Guia

Boas Práticas de Proteção de Dados Pessoais no STF

STF
SUPREMO TRIBUNAL FEDERAL

STF
SUPREMO TRIBUNAL FEDERAL

Supremo Tribunal Federal

Ministro Luís Roberto Barroso

Presidente

Ministro Edson Fachin

Vice-Presidente

Ministro Gilmar Mendes

Ministra Cármen Lúcia

Ministro Dias Toffoli

Ministro Luiz Fux

Ministro Alexandre de Moraes

Ministro Nunes Marques

Ministro André Mendonça

Ministro Cristiano Zanin

Ministro Flávio Dino

22/2/2024 - Composição atual. Foto: Fellipe Sampaio/STF

SUMÁRIO

APRESENTAÇÃO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 - LGPD) é um marco na defesa dos direitos fundamentais de privacidade e de proteção de dados. Ela se aplica a qualquer organização que realize atividades de tratamento de dados pessoais, independentemente do porte ou setor. Tratamento de dados diz respeito a qualquer operação realizada com dados pessoais, abrangendo ações como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão e extração. A Lei Geral de Proteção de Dados (LGPD) considera tratamento tanto as atividades realizadas em meios digitais quanto as feitas em meios físicos.

A LGPD se baseia em princípios como respeito à privacidade, à autodeterminação informativa, ao desenvolvimento econômico e tecnológico, à livre iniciativa, à defesa do consumidor, aos direitos humanos e à inviolabilidade da intimidade, honra e imagem. No Supremo Tribunal Federal (STF), lidar com dados pessoais faz parte do trabalho diário, seja na função jurisdicional – dados contidos em processos judiciais –, seja na função administrativa – gestão de recursos humanos, elaboração de contratos administrativos e utilização de sistemas, entre outras atividades. Por isso, os princípios e procedimentos da LGPD devem nortear nossas ações diárias. Todos nós, Ministros, servidores, colaboradores e estagiários, somos responsáveis pelo sucesso dessa missão.

O presente guia é um dos produtos do Grupo de Trabalho instituído pela Portaria STF nº 105/2024, para apoiar as atividades de adequação do Supremo Tribunal Federal às disposições da LGPD. Seu objetivo é para ajudar você a entender os princípios e práticas que garantem o uso responsável de dados pessoais, protegendo a privacidade e evitando riscos à segurança das informações. Diversos documentos auxiliaram a sua elaboração: Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado[1] e Guia Orientativo para Tratamento de dados pessoais pelo Poder Público[2], ambos da ANPD, Guia de Boas Praticas de Proteção de Dados para a Indústria[3] e guias da *Information Commissioner's Office* (ICO)[4].

Em complemento a esse Guia, recomendamos a consulta ao Glossário de Proteção de Dados Pessoais e Privacidade, elaborado pela Autoridade Nacional de Proteção de Dados (ANPD)[5].

---

[1] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/uia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

2 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf

3 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

4 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

5 https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd

1. INTRODUÇÃO À LGPD: ENTENDA O BÁSICO

1.1 Dado pessoal: o que é e por que importa?

Dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável (art. 5º, I, da LGPD). Isso inclui dados como nome, RG, CPF, gênero, local e data de nascimento, e-mail, número de telefone, entre outros.

Mesmo quando uma informação não menciona diretamente o nome de alguém, ela pode ser considerada um dado pessoal se permitir a identificação da pessoa. Por exemplo, o número de CPF ou de RG não precisa ser acompanhado do nome do titular para que essa informação esteja relacionada a uma pessoa específica. Do mesmo modo, o número de celular de um indivíduo pode ser usado para identificar uma pessoa se utilizado combinado com outros dados.

Mesmo dados públicos, como o número de inscrição na OAB do advogado, ou corporativos, como o número da matrícula de servidores e e-mail institucionais, são considerados dados pessoais e protegidos pela LGPD.

Como identificamos diretamente uma pessoa?

Um indivíduo é diretamente identificável quando possuímos informações que permitem sua identificação imediata, como seu nome completo e endereço

Exemplo:

Ana Clara Souza

Rua das Flores, 123, Apto 45, Jardim das Rosas, São Paulo/SP.

Um endereço de e-mail corporativo pode identificar diretamente o indivíduo (pois é um identificador exclusivo), bem como fornecer mais informações sobre o indivíduo (ou seja, onde ele trabalha).

