tornada pública. Essa decisão é aplicável tanto aos pedidos formulados com base na LAI, quanto às hipóteses de divulgação em transparência ativa.

A decisão deve ser construída a partir dos elementos analisados nas etapas anteriores. Não se trata de uma avaliação intuitiva ou abstrata. É fundamental destacar que não há hierarquia prévia entre o direito de acesso à informação e o direito à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. A decisão deve ser sempre feita a partir da análise do caso concreto, de forma contextualizada e devidamente motivada, demonstrando de forma clara como os benefícios coletivos e os riscos de dano foram considerados para definir a possibilidade ou não de divulgação da informação.

Aplicação da ponderação

Benefício para a coletividade	Risco concreto para o titular	Possibilidade de divulgação
Elevado benefício	Baixo risco	Alta
Elevado benefício	Risco moderado, com possibilidade de mitigação	Alta
Reduzido benefício	Alto risco	Baixa

5. Análise da necessidade e adoção de salvaguardas para mitigação de riscos ao titular

Essa etapa é especialmente relevante quando o resultado da ponderação entre o direito de acesso à informação e a proteção à intimidade, vida privada, honra e imagem aponta para a necessidade de restrição de acesso à informação pessoal em razão de elevados riscos ao titular. Nesse caso, o agente público deve avaliar se é possível aplicar medidas

de salvaguarda que protejam os dados e reduzam os riscos aos titulares. Isso tende a privilegiar o direito de acesso à informação quando, do contrário, a demanda não poderia ser atendida.

Assim, é importante avaliar quais dados pessoais são efetivamente necessários para atender ao interesse coletivo identificado e como é possível aplicar as medidas de salvaguarda. Essa análise decorre da aplicação dos princípios da finalidade, adequação e necessidade, previstos no art. 6º da LGPD, segundo os quais o tratamento de dados pessoais deve se limitar ao mínimo necessário para a finalidade pretendida, com dados pertinentes, compatíveis, proporcionais e não excessivos. Ela também decorre da aplicação dos princípios da segurança e da prevenção, igualmente previstos no art. 6º da LGPD, que determinam a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais e a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Nesse contexto, observa-se que a análise da necessidade e a aplicação de salvaguardas são importantes ainda que a ponderação entre os direitos aponte para a possibilidade de divulgação do dado pessoal.

É dever do Estado, portanto, em cumprimento simultâneo às obrigações estabelecidas pela LAI e pela LGPD, assegurar que o acesso à informação pessoal seja restrito ao mínimo necessário à proteção do interesse público e geral preponderante. Tal diretriz concretiza o princípio da proporcionalidade e evita exposições desnecessárias da esfera privada dos indivíduos, garantindo que a transparência se realize de forma responsável, equilibrada e de acordo com a Constituição.

Da mesma maneira, é dever do Estado, mesmo estando diante de situações legítimas de tratamento de dados pessoais, adotar medidas a fim de prevenir a ocorrência de danos aos titulares. Essa diretriz concretiza o princípio da prevenção, que reconhece a existência de riscos intrínsecos ao tratamento de dados pessoais e, portanto, exige uma postura proativa de mitigação desses riscos.

A aplicação do princípio da necessidade e de medidas de salvaguarda objetiva garantir o alcance do benefício pretendido a partir da divulgação do dado, com a exposição mínima e segura de dados pessoais. Para tal, deve-se, primeiramente, identificar o conjunto mínimo necessário de dados; e, posteriormente, verificar se há medidas de salvaguarda que protejam os dados e mitiguem os riscos aos titulares para alcance do mesmo benefício. Ambas serão explicadas a seguir.

IMPORTANTE

Após análise da necessidade e avaliação das salvaguardas que podem ser aplicadas para mitigar os riscos ao titular do dado, deve-se retomar o passo 4, realizando novamente a ponderação. Nesse momento, o agente deve avaliar se o novo conjunto de dados pessoais em análise favorecerá a divulgação.

a) Identificação do conjunto de dados pessoais necessários

Ao analisar a demanda, seja para atendimento a pedido de acesso à informação, seja para divulgação em transparência ativa, o agente público deve identificar o conjunto de dados pessoais necessários e indispensáveis para atingir ao benefício coletivo pretendido, especialmente quando considerado o risco concreto ao titular.

Essa avaliação deve considerar, entre outros aspectos:

- se todos os dados solicitados são necessários para atingir o interesse coletivo identificado;
- se é possível excluir campos, reduzir o nível de detalhamento ou apresentar informações de forma agregada sem causar prejuízo aos benefícios coletivos gerados, de modo a minimizar riscos ao titular;
- se a divulgação integral do dado é adequada, necessária e proporcional à finalidade pública pretendida.

A tabela a seguir traz alguns exemplos que podem auxiliar a análise a ser realizada.

Benefício coletivo identificado	Dado a ser divulgado (Indispensável)	Dado que não deve ser divulgado (Excessivo)
Fiscalização de gastos com pessoal, a partir de informações sobre a folha de pagamento de servidores públicos.	Nome completo do servidor, CPF descaracterizado (conforme padrão indicado na capítulo 5), cargo, lotação e remuneração bruta/líquida.	RG, endereço residencial, telefone pessoal, informações sobre empréstimos, e dados bancários.
Controle social de beneficiários de políticas assistenciais, para identificar recebimentos indevidos.	Nome do beneficiário, CPF descaracterizado (conforme padrão indicado na capítulo 5), valor do benefício e município de residência.	Dados de saúde ou vulnerabilidade específica, endereço e telefone pessoal, idade, raça e sexo (salvo se for requisito para o recebimento do benefício).
Controle social dos processos de licitação e contratos, para identificação de desvios ou casos de corrupção.	Nome ou razão social do contratado, CNPJ, objeto e valor do contrato.	Endereço pessoal de sócios e e-mails pessoais.
Acompanhamento de despesas com viagens a serviço pagas com recurso público.	Nome do viajante, CPF descaracterizado (conforme padrão indicado na capítulo 5), origem e destino, motivo da viagem, valor das diárias recebidas, valor da passagem.	Número do passaporte, detalhes de acompanhantes familiares ou fotos de caráter privado.
Controle social do acesso a cargos públicos por meio de concurso.	Nome do candidato, CPF descaracterizado (conforme padrão indicado na capítulo 5) ou número de inscrição, nota final e classificação no certame.	Endereço completo, nome da mãe, informações de heteroidentificação e limitações de capacidade (salvo se forem requisitos para acesso às vagas).

Ressalta-se que a minimização de dados a serem divulgados não pode ser utilizada com o intuito de restringir, desnecessariamente, o acesso à informação pessoal para proteção do evidente interesse público.

b) Aplicação de salvaguardas apropriadas

Identificado o conjunto mínimo de dados pessoais que podem ser divulgados, o órgão deve, ainda, verificar se existem salvaguardas capazes de preservar o conteúdo informativo essencial sem expor desnecessariamente dados pessoais. Sempre que houver alternativa menos invasiva apta a atender ao interesse público, preservando o conteúdo informativo essencial, esta alternativa deve ser priorizada.

Veja exemplos de situações e salvaguardas possíveis:

Medidas de salvaguarda	Descrição resumida	Exemplo de quando usar
Anonimização	Elimina identificadores diretos e indiretos, impedindo a identificação do titular.	Disponibilização de bases de dados de saúde ou educação para análises estatísticas, sem qualquer dado que permita identificar indivíduos.
Pseudonimização	Substitui ou separa identificadores, permitindo a identificação apenas com informações adicionais mantidas separadamente.	Disponibilizar informações sobre saúde pública substituindo nome, CPF ou número do cartão do SUS por um código, por exemplo Paciente A1234, enquanto a informação que relaciona esse código à pessoa real permanece armazenada separadamente e com acesso restrito.
Tarjamento de informações	Oculta de forma permanente informações em um documento, de modo a impedir sua visualização e recuperação.	Divulgação de processo administrativo disciplinar com tarjas em dados pessoais sensíveis.
Agregação	Agregação de dados individuais, apresentando-os de forma consolidada, de modo que representem um grupo ou conjunto.	Divulgação de quantitativos de pessoas beneficiárias de políticas públicas por região, faixa etária ou nível de ensino.
Certidões ou extratos	Resume informações essenciais, sem expor documentos completos.	Certidões de processos administrativos disciplinares sobre assédio sexual ou moral com principais informações.

Como já mencionado anteriormente, na pseudonimização, os dados pessoais deixam de ser atribuídos a um titular específico, salvo mediante o uso de informações adicionais mantidas separadamente. Isso não elimina a natureza pessoal dos dados nem os retira do âmbito de aplicação da LGPD. A anonimização, por sua vez, descaracteriza o dado como pessoal, desde que a reidentificação do titular não seja possível mediante meios técnicos razoáveis e disponíveis no momento do tratamento. Assim, o acesso à informação anonimizada ou pseudonimizada elimina ou reduz significativamente os riscos ao titular dos dados.

6. Registro da decisão final

A partir das informações geradas nas etapas anteriores, o órgão ou entidade deve tomar a decisão final quanto à possibilidade de divulgação da informação, ou da necessidade de restrição de acesso ao dado pessoal. A decisão final adotada deve ser motivada e registrada.

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 da intimidade, vida privada, honra e imagem das pessoas, 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 e se foram observados os princípios da necessidade e da prevenção, inclusive com a avaliação da adoção de meios alternativos menos invasivos.

Quando a decisão for pelo acesso parcial à informação demandada, em decorrência da aplicação do princípio da necessidade e da adoção de salvaguardas, o órgão ou entidade deverá explicitar os critérios adotados e indicar quais informações não foram entregues.

O registro da decisão deve ser realizado tanto na resposta a pedidos de acesso à informação formulados com base na Lei de Acesso à Informação (LAI), quanto no âmbito da definição do conteúdo a ser disponibilizado em transparência ativa. Tal registro evidenciará a análise realizada e os critérios determinantes para decidir pela divulgação ou pela restrição de acesso ao dado. Trata-se de documento comprobatório da atuação responsável do agente público.

Nos pedidos de acesso à informação, a decisão deverá ser registrada no sistema oficial utilizado para o tratamento dos pedidos de acesso à informação. Nas decisões relativas à transparência ativa, caberá a cada órgão ou entidade definir a forma de registro mais adequada, observados seus procedimentos internos e a necessidade de assegurar a rastreabilidade e a fundamentação da decisão.

Nos casos de disponibilização em transparência ativa, a elaboração de relatório de impacto à proteção de dados pessoais pode auxiliar a motivação da decisão a ser proferida pela autoridade competente, além de fortalecer a sua conformidade com a legislação de proteção de dados pessoais. A avaliação quanto à necessidade de elaboração do documento deve considerar as peculiaridades do caso concreto, em particular, a existência de alto risco às liberdades civis e aos direitos fundamentais dos cidadãos, observado o disposto nos art. 5º, XVII, e no art. 38, da LGPD.

ORIENTAÇÃO PARA REGISTRO DA DECISÃO SOBRE DIVULGAÇÃO DE DADOS PESSOAIS

O órgão ou unidade responsável deverá registrar a decisão de forma clara e fundamentada, contemplando, sempre que possível, os seguintes aspectos:

Dados pessoais envolvidos: descrever, de forma sucinta, os dados analisados, sua natureza (indicando, quando for o caso, a presença de dados sensíveis) e a relação do titular com o Estado no contexto da informação;

Interesse público: explicitar o interesse público geral e preponderante que está sendo considerado como fundamento para divulgação, indicando de

que maneira a disponibilização da informação pode contribuir para a coletividade;

Riscos ao titular: apontar os principais impactos negativos que a divulgação pode gerar ao titular dos dados, com avaliação qualitativa de sua probabilidade e gravidade;

Necessidade e proporcionalidade: demonstrar que os dados pessoais são necessários para atingir a finalidade pública pretendida, indicando, quando pertinente, a exclusão de informações excessivas e as medidas adotadas para mitigação de riscos (como agregação, anonimização ou restrição parcial);

Decisão: registrar a conclusão quanto à possibilidade de divulgação da informação (integral, parcial ou restrição de acesso), com fundamentação objetiva que evidencie a ponderação entre o interesse público e a proteção de dados pessoais.

Tabela de exemplos concretos de aplicação do teste de interesse público

Na sequência, apresenta-se uma tabela resumida de exemplos concretos da aplicação do Teste de Interesse Público, para a avaliação da possibilidade de divulgação de dados pessoais, destinada a ilustrar como a ponderação entre o interesse público na divulgação e o risco de dano ao titular pode conduzir a diferentes resultados decisórios, conforme as circunstâncias de cada caso.

Dado analisado	Tipo de Titular	Proximidade do titular com o Estado	Benefício coletivo com a divulgação do dado	Risco ao titular decorrente da divulgação	Decisão baseada na ponderação entre os direitos
Nome completo e remuneração de servidor público	Agente público	Relação alta	Alto: permite o controle social do uso de recurso público e a verificação de possível enriquecimento ilícito.	Baixo: risco à segurança e a fraudes.	Conceder o acesso, observado que o CPF deve ser descaracterizado, conforme padrão indicado no capítulo 5.
Nome completo e remuneração de pessoa que não é servidor público, nem presta serviço ao Estado	Particular	Relação inexistente ou muito baixa	Inexistente: não há recurso público envolvido.	Moderado: risco à segurança e de ocorrência de fraudes.	Negar o acesso, já que não há interesse coletivo preponderante.