Exemplo:

anaclara@stf.jus.br

Com isso, você pode identificar que uma pessoa chamada Ana Clara trabalha no STF.

Existe ainda uma categoria especial de dados pessoais: os dados pessoais sensíveis. São informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político; dado referente à saúde ou à vida sexual e dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II, da LGPD). Esses dados podem ser utilizados para finalidades discriminatórias e, por isso, seu tratamento requer um cuidado especial e só pode ocorrer em hipóteses específicas previstas na LGPD.

Os dados de crianças e adolescentes também exigem maior cuidado e devem seguir procedimentos específicos, na forma do art. 14 da LGPD. Em primeiro lugar, o tratamento desses dados deve ser realizado com o consentimento específico **e em destaque** dado por pelo menos um dos pais ou pelo responsável legal. Além disso, as informações sobre o tratamento dos dados deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

1.2 Tratamento de dados: o que isso significa na prática?

Tratamento de dados é qualquer operação realizada com informações pessoais, seja em meio digital ou físico (art. 5º, X, da LGPD). Isso inclui ações como:

- Coletar (ex.: preencher um formulário);
- Classificar (ex.: organizar dados em uma planilha);
- Utilizar (ex.: enviar um e-mail usando os dados fornecidos);
- Armazenar (ex.: guardar informações em arquivos digitais ou em papel);
- Eliminar (ex.: excluir documentos desnecessários).

Outras atividades, como transmitir, modificar ou compartilhar informações, também são formas de tratamento de dados pessoais (art. 5º, X, da LGPD).

Exemplos práticos no dia a dia do STF:

- ***Formulários de inscrição para eventos:***
  Quando divulgamos um formulário eletrônico para participação em um evento do STF, estamos coletando dados pessoais dos inscritos.
- ***Fichas cadastrais em papel:***
  Ao solicitar o preenchimento de uma ficha cadastral, mesmo que o documento seja arquivado fisicamente, ele também está sujeito às normas de proteção de dados.
- ***Pedidos de passagens ou diárias no sistema SEI:***
  Esses pedidos incluem informações pessoais, como nomes e documentos, configurando atividades de tratamento de dados.
- ***Elaboração de decisões judiciais:***
  Ao redigir uma minuta de decisão mencionando o nome das partes, ocorre o tratamento de dados pessoais.

Em todas essas situações, é essencial garantir o cumprimento da LGPD. Isso significa adotar práticas que protejam os dados pessoais, evitando usos indevidos e respeitando os direitos dos titulares.

FIQUE ATENTO!

Adote a política da mesa e telas limpas:

Guarde todos os documentos com dados pessoais em locais seguros, como gavetas ou armários trancados, quando não estiverem em uso.

Bloqueie ou desligue computadores, laptops e outros dispositivos eletrônicos ao se ausentar da mesa de trabalho.

Evite deixar anotações, post-its ou outros materiais com informações confidenciais em locais visíveis ou de fácil acesso.

Utilize procedimentos seguros para descartar documentos com dados pessoais, como trituradores de papel ou serviços de destruição de documentos.

FIQUE ATENTO!

Cuidados na redação de despachos e decisões

Quando estiver minutando um despacho ou decisão, evite incluir dados pessoais desnecessários, como nome das partes, endereço e números de documentos. Adote como estratégia não mencionar dados pessoais, nem mesmo as iniciais dos nomes. Se for indispensável, use termos como "recorrente A", "primeiro recorrente", "autor", "réu" e assim por diante.

Preservar a identidade dos titulares de dados e garantir os seus direitos à privacidade e à proteção de dados requer o nosso esforço conjunto. Lembre-se que os dados em decisões judiciais são públicos e, em regra, estarão disponíveis para sempre na internet.

1.3 Agentes de tratamento: quem são e o que fazem?

De acordo com a LGPD, são agentes de tratamento de dados pessoais o controlador e o operador.

O **controlador** é a pessoa ou entidade responsável pelas decisões referentes ao tratamento de dados pessoais. Esse agente pode realizar diretamente o tratamento ou delegá-lo a um operador. No STF, o controlador é União, representada pelo Tribunal e dirigida por sua Alta Administração (art. 13 da Resolução STF nº 759/2021).