Nome e CPF de beneficiário de política assistencial (Bolsa Família)	Particular - beneficiário de recurso público	Relação moderada	Alto: permite a fiscalização do uso de recursos públicos e a identificação de beneficiários indevidos.	Baixo: risco de estigmatização social devido à exposição de condição socioeconômica.	Conceder o acesso, observando que o CPF deve ser descaracterizado, conforme padrão indicado no capítulo 5.
Nome e CPF de beneficiárias de programa de proteção à vítima (violência contra a mulher)	Particular - beneficiário de recurso público	Relação moderada	Alto: pode viabilizar a avaliação da política pública, para verificação da efetividade e cobertura, por exemplo.	Muito alto: risco de reidentificação e localização da vítima, podendo resultar em violência física, revitimização, perseguição pelo agressor, exposição pública de situação de vulnerabilidade e agravamento de danos psicológicos.	Negar o acesso individualizado. É possível fornecer dados agregados ou anonimizados.
Matrícula funcional de servidor	Agente público	Relação alta	Alto, pois permite o cruzamento de dados e distinção de homônimos.	Muito baixo: risco residual de uso indevido para tentativas de fraude ou engenharia social, sem potencial relevante de dano quando desvinculado de outros dados pessoais.	Conceder o acesso.
Endereço residencial de servidor público	Agente público	Relação alta	Baixo: trata-se de informação da vida privada, sem relação entre o agente e o Estado.	Alto: risco à segurança do agente público e de sua família. Alto: risco de localização física do servidor e de seus familiares, podendo resultar em ameaças, perseguições, assédio presencial ou violência, especialmente em razão do exercício da função pública.	Negar o acesso
Prontuário médico de usuário do SUS	Usuário de serviço público	Relação baixa	Alto: pode viabilizar a avaliação da política pública de saúde, para verificação da efetividade e cobertura, por exemplo.	Alto: risco de discriminação social, profissional ou institucional em razão de condições de saúde; estigmatização; violação excessiva da intimidade; uso indevido das informações por terceiros (empregadores, seguradoras etc.).	Negar o acesso individualizado. É possível fornecer dados agregados ou anonimizados

Compromissos oficiais de ministro de Estado	Agente público em cargo de chefia	Relação alta	Alto: permite a verificação de potenciais conflitos de interesse relacionados à atuação do agente.	Baixo: possibilidade de uso das informações para antecipar compromissos e deslocamentos, podendo gerar riscos à segurança física da autoridade ou interferências externas.	Conceder o acesso integralmente, salvo exceções de segurança, que podem ser mitigadas com publicação após a realização do compromisso.

4.3. TRANSPARÊNCIA POR DESENHO

O roteiro decisório, apresentado neste capítulo, focou na análise de casos concretos, ou seja, de pedidos de LAI ou de análises sobre a publicação de informações em transparência ativa. No entanto, o órgão pode se adiantar a essas demandas e adotar medidas prévias para conciliar a transparência e proteção da intimidade, vida privada, honra e imagem. Para isso, podem ser utilizadas, desde a concepção, técnicas que tenham como objetivo facilitar a futura divulgação de informações públicas. A adoção desse conjunto de técnicas em políticas, sistemas, bases de dados, processos e rotinas se chama Transparência por desenho.

A proposta é de que os órgãos reflitam sobre questões como as seguintes:

- Como se planejar com antecedência para identificar dados cujo acesso deve ser restrito?
- Como adotar medidas prévias para tratá-los?
- É possível pensar desde o início na organização dos dados para que, no futuro, a transparência seja facilitada a partir da aplicação dos princípios da finalidade, adequação e necessidade?

Assim, atua-se proativamente para a conciliação entre transparência e proteção de dados pessoais. Sempre que possível, devem ser adotadas, de forma antecipada, técnicas de transparência por desenho, com o objetivo de viabilizar o acesso à informação de forma compatível com a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas.

A transparência por desenho consiste na incorporação - desde a fase de concepção de políticas públicas, de sistemas de informação, de bases de dados, de 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 restrição de acesso.

Deve-se observar, por exemplo, o princípio da necessidade. A coleta e o registro de infor-

mações em documentos, sistemas e bases de dados devem limitar-se ao mínimo de dados indispensáveis à implementação da política pública ou do processo administrativo. Dessa forma, é possível antecipar decisões sobre o que poderá ser divulgado, em que nível de detalhamento e com quais salvaguardas, evitando análises que ocorram apenas de forma reativa no momento da divulgação em transparência ativa ou do atendimento a pedidos de acesso à informação.

A transparência por desenho contribui para a aplicação harmônica da LAI e da LGPD, permitindo ampliar a transparência com controle de riscos e observância dos princípios da finalidade, adequação e necessidade.

Uma prática simples de transparência por desenho, por exemplo, é a de substituir a assinatura manuscrita pela assinatura eletrônica em documentos administrativos. A assinatura manuscrita é um dado pessoal que precisa ser protegido antes da divulgação, o que gera trabalho extra de tarjamento toda vez que o documento é solicitado ou publicado.

A seguir, serão apresentadas etapas importantes para a implementação da transparência por desenho, para organização de fluxos de trabalho, processos e sistemas para facilitar o acesso futuro à informação. Isso possibilitará a redução de decisões caso a caso e de retrabalho, assegurando maior previsibilidade na divulgação das informações e minimizando riscos de exposição indevida de dados pessoais.

Identificar processos que produzem informação de interesse coletivo e geral

O órgão deve identificar quais são os processos administrativos que geram informações diretamente relacionadas às obrigações legais de transparência ativa, além daqueles com informações mais demandadas pela sociedade.

Relaciona-se, a seguir, tipos de processos que são executados por todos os órgãos e entidades da Administração Pública, que geram informações de interesse coletivo e geral:

- Planejamento e execução orçamentária;
- Aquisição e contratação, inclusive a etapa de execução;
- Contratação de terceirizados;
- Repasses ou transferências de recursos financeiros;
- Planejamento e resultado de programas, projetos e ações;
- Processos de pessoal relativos a nomeações, designações, exonerações, dispensa etc.;
- Concessão de diárias e passagens;
- Concursos públicos;
- Governança institucional: atas e resoluções dos comitês internos de governança, programa de integridade etc.;
- Sanções administrativas aplicadas a pessoas, a empresas, a organizações não governamentais e a servidores públicos, no âmbito de cada órgão.

Além desses, é preciso identificar processos específicos, relativos às competências próprias de cada órgão ou entidade, que ensejam interesse social.

Revisar fluxos de trabalho e procedimentos

Após a identificação dos processos, deve-se, progressivamente, revisar os fluxos de trabalho e procedimentos adotados com o intuito de minimizar a coleta e o registro de informações. Devem ser mantidas apenas aquelas essenciais à execução do processo ou à implementação da política pública. Por exemplo, o instrumento contratual deve indicar o seu fiscal no âmbito do órgão. Nesse caso, é suficiente registrar o nome do servidor e sua matrícula SIAPE. Informações como RG, telefone ou e-mail pessoal, por exemplo, não precisam constar no documento. Se necessário, deve-se utilizar os dados institucionais de contato.

Em seguida, deve-se estruturar fluxos e procedimentos para realizar a segregação prévia de informações, de modo a distinguir os dados necessários ao controle social daqueles que demandam proteção. Por exemplo, para processos que exigem a anexação de documentos pessoais, documentos bancários etc., é possível armazenar essas informações separadamente.

Criar funcionalidades de consulta e extração de dados para ampla divulgação

Os sistemas eletrônicos devem permitir consultas ou extração de dados incorporando mecanismos técnicos de proteção, como mascaramento automático ou anonimização, de modo a viabilizar a divulgação posterior, sem necessidade de retrabalho para o tratamento de informações relativas à intimidade, à vida privada, à honra e à imagem.

Também é uma alternativa permitir a consulta ou extração de dados agregados, sem a individualização dos dados, inviabilizando o acesso às informações pessoais protegidas nos termos da LAI. Essa prática é especialmente relevante em bases relacionadas a beneficiários de políticas públicas ou em bases utilizadas para fins estatísticos ou de pesquisa. Possibilita-se a divulgação de dados como valores, quantitativos, localidade ou datas, sem identificação direta dos titulares.

5. ENTENDIMENTOS SOBRE A PUBLICIDADE DE DADOS PESSOAIS

Este capítulo reúne orientações práticas para o cumprimento do direito ao acesso à informação, garantindo a proteção necessária de dados pessoais, no contexto de documentos e atividades comuns à Administração Pública, como licitações, contratos, gestão de pessoas, benefícios sociais, auditorias, fiscalização e atividades regulatórias. O objetivo é apoiar os órgãos e entidades na identificação de quais dados pessoais devem ser divulgados e quais devem ser de acesso restrito.

As orientações deste capítulo refletem entendimentos consolidados da CGU, jurisprudência dos tribunais superiores e normas aplicáveis, servindo como ponto de partida para a análise das demandas e indicando o tratamento aplicável em regra. Quando o caso concreto se enquadrar nas hipóteses aqui apresentadas e inexistirem circunstâncias específicas aptas a justificar a restrição, a decisão será pela publicidade. Nas demais hipóteses, cada órgão deve avaliar as circunstâncias específicas, que podem justificar tratamento diverso do indicado como orientação geral.

DIVULGAÇÃO DE CPF EM RESPOSTA A PEDIDOS DE ACESSO À INFORMAÇÃO OU PARA CUMPRIMENTO DE OBRIGAÇÕES DE TRANSPARÊNCIA ATIVA

O CPF é um dado que permite a identificação única de uma pessoa natural. Sua divulgação, de forma parcialmente descaracterizada, associada ao nome completo do titular possibilita a desambiguação em caso de homônimos. O objetivo da descaracterização é evitar o risco de que os números de CPF sejam utilizados para a realização de fraudes. Dessa forma, publica-se apenas o mínimo necessário para fins de transparência.

O Poder Executivo federal adota um formato padrão para a descaracterização de números de CPF, baseado em previsão da Lei de Diretrizes Orçamentárias (LDO) para divulgação de dados de terceirizados. De acordo com essa norma, devem ser ocultados os três primeiros dígitos e os dois dígitos finais do número original, o que resulta no seguinte formato: ***.999.999-**. A LDO de 2010 foi a primeira a apresentar essa norma, que passou a ser repetida nas leis dos anos seguintes. Esse formato é adotado, por exemplo, no Portal da Transparência do Poder Executivo federal para quaisquer CPFs divulgados.

Cabe destacar, no entanto, que esse formato é sugerido para cumprimento da LAI, da Lei de Governo Digital (Lei nº 14.129/2021), da Lei Complementar nº 101/2000 (art. 48-A), e outras normas de transparência pública. Em determinados casos, faz-se necessária a publicação do número completo do CPF com o objetivo de conferir validade jurídica a atos administrativos, por exemplo. Ressalta-se que cada órgão deve analisar a sua realidade, para decidir pela divulgação integral ou parcial do CPF.

Acórdão nº 1511/2025 do Tribunal de Contas da União (TCU) - Plenário

Em 2025, o TCU analisou a remoção da publicação proativa de documentos anexados a convênios, contratos e outros termos de parceria registrados na plataforma Transferegov.br, de responsabilidade do Ministério da Gestão e Inovação em Serviços Públicos. A exclusão dos anexos objetivou proteger informações pessoais relativas à vida privada.

No julgado, o Tribunal entendeu que a divulgação de dados pessoais, como nome completo e CPF, é essencial para garantir a transparência e rastreabilidade na execução de recursos públicos, desde que sejam resguardados dados sensíveis e informações como endereço, telefone e e-mail pessoais.

O referido Acórdão determinou que o Transfere.gov deve publicar o número completo do CPF de pessoas naturais - agentes políticos, gestores e demais servidores, efetivos ou em comissão, envolvidos com a execução de recursos decorrentes de convênios e congêneres, assim como de representantes de empresas e entidades privadas que realizem convênios e congêneres ou firmem contratos administrativos com o Poder Público.

No caso do Transferegov.br, a decisão do TCU ponderou que a transparência se sobrepõe à proteção do CPF nos casos específicos indicados.

A decisão evidencia que os órgãos devem analisar, nas situações específicas, se o tarjamento parcial do CPF é adequado para suas especificidades.

DADOS PESSOAIS DE AGENTES PÚBLICOS

Agentes públicos estão sujeitos a um nível diferenciado de proteção de dados pessoais, em razão das funções que exercem. As informações relacionadas ao exercício de suas atribuições e ao uso de recursos públicos constituem informações de interesse público, essenciais ao controle da legalidade, moralidade e eficiência administrativa.

O Supremo Tribunal Federal, no julgamento da Suspensão de Segurança nº 3.902/SP, de relatoria do Ministro Ayres Britto, afirmou que dados como remuneração, cargos, funções e órgão de lotação constituem informações de interesse coletivo ou geral e que a publicação deles não viola a intimidade ou a vida privada, por estarem diretamente vinculados ao exercício da função pública. Além disso, permanecem protegidos os dados que possuem relação com o exercício da função pública, tais como aqueles sujeitos a sigilo legal específico e informações cuja divulgação possa comprometer a segurança institucional, da sociedade ou do próprio agente público. Nesses casos, a restrição deve ser feita de forma proporcional e deve ser devidamente motivada.