O papel do controlador é central, pois a LGPD lhe atribui obrigações específicas, como:

- Elaborar relatórios de impacto à proteção de dados pessoais (art. 38);
- Comprovar que o consentimento obtido dos titulares atende às exigências legais (art. 8º, § 2º);
- Comunicar à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidentes de segurança (art. 48).

Nos casos em que dois ou mais agentes participam da definição dos elementos essenciais do tratamento de dados, configura-se **controladoria conjunta**. As decisões conjuntas podem ser tomadas a partir de uma atuação comum, em que há verdadeira atuação conjunta, ou por meio de decisões convergentes que, apesar de distintas, são complementares.

O **operador** é a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, no nosso caso, em nome do STF (art. 18 da Resolução STF n° 759/2021). A principal diferença entre controlador e operador está no poder de decisão: enquanto o controlador define as finalidades e meios do tratamento, o operador atua exclusivamente dentro dos limites determinados pelo controlador. Além disso, as responsabilidades por reparação de danos decorrentes de atos ilícitos no tratamento de dados são diferentes para o controlador e o operador, conforme os arts. 42 a 45 da LGPD.

FIQUE ATENTO!

A definição de cada pessoa ou organização como controlador ou operador é definido com base nas atividades realizadas em cada processo de trabalho. Isso significa que uma mesma organização pode atuar como operador em um contexto e como controlador em outro, dependendo da situação específica.

Embora a relação entre os agentes de tratamento seja frequentemente formalizada em contratos, a identificação efetiva de cada agente (controlador ou operador) depende das funções que cada um exerce na prática. O aspecto mais importante para determinar se uma organização está atuando como controladora é o poder de decisão que ela possui sobre os elementos essenciais do tratamento, como a definição da finalidade do tratamento, da natureza dos dados pessoais tratados e a duração do processo.

Exemplo:

O STF contrata uma empresa para desenvolver e implementar uma solução de inteligência artificial para realizar o tratamento automatizado de decisões com base em um banco de dados gerido pelo próprio STF.

A empresa realizará as operações necessárias para viabilizar a entrega da solução de IA, seguindo as instruções fornecidas pelo STF e estabelecidas em contrato.

Nessa hipótese, o STF é o controlador e detém obrigações legais específicas em face dos titulares e da ANPD, conforme previsto na LGPD. A empresa é a operadora, uma vez que realiza o tratamento dos dados exclusivamente conforme as instruções fornecidas pelo controlador.

Também existe a figura do **suboperador**, que é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador. A relação direta do suboperador é com o operador e não com o controlador. No entanto, independentemente dos acordos entre o operador e o suboperador, ambos podem, conforme o caso, desempenhar a função de operador e ser responsabilizados perante a ANPD.

Exemplo: Ferramenta web e serviço de armazenagem

O STF coleta de dados de saúde dos seus servidores, como aqueles referentes aos exames admissionais e demissionais, bem como os coletados em consultas realizadas pela equipe da SIS. Todavia, a guarda e a coleta desses dados são realizadas com o uso de ferramenta web de uma empresa contratada pelo Tribunal.

O STF determina quais dados quer coletar, por quanto tempo pretende mantê-los e que tipo de processamento pretende fazer com esses dados e, portanto, ele é controlador.

A empresa contratada, por sua vez, toma algumas decisões técnicas sobre protocolos de acesso, de armazenagem, de backup, de proteção contra invasões, todas de acordo com as especificações de segurança exigidas pelo STF. Essa empresa é operadora.

Percebendo que o volume de dados a ser guardado é superior à capacidade de seus bancos de dados internos, a empresa, com a autorização do STF, contrata a Microsoft para serviço de armazenagem dos dados em nuvem. A Microsoft é uma suboperadora.

FIQUE ATENTO!

Não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento.

Além dos agentes de tratamento, o **encarregado de proteção de dados** também exerce papel relevante para a proteção de dados. Conforme o artigo 41 da LGPD, o controlador de dados deverá indicar um encarregado pelo tratamento de dados pessoais, que será o canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados – ANPD. No STF, a **Secretaria de Relações com a Sociedade** é a unidade encarregada de proteção de dados (Portaria STF nº 104/2024).

No exercício de suas funções, o encarregado tem a importante responsabilidade de promover e disseminar a cultura da proteção de dados pessoais dentro da organização. Isso inclui atividades como receber solicitações dos titulares dos dados e da ANPD, adotar as providências necessárias e orientar os funcionários e contratados sobre as práticas adequadas para garantir a proteção das informações pessoais.