A seguir serão apresentadas considerações sobre a divulgação de dados de agentes públicos:

Tipo de informação	Regra geral de divulgação	Observação
Nome completo do agente público	Deve ser divulgado	O nome completo, sem outras informações associadas, não é protegido pelo art. 31 da LAI. É dado de identificação mínimo para qualquer relação do indivíduo com a sociedade.
Identificação do agente responsável por ato administrativo (assinatura de contrato, despachos, nota técnica, tomada de decisão)	Deve ser divulgada	Informação diretamente relacionada ao exercício da função pública. Ressalva: pode ser restringida se houver risco concreto à segurança ou à integridade física do servidor (exemplo: servidor em atividade policial ou servidor com medida protetiva).
Currículos e títulos acadêmicos de servidores públicos	Devem ser divulgados	Informação pessoal de interesse coletivo, conforme "Enunciado CGU nº 7/2023"4. São informações necessárias à avaliação da capacidade técnica para o exercício do cargo.
Cargo e função	Devem ser divulgados	Informação diretamente relacionada ao exercício da função pública
Lotação do servidor	Deve ser divulgada	Informação diretamente relacionada ao exercício da função pública Ressalva: pode ser restringida se houver risco concreto à segurança ou à integridade física do servidor (exemplo: servidor em atividade policial ou servidor com medida protetiva).
Matrícula funcional (SIAPE ou equivalente)	Deve ser divulgada	Informação diretamente relacionada ao exercício da função pública. Número pode ser divulgado de forma integral.
CPF	Deve ser divulgado	A divulgação deve ser realizada de forma descaracterizada, conforme padrão indicado no Guia.
Nome do servidor que realizou alguma ação em sistemas do Governo (com perfil de servidor)	Deve ser divulgado	Informação diretamente relacionada ao exercício da função pública.
E-mail funcional	Deve ser divulgado	O e-mail funcional de agentes públicos pode ser divulgado, por se tratar de dado relativo à função pública exercida. Nos casos em que o pedido de informação demanda a relação completa de e-mail dos servidores do órgão, por exemplo, é admitida a negativa em razão do risco de ataques cibernéticos em massa, que afete a segurança da infraestrutura tecnológica do órgão.
Remuneração	Deve ser divulgada	Informação pessoal de interesse coletivo.
Registro de frequência	Deve ser divulgado	Informação diretamente relacionada ao exercício da função pública.

4 Enunciado CGU n. 7/2023 - Títulos acadêmicos e currículos de agentes públicos.

Informações sobre currículos de agentes públicos, como títulos, experiência acadêmica e experiência profissional, são passíveis de acesso público, uma vez que são utilizadas para a avaliação da capacidade, aptidão e conhecimento técnico para o exercício de cargos e funções públicas.

Detalhes sobre descontos na folha de ponto (pensão alimentícia, empréstimos consignados)	Não deve ser divulgado	Informação relativa à intimidade, vida privada, honra ou imagem, sem relação com a função pública.
Assinatura manuscrita do servidor	Não deve ser divulgada	Informação desnecessária ao controle social e fiscalização da atuação pública.
Endereço residencial, telefone e e-mail pessoais	Não devem ser divulgados	Informação relativa à intimidade, vida privada, honra ou imagem, sem relação com a função.
Dados de saúde do servidor (atestados, carteira de vacinação)	Não deve ser divulgado	Informação relativa à intimidade, vida privada, honra ou imagem, sem relação com a função.

Observação: A tabela indica a regra geral de divulgação, no entanto, deve-se analisar, no caso concreto, se há alguma especificidade que ocasione riscos significativos ao titular do dado.

DADOS PESSOAIS CONSTANTES DE PROCESSOS SELETIVOS E DADOS DE FORMAÇÃO E EXPERIÊNCIA DE SERVIDORES E EMPREGADOS PÚBLICOS

A divulgação de dados pessoais constantes de processos seletivos e de informações relativas à formação e à experiência de servidores e empregados públicos deve observar o equilíbrio entre os princípios da publicidade e da proteção de dados pessoais. A transparência é legítima quando a divulgação for necessária ao controle social, à verificação da lisura dos certames e à avaliação da atuação estatal.

Podem ser divulgados, no âmbito dos processos seletivos, os dados indispensáveis à verificação da impessoalidade e do cumprimento das regras do certame, tais como lista de aprovados, notas dos aprovados, classificação final, critérios de avaliação e demais informações objetivas sobre os resultados.

Em relação aos servidores e empregados públicos, é legítima a divulgação de formação acadêmica, títulos, cargo, função, lotação, remuneração e histórico profissional relacionado ao exercício da função pública, por se tratar de informações de interesse coletivo, diretamente vinculadas à atuação estatal e ao uso de recursos públicos.

No caso de concursos públicos ou outros processos seletivos, é possível divulgar alguns dados pessoais sensíveis estritamente necessários à compreensão e à fiscalização do certame ou do processo de promoção funcional, quando expressamente previstos como critérios ou condicionantes de seleção ou progressão. Nesses casos, a divulgação deve restringir-se ao mínimo necessário para demonstrar o cumprimento das regras do edital ou do regulamento, como ocorre, por exemplo, com idade, raça ou gênero utilizados como critérios de ação afirmativa ou de enquadramento específico, vedada qualquer exposição excessiva ou desvinculada da finalidade pública.

Não devem ser divulgados, por outro lado, os dados pessoais inseridos na esfera estritamente privada e que não sejam necessários à transparência administrativa. Incluem-se, no caso de processos seletivos: endereço, telefone, e-mail, dados bancários e outros dados dos candidatos que não constituam critério de seleção. Da mesma forma, em rela-

ção a servidores e empregados públicos, permanecem protegidos: endereço residencial, contatos particulares (e-mail não institucional e telefone pessoal) e dados pessoais sem relação direta com o exercício da função ou com critérios objetivos de seleção ou promoção.

DADOS PESSOAIS EM PROCESSOS ADMINISTRATIVOS DISCIPLINARES

As informações constantes de processos administrativos disciplinares (PADs) concluídos, em tese, são públicas, ressalvadas aquelas protegidas por sigilo legal ou que envolvam dados pessoais relativos à intimidade, vida privada, honra e imagem das pessoas, protegidos nos termos da LAI. A divulgação é legítima por se referir a condutas funcionais praticadas no exercício da função pública, atendendo ao interesse coletivo no acompanhamento da apuração disciplinar das condutas de agentes públicos e ao princípio da publicidade administrativa.

A publicidade dos PADs varia conforme a fase do processo:

- **PAD em curso**: o acesso é restrito às partes diretamente interessadas, nos termos do art. 7º, § 3º, da Lei nº 12.527/2011 (LAI), que autoriza a restrição temporária quando a divulgação puder comprometer a apuração dos fatos ou a eficácia do procedimento. No âmbito do Poder Executivo federal, a restrição de acesso ao PAD em curso também se fundamenta na Lei nº 8.112/1990: o art. 150 assegura o sigilo necessário à elucidação dos fatos e o caráter reservado das atividades da comissão, 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.
- **PAD concluído**: em tese, é público, ressalvadas as informações protegidas por sigilo legal e as informações pessoais protegidas nos termos da LAI, devendo a divulgação observar os princípios da finalidade, necessidade e proporcionalidade.

O QUE DIZEM AS NORMAS?

Enunciado CGU nº 14/2016 – Restrição de Acesso a 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."

Enunciado CGU nº 3/2023 – Procedimentos disciplinares de militares.

Aplicam-se aos pedidos de acesso a processos administrativos disciplinares conduzidos no âmbito das Forças Armadas as mesmas regras referentes aos servidores civis, cabendo restrição a terceiros somente até o seu julgamento, nos termos do art.7º, parágrafo 3º, da Lei nº 12.527/2011, regula-

mentado pelo art. 20, caput, do Decreto nº 7.724/2012. Assim, os processos administrativos disciplinares de militares são passíveis de acesso público uma vez concluídos, sem prejuízo da proteção das informações pessoais sensíveis e legalmente sigilosas.

A tabela a seguir elenca dados divulgáveis e dados restritos em processos administrativos disciplinares:

Tipo de informação	Regra geral de divulgação	Observações
PAD em curso	Acesso restrito	Restrição temporária para preservar a apuração, conforme art. 7º, § 3º, da LAI.
PAD concluído	Deve ser divulgado	Publicidade voltada ao controle social da responsabilização funcional, ressalvadas as informações protegidas por sigilo legal e as informações pessoais protegidas pela LAI.
Nome do servidor que sofreu o PAD	Deve ser divulgado, após conclusão.	Informação vinculada ao exercício da função pública. Para PADs sobre assédio moral, sexual ou discriminação: não se deve divulgar o nome do servidor envolvido para processos arquivados ou quando não foi identificada a sua relação com a autoria dos fatos. Trata-se de proteção necessária à privacidade do servidor, para evitar a estigmatização e o estímulo à denunciação caluniosa.
Cargo, lotação e matrícula funcional do servidor que sofreu o PAD	Devem ser divulgados	Dados funcionais de interesse coletivo.
Descrição da infração	Deve ser divulgada	Deve ser objetiva e observar os princípios da finalidade, necessidade e proporcionalidade.
Tipo de sanção aplicada	Deve ser divulgada	Essencial para a transparência administrativa.
Dados de saúde, familiares ou bancários	Não devem ser divulgados	Informações da vida privada e dados pessoais sensíveis.
Dados pessoais de terceiros citados	Não devem ser divulgados	Devem ser protegidos, salvo previsão legal específica. Ressalta-se que deve ser tomado especial cuidado para que não sejam divulgadas informações que permitam a reidentificação da vítima, do/a denunciante e das testemunhas. Busca-se evitar a revitimização e a vinculação da vítima aos atos praticados contra si, preservando sua intimidade, além de reduzir a exposição das testemunhas para não desestimular seu depoimento por receio de retaliação.

Observação: A tabela indica a regra geral de divulgação, no entanto, deve-se analisar, no caso concreto, se há alguma especificidade que ocasione riscos significativos ao titular do dado.

BOA PRÁTICA

Recomenda-se que os órgãos instruam os PADs considerando que, após a conclusão, o processo é público. Recomenda-se estruturar o processo de modo a facilitar a identificação de hipóteses de sigilo legal e de informações pessoais protegidas nos termos da LAI, viabilizando a divulgação de forma rápida, segura e consistente, com redução de retrabalho e de riscos de exposição indevida. Sempre que necessário, deve ser preparada versão pública do PAD, com divulgação parcial e devidamente motivada.

DADOS PESSOAIS EM LISTAS DE CONTROLE DE ACESSO A PRÉDIOS PÚBLICOS

Os registros de entrada e saída de pessoas em prédios públicos são, em regra, passíveis de acesso público, por contribuírem para a transparência da atuação administrativa e para a prevenção de conflitos de interesse, tráfico de influência e outros riscos à integridade pública.

No entanto, como envolvem dados pessoais de visitantes, o acesso deve ser concedido de forma proporcional. Veja a seguir quais dados da lista de controle de acesso podem ser divulgados:

Tipo de informação	Exemplos de dados coletados	Regra geral de divulgação	Observações
Identificação	Nome completo; instituição pública ou privada que representa.	Deve ser divulgado.	Deve ser fornecido, pois é essencial para a transparência sobre encontros com agentes públicos.
Motivo da visita	Reunião, entrega de documentos, audiência etc.	Deve ser divulgado.	Deve incluir o nome e setor da pessoa visitada.
Horário de entrada e saída	Data e hora.	Deve ser divulgado.	Importante para a análise de padrões de visita.
Documento de identificação	RG, CPF, CNH ou equivalente.	Deve ser divulgado.	Preferencialmente, deve-se divulgar o CPF de forma descaracterizada, conforme padrão indicado no Guia. Se o CPF for divulgado, os demais números não precisam ser fornecidos. Caso sejam, também devem ser parcialmente tarjados. Não há, no entanto, formato padrão sugerido.
Foto	Capturada ou do documento.	Não deve ser divulgado.	Trata-se de dado pessoal de imagem.
Informações de contato	Telefone, e-mail.	Não deve ser divulgado.	Dados da vida privada não necessários para o fim de controle social.
Dados do veículo	Placa, modelo, cor.	Não deve ser divulgado.	Desnecessários para a finalidade de controle social.

Outros dados identificativos	Assinatura, biometria.	Não deve ser divulgado.	Devem ser protegidos por envolverem dados pessoais sensíveis.

Observação: A tabela indica a regra geral de divulgação, no entanto, deve-se analisar, no caso concreto, se há alguma especificidade que ocasione riscos significativos ao titular do dado.

O QUE DIZEM AS NORMAS?

Enunciado CGU nº 1/2023 - Registros de entrada e saída de prédios públicos.

Os registros de entrada e saída de pessoas em órgãos públicos, inclusive no Palácio do Planalto, são passíveis de acesso público, exceto quando as agendas sobre as quais eles se refiram forem classificadas por se enquadrarem em hipótese legal de sigilo ou estiverem sob restrição temporária de acesso à informação, nos termos do art. 7º, § 3º da Lei n. 12.527/11.

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.

É possível que esses dados tenham o acesso negado mediante decisão motivada, por exemplo quando se referirem a pessoas que se encontrem em condições especiais de proteção (refugiados, crianças e adolescentes, testemunhas, investigados em processo administrativo não concluído ou denunciantes). Nesses casos, a divulgação de tais informações pode acarretar prejuízos à intimidade, à vida privada, à honra ou à imagem, bem como comprometer a segurança institucional ou a eficácia das atividades do órgão, sendo legítima a adoção de medidas de restrição ou de acesso parcial da informação, nos termos da Lei nº 12.527/2011.

Boa prática

Recomenda-se que os órgãos e entidades públicas aprimorem seus sistemas de controle de acesso, de modo a viabilizar o fornecimento das informações passíveis de divulgação, preferencialmente por meio de campos segregados, mascaramento automático e mecanismos de anonimização, assegurando simultaneamente o direito de acesso aos registros de entrada e saída, sem a criação de obstáculos indevidos ao exercício do direito de acesso à informação, com divulgação parcial e devidamente motivada.

DADOS PESSOAIS EM PROCESSOS LICITATÓRIOS E CONTRATOS ADMINISTRATIVOS

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 e promover confiança social nas instituições públicas.

Editais, atas, contratos e aditivos devem ser publicados em portais oficiais e plataformas de transparência, ressalvadas as informações protegidas por sigilo legal ou os dados pessoais restritos.

O QUE DIZEM AS NORMAS?