Por atuar como ponto de contato entre os titulares dos dados e a ANPD, é fundamental que as informações de contato do encarregado de dados estejam sempre acessíveis para o público interno e externo, conforme exigido pelo § 1º do art. 41 da LGPD. No STF, essas informações estão disponíveis no Portal LGPD[6].

[6] https://portal.stf.jus.br/lgpd/

2. CUMPRINDO A LGPD: PASSO A PASSO PARA A CONFORMIDADE

2.1 Princípios fundamentais

Toda operação de tratamento de dados pessoais deve estar em conformidade com os princípios estabelecidos no artigo 6º da LGPD.

a) Boa-fé objetiva

O tratamento de dados deve ser pautado nos ditames éticos e morais.

b) Finalidade

O tratamento de dados deve visar propósitos legítimos, específicos e claros ao longo de todo o processo. Se a finalidade for alterada durante o tratamento, ela não deve ser incompatível com os objetivos iniciais.

No setor público, o tratamento de dados pessoais deve atender a uma finalidade pública, na persecução do interesse público com o objetivo de executar as competências legais ou cumprir as atribuições institucionais do serviço público, conforme previsto no art. 23 da LGPD.

Portanto, o tratamento de dados pessoais pelo Poder Público deve estar sempre associado a uma finalidade pública, que seja:

- legítima, ou seja, lícita e compatível com o ordenamento jurídico, além de estar amparada em uma base legal que autorize o tratamento;
- específica, ou seja, a finalidade deve permitir delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais;
- explícita, ou seja, expressa de forma clara e precisa; e
- informada, ou seja, disponibilizada em linguagem simples, acessível e facilmente compreensível para o titular dos dados.

O princípio da finalidade limita o uso posterior dos dados pessoais. Ou seja, qualquer uso secundário dos dados só pode ser realizado para finalidades compatíveis com a finalidade original. Para avaliar essa compatibilidade, devem ser considerados os seguintes aspectos:

- o contexto e as circunstâncias relevantes do caso concreto;
- se há conexão fática ou jurídica entre a finalidade original e a que fundamenta o tratamento posterior;
- a natureza dos dados pessoais, adotando-se posição de maior cautela quando abrangidos dados sensíveis;
- as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos;
- o interesse público e a finalidade pública específica do tratamento posterior, bem como o seu vínculo com as competências legais dos órgãos ou entidades envolvidos.

Por fim, quanto aos dados públicos, o art. 7º, § 3º, da LGPD autoriza o seu tratamento, desde que observadas a finalidade, a boa-fé e o interesse público que justifiquem a sua utilização. O tratamento posterior desses dados só pode ser realizado se observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na lei.

c) Adequação

O tratamento deve ser compatível com as finalidades informadas ao titular.

d) Necessidade

O tratamento de dados deve se restringir ao mínimo necessário para cumprir suas finalidades, abrangendo apenas os dados que sejam pertinentes, proporcionais e adequados. Em outras palavras, esse princípio exige que se colete a menor quantidade possível de dados pessoais. Assim, é essencial verificar se as informações normalmente coletadas são realmente necessárias para as finalidades pretendidas, não sendo permitida a coleta de dados sem um propósito específico e legítimo identificado para o tratamento.

O princípio da necessidade aplica-se também após a coleta de dados, impondo que se avalie se são necessários tratamentos posteriores daqueles dados, como o armazenamento e o processamento.

Exemplo: Dados coletados para elaboração de contrato administrativo

O STF contrata, por licitação, uma empresa para prestação de serviço de limpeza. Para firmar o contrato, tanto o representante da empresa quanto o servidor público que assinará o contrato fornecem os seus dados, como nome, profissão, CPF, RG, estado civil e endereço residencial. Para dar publicidade à contratação da empresa, o contrato é divulgado no portal do STF.

É possível que dados como estado civil e endereço residencial não sejam necessários para a identificação dos responsáveis pela contratação e para viabilizar o exercício do controle social sobre a atividade do órgão público. Assim, a fim de limitar o tratamento ao mínimo necessário para a realização de suas finalidades, o ideal é não coletar esses tipos de dados.

e) Livre acesso

Os titulares dos dados têm o direito de consultar, gratuitamente, a forma e a duração do tratamento, bem como a integralidade de seus dados pessoais, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento.

f) Qualidade dos dados

Os dados dos titulares devem ser exatos, claros, relevantes e atualizados.

g) Transparência

Devem ser disponibilizadas aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

O art. 9º da LGPD delimita as informações que devem ser disponibilizadas aos titulares, entre as quais:

- forma, duração e finalidade específica do tratamento;
- identificação e informações de contato do controlador;
- informações sobre o uso compartilhado de dados e a finalidade;
- responsabilidades dos agentes que realizarão o tratamento; e
- direitos do titular, com menção explícita aos direitos contidos no art. 18.

Além dessas informações, a organização deve divulgar a identidade e as informações de contato do encarregado (art. 41, § 1º).

Exemplo: Princípio da transparência no setor público

Uma pessoa tem seus dados coletados pela recepção de um órgão público para fins de segurança patrimonial e dos servidores. Para atender a outros dispositivos legais e dar publicidade a atos do órgão, caso essa pessoa realize uma reunião com uma autoridade, seu nome poderá ser divulgado na agenda pública da autoridade, salvo eventual restrição legal.

Em geral, essa pessoa deverá ser informada das finalidades que justificam a coleta e o tratamento, incluindo a de que parte ou a totalidade deles poderá ser divulgada para atender normas específicas que tratem de divulgação de agenda pública. Entre outras possibilidades, essas informações podem constar da política de privacidade ou documento equivalente, disponibilizada na página do órgão público na internet.

h) Segurança

Os dados pessoais devem ser protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão por meio de medidas técnicas e administrativas.

i) Prevenção

Devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

j) Não discriminação

O tratamento de dados não deve ser realizado para fins discriminatórios, ilícitos ou abusivos.

k) Responsabilização e prestação de contas

O agente deve adotar medidas eficazes e deve ser capaz de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e a eficácia dessas medidas.

Os princípios da legislação são fundamentais e devem nortear todos os processos de tratamento de dados ao longo de todo o tratamento. Assim, antes mesmo de iniciar uma operação envolvendo dados pessoais, a pessoa deve levar em consideração algumas questões:

- Todos os dados pessoais que irei coletar são necessários para a minha operação?
- Eu irei violar algum direito do titular com a minha operação de tratamento de dados?
- O titular foi informado sobre os usos que farei dos dados?
- Eu consigo possibilitar o acesso do titular a informações sobre seus dados pessoais?
- Onde e como irei guardar os dados?
- Os dados que estou tratando estão seguros?
- A finalidade que eu inicialmente estabeleci foi finalizada? Eu, ainda, preciso de todos os dados que coletei inicialmente?
- A finalidade inicial foi alterada ao longo do tratamento?

2.2 Quando o tratamento de dados é permitido?

O art. 7º da LGPD lista as 10 hipóteses de bases legais que devem fundamentar o tratamento de dados pessoais não sensíveis:

BASES LEGAIS (art. 7º da LGPD)

- **Consentimento** (inciso I).
- **Cumprimento de obrigação legal ou regulatória pelo controlador** (inciso II) – essa base legal não se restringe às obrigações que decorrem de leis federais, estaduais e municipais, abarcando obrigações decorrentes de atos infralegais, tais como decretos, portaria, instruções normativas, entre outros.
- **Execução de políticas públicas pela Administração Pública** (inciso III).
- **Realização de estudos por órgão de pesquisa** (inciso IV).
- **Execução de contrato** (inciso V) – o titular deve fazer parte do contrato.
- **Exercício regular de direitos em processo judicial, administrativo ou arbitral** (inciso VI).
- **Proteção da vida ou da incolumidade física do titular ou de terceiros** (inciso VII).
- **Tutela da saúde** (inciso VIII) – deve ser realizada por profissionais de saúde, serviços de saúde ou autoridade sanitária.

- **Legítimo interesse** (inciso IX) – não pode ser aplicada quando prevalecerem direitos e liberdades fundamentais do titular, tais como: o direito à vida, à igualdade, à dignidade – que exijam a proteção dos dados pessoais.
- **Proteção do crédito** (inciso X).

Já as hipóteses que autorizam o tratamento de dados pessoais sensíveis estão previstas no art. 11 da LGPD:

BASES LEGAIS DADOS SENSÍVEIS (art. 11 da LGPD)

- **Consentimento específico e destacado** (inciso I).

Quando o dado for indispensável para (inciso II):

- **Cumprimento de obrigação legal ou regulatória pelo controlador** (alínea a).
- **Execução de políticas públicas pela Administração Pública** (alínea b).
- **Realização de estudos por órgão de pesquisa** (alínea c).
- **Exercício regular de direitos em contrato, processo judicial, administrativo ou arbitral** (alínea d).
- **Proteção da vida ou da incolumidade física do titular ou de terceiros** (alínea e).
- **Tutela da saúde** (alínea f) – deve ser realizada por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- **Prevenção à fraude e à segurança do titular** (alínea g).

Algumas bases legais apresentam maiores desafios e reflexões e serão examinadas de forma mais aprofundada.

a) Consentimento

De acordo com o art. 5º, XII, da LGPD, o consentimento é definido como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica". Além disso, no caso de dados sensíveis, o consentimento deve ser fornecido "de forma específica e destacada, para finalidades específicas" (art. 11, I, da LGPD).

Dessa forma, a autorização do titular deve ser clara e intencional, permitindo-lhe entender exatamente para que seus dados serão utilizados. A autorização tácita e as finalidades genéricas são proibidas. O consentimento deve envolver uma escolha real entre autorizar ou recusar o tratamento, com a possibilidade de revogação a qualquer momento. Caso o titular não tenha a liberdade de retirar o consentimento a qualquer momento, essa base legal não será válida (art. 8º, § 5º, da LGPD).

Por essas características, em muitas situações, o consentimento não será a base legal mais adequada para o tratamento de dados pessoais pelo Poder Público, especialmente quando o tratamento for necessário para cumprir obrigações legais ou desempenhar atribuições institucionais. Nesses casos, o órgão ou entidade pública exerce prerrogativas estatais típicas, o que cria uma relação desigual em que o titular não tem condições de manifestar sua vontade livremente sobre o uso de seus dados pessoais.

Apesar disso, o consentimento pode ser utilizado como base legal em algumas circunstâncias no contexto do Poder Público, desde que o uso dos dados não seja compulsório e a atuação estatal não se baseie em prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais.

Exemplo de uso do consentimento no Poder Público

No contexto do STF, o consentimento pode ser obtido quando são promovidos eventos abertos ao público, como seminários ou palestras. Nesses casos, ao coletar dados pessoais de inscrição, como e-mail e telefone, para enviar materiais do evento ou pesquisas de satisfação, o STF deve garantir que o consentimento seja explícito e informado, de forma que o titular saiba exatamente que esses dados serão usados para essa finalidade específica e possa revogar o consentimento a qualquer momento.

b) Legítimo interesse

A base legal do legítimo interesse autoriza o tratamento de dados pessoais de natureza **não sensível** quando necessário ao atendimento de interesses legítimos do controlador ou de terceiros, desde que não prevaleçam os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 7º, IX, da LGPD). **Portanto, a base legal não é aplicável ao tratamento de dados pessoais sensíveis**.

Por ser uma base legal mais flexível, sua utilização exige uma análise cuidadosa de proporcionalidade. É necessário equilibrar, de um lado, os interesses do controlador ou de terceiros no uso dos dados pessoais e, de outro, os direitos e as legítimas expectativas do titular. Além disso, conforme o art. 18, § 2º, da LGPD, o titular tem o direito de se opor ao tratamento de seus dados fundamentado no legítimo interesse, caso os requisitos legais não sejam cumpridos.

No âmbito do setor público, o uso do legítimo interesse é ainda mais restrito. Em particular, a sua utilização não é apropriada quando o tratamento de dados pessoais é realizado de forma compulsória ou quando for necessário para o cumprimento de obrigações e atribuições legais do Poder Público.

Nessas situações, não é possível realizar uma ponderação legítima entre as expectativas dos titulares. Por isso, recomenda-se que órgãos e entidades públicas, em geral, evitem recorrer ao legítimo interesse. Bases legais mais apropriadas, como a execução

de políticas públicas ou o cumprimento de obrigações legais, são preferíveis para fundamentar o tratamento de dados pessoais nessas condições.

Exemplo: Segurança da informação

Entidade pública realiza tratamento de dados pessoais de seus servidores com a finalidade de garantir a segurança dos sistemas de informação utilizados. Isso inclui ações como viabilizar a autenticação de usuários e prevenir que softwares maliciosos criem vulnerabilidades na rede interna.

Como esse tratamento de dados não está relacionado