Enunciado CGU nº 5/2023 - Sigilo de licitações, contratos e gastos governamentais

Informações sobre licitações, contratos e gastos governamentais, inclusive as que dizem respeito a processos conduzidos pelas Forças Armadas e pelos órgãos de polícia e de inteligência, são em regra públicas e eventual restrição de acesso somente pode ser imposta quando o objeto a que se referem estritamente se enquadrar em uma das hipóteses legais de sigilo.

A tabela a seguir apresenta os dados divulgáveis e dados restritos em licitações e contratos administrativos:

Tipo de informação	Exemplos de dados	Regra geral de divulgação	Observações
Identificação da empresa contratada	Razão social, nome empresarial, CNPJ, endereço	Deve ser divulgada	Dados de pessoas jurídicas não são dados pessoais e são indispensáveis ao controle social.
Representante legal da empresa	Nome completo e cargo	Deve ser divulgado	Informação necessária para identificar quem atua em nome da contratada.
CPF do representante legal	Número do CPF	Deve ser divulgado	Deve ser descaracterizado, conforme padrão indicado no capítulo 5.
Propostas e documentos técnicos	Preços, planilhas, cronogramas, metodologias	Deve ser divulgado	Essenciais para garantir a isonomia, a competitividade e a legalidade do certame.
Atas e decisões do processo	Julgamento, adjudicação, homologação	Deve ser divulgado	Atos administrativos públicos vinculados ao exercício da função pública.
Contratos e termos aditivos	Objeto, valores, prazos, cláusulas	Deve ser divulgado	Instrumentos de execução da despesa pública.

Notas fiscais e pagamentos	Valores, datas, empresa favorecida	Deve ser divulgado	Informação necessária à prestação de contas do gasto público.
Assinatura manuscrita	Imagem da assinatura	Não deve ser divulgada	Dado pessoal suscetível a fraude, sem relevância para o controle social.
Dados bancários da contratada	Conta, agência, chave PIX	Não devem ser divulgados	Informação desnecessária ao controle social.

Observação: A tabela indica a regra geral de divulgação, no entanto, deve-se analisar, no caso concreto, se há alguma especificidade que ocasione riscos significativos ao titular do dado.

O QUE DIZEM AS NORMAS?

Lei de Acesso à Informação (Lei nº 12.527/2011):

Art. 8º É dever dos órgãos e entidades públicas promover, **independentemente de requerimentos**, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

§ 1º Na divulgação das informações a que se refere o caput, deverão constar, no mínimo:

[...]

IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;

[...]

Lei do Governo Digital (Lei nº 14.129/2021):

Art. 29. Os dados disponibilizados pelos prestadores de serviços públicos, bem como qualquer informação de transparência ativa, são de livre utilização pela sociedade, observados os princípios dispostos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

§ 2º Sem prejuízo da legislação em vigor, os órgãos e as entidades previstos no art. 2º desta Lei deverão divulgar na internet:

[...]

V - as licitações e as contratações realizadas pelo Poder ou órgão independente;

VI - as notas fiscais eletrônicas relativas às compras públicas;

[...]

Lei de Licitações e Contratos Administrativos (Lei nº 14.133/2021):

Art. 5º Na aplicação desta Lei, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da **publicidade**, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da **transparência**, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as

disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

[...]

Art. 13. Os atos praticados no processo licitatório são públicos, ressalvadas as hipóteses de informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado, na forma da lei.

Parágrafo único. A publicidade será diferida:

I - quanto ao conteúdo das propostas, até a respectiva abertura;

II - quanto ao orçamento da Administração, nos termos do art. 24 desta Lei.

DADOS PESSOAIS EM PROCESSOS ADMINISTRATIVOS DE AUDITORIA, FISCALIZAÇÃO, CONTROLE, LICENCIAMENTOS E OUTORGAS

As informações constantes de processos administrativos de auditoria, fiscalização, controle, licenciamentos e outorgas são, em regra, públicas após a conclusão, ressalvadas as hipóteses de sigilo legal e a proteção de informações relativas à intimidade, vida privada, honra ou imagem.

Em linhas gerais, os processos de auditoria, fiscalização e controle no Poder Executivo federal visam garantir a legalidade, a eficiência e a integridade da atuação pública. A auditoria avalia riscos e resultados, a fiscalização verifica o cumprimento de normas e aplica sanções, e o controle coordena essas ações para corrigir falhas e aprimorar a gestão.

Já os processos de licenciamento e outorga são aqueles pelos quais o Estado autoriza, condiciona e regula o exercício de atividades privadas ou o uso de recursos e serviços públicos, visando proteger o interesse coletivo e assegurar o cumprimento de normas legais.

Pela natureza dos processos, evidencia-se que a sua publicidade é essencial para o controle social, a prestação de contas, a prevenção de irregularidades e o fortalecimento da integridade pública.

Para todos os casos, a extensão do acesso varia conforme a fase do procedimento:

- **Processos em curso**: o acesso é, em regra, restrito às partes diretamente interessadas, especialmente quando os documentos ainda possuem natureza preparatória. Por exemplo, partes envolvidas em um Processo Administrativo Disciplinar.
- **Processos concluídos**: com a edição da decisão final, o processo torna-se publicamente acessível, nos termos do art. 7º, §3º, da Lei nº 12.527/2011 e do art. 20 do Decreto nº 7.724/2012.

A presença de dados pessoais no processo não afasta a publicidade. Devem ser protegidas apenas as informações relativas à intimidade, vida privada, honra ou imagem que

não sejam necessárias ao controle social, ou dados submetidos a sigilo legal específico, como sigilo bancário ou fiscal. Nessas hipóteses, recomenda-se o acesso parcial da informação, com tarjamento de dados específicos e limitados.

Para os processos que resultam na aplicação de sanções, vale destacar o art. 29, inciso IX, §3º da Lei nº 14.129/ 2021 (Lei do Governo Digital), que traz a obrigação de sua publicação em transparência ativa. Isso inclui as sanções aplicadas a pessoas naturais.

> *Lei nº 14.129/2021*
>
> *Art. 29 [...]*
>
> ...
>
> *§ 2º Sem prejuízo da legislação em vigor, os órgãos e as entidades previstos no art. 2º desta Lei deverão divulgar na internet:*
>
> ...
>
> *IX - as sanções administrativas aplicadas a pessoas, a empresas, a organizações não governamentais e a servidores públicos;*
>
> ...

Citam-se algumas práticas consolidadas de transparência ativa na divulgação de informações decorrentes de processos de fiscalização e controle: o Ministério do Trabalho e Emprego (MTE) divulga o Cadastro de Empregadores que submeteram trabalhadores a condições análogas à escravidão ("Lista Suja"); a Controladoria-Geral da União (CGU), por meio do Portal da Transparência, divulga o Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), que traz dados sobre sanções administrativas que restringem o direito de participar de licitações ou celebrar contratos com a Administração Pública, incluindo sanções aplicadas a pessoas físicas; a CGU mantém ainda repositório público de relatórios de auditoria e fiscalização, redigidos desde a origem para divulgação, com a finalidade de ampliar a transparência e permitir o acompanhamento das ações de controle interno.

DADOS PESSOAIS SOBRE BENEFICIÁRIOS DE PROGRAMAS SOCIAIS

A divulgação de dados pessoais de beneficiários de programas sociais é, em regra, legítima e necessária, pois atende a um interesse público preponderante relacionado à transparência e ao controle social da aplicação de recursos públicos.

Os programas sociais consistem em transferências diretas de recursos públicos a cidadãos, voltadas à proteção social e redução da pobreza, como Bolsa Família, Benefício de Prestação Continuada (BPC), Auxílio Emergencial e outros. Por serem financiados com recursos públicos, algumas informações dos beneficiários são essenciais para garantir a correta execução das políticas públicas, viabilizar o controle social, prevenir irregularidades, assegurar o cumprimento dos critérios legais de elegibilidade e evitar fraudes, abusos e favorecimentos indevidos.

A divulgação dos dados de beneficiários não é irrestrita. Deve-se observar a necessidade, adequação e proporcionalidade da publicidade para a finalidade pretendida, de modo a evitar a exposição excessiva ou indevida de pessoas em situação de vulnerabilidade. Como regra, deve-se priorizar a divulgação de dados estritamente necessários ao controle social, para mitigação dos riscos ao titular do dado. O Portal da Transparência do Governo Federal adota modelo compatível com essas diretrizes, permitindo consultas públicas sobre beneficiários de programas sociais.

Em regra, são divulgadas as seguintes informações:

Tipo de informação	Regra geral de divulgação	Observações
Nome completo do beneficiário	Deve ser divulgado	Necessário para o controle social e a verificação de pagamentos. O nome dos beneficiários crianças e adolescentes não deve ser divulgado a terceiros não autorizados.
Nome do representante do beneficiário	Deve ser divulgado	Necessário para o controle social e a verificação de pagamentos.
Número de identificação social (NIS)	Deve ser divulgado	Necessário para o controle social e a verificação de pagamentos.
CPF	Deve ser divulgado	Deve ser descaracterizado, conforme padrão indicado no capítulo 5.
Município e Unidade da Federação	Deve ser divulgado	Informação relevante para análise territorial das políticas públicas.
Programa social	Deve ser divulgado	Permite identificar a política pública e seus critérios de elegibilidade.
Valores recebidos	Deve ser divulgado	Essencial para a transparência e fiscalização do gasto público.
Endereço residencial	Não deve ser divulgado	Informação da vida privada, sem relação com a finalidade de controle social.
Dados de contato	Não devem ser divulgados	Telefone e e-mail são dados pessoais da vida privada, desnecessários à transparência.
Informações socioeconômicas detalhadas	Não devem ser divulgadas	Podem gerar estigmatização e não são, em tese, necessárias ao controle social.
Dados sensíveis	Não devem ser divulgados	Incluem informações de saúde e deficiência, por exemplo.

Observação: A tabela indica a regra geral de divulgação, no entanto, deve-se analisar, no caso concreto, se há alguma especificidade que ocasione riscos significativos ao titular do dado.

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 respeitada 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 7.724/2012.

Embora a transparência pública seja a regra, a identificação nominal do beneficiário deve ser omitida ou anonimizada quando colocar em risco o titular ou a eficácia da política, como em dados de programas de proteção à vida (vítimas, testemunhas, mulheres em situação de violência, crianças, adolescentes).

DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES: CAUTELA REFORÇADA

A divulgação de dados pessoais de crianças e adolescentes exige cautela reforçada, sempre considerando o princípio do melhor interesse e as diretrizes estabelecidas nas normas que regem a proteção desse grupo. Nesse sentido, em atenção aos princípios da segurança e da prevenção (art. 6º, incisos VII e VIII, da LGPD), o órgão deve fazer uso de meios que reduzam a exposição de crianças e adolescentes, mediante, por exemplo, anonimização, concessão de acesso parcial, agregação de dados ou outras técnicas ou medidas de segurança.

Em atenção ao princípio da prevenção (art. 6º, VIII, da LGPD), a avaliação dos riscos deve ser mais rigorosa quando da divulgação de dados pessoais desse público. Devem ser considerados, por exemplo, possíveis prejuízos que possam afetar o desenvolvimento ou os direitos fundamentais das crianças e adolescentes.

A maior vulnerabilidade desse público também precisa ser considerada na ponderação entre a transparência e a privacidade. Em muitos casos, o controle social pode ser plenamente assegurado com a divulgação de informações estatísticas, anonimizadas ou desidentificadas, preservando-se os dados pessoais de crianças e adolescentes e garantindo a observância do princípio do melhor interesse.

DADOS DE ESTUDANTES BENEFICIÁRIOS DE BOLSAS E AÇÕES AFIRMATIVAS

A divulgação de informações sobre estudantes que recebem bolsas ou utilizam cotas é legítima e necessária. Como essas políticas envolvem o uso de recursos públicos para promover a ciência e a inclusão, a sociedade tem o direito de acompanhar sua execução.

Órgãos e instituições de ensino (como Universidades, Institutos Federais, CAPES e CNPq) devem divulgar os dados de beneficiários de bolsas de pesquisa, iniciação científica e auxílios de assistência (moradia e permanência). Essa prática segue o princípio da pu-

blicidade e permite verificar a correta aplicação das verbas. Em regra, as informações públicas são:

- Nome do bolsista ou beneficiário;
- Matrícula do estudante;
- CPF descaracterizado, conforme padrão indicado no capítulo 5;
- Instituição e programa de vínculo;
- Valor do benefício recebido.

Também é possível divulgar informações sobre estudantes beneficiários de ações afirmativas, como cotas raciais ou sociais. A possibilidade de divulgação deve ser avaliada no caso concreto, considerando a necessidade da divulgação para atender ao interesse público e ao controle social da política pública. A divulgação de dados individualizados pode ser legítima, ainda que envolva o tratamento de dados pessoais sensíveis, desde que seja necessária para essa finalidade e se restrinja às informações estritamente necessárias, permitindo verificar o cumprimento dos critérios de ingresso, prevenir e identificar fraudes, fortalecer a legitimidade das ações afirmativas e contribuir para seu aperfeiçoamento. O órgão deve observar os princípios da necessidade e da proporcionalidade. Sempre que suficientes para assegurar a transparência da política pública, devem ser privilegiadas informações agregadas.

No caso de estudantes crianças e adolescentes, em regra, o nome não deve ser divulgado. Nesses casos, deve-se divulgar o nome do responsável, quando a informação existir. No entanto, a demanda pela informação deve sempre ser avaliada no caso concreto para identificar eventual preponderância do interesse público e geral em relação à intimidade, vida privada, honra ou imagem de crianças e adolescentes.

IMPORTANTE

A divulgação deve sempre respeitar a privacidade. Não devem ser expostos dados sensíveis, como prontuários médicos, laudos de saúde ou detalhes íntimos da situação socioeconômica que possam gerar estigmatização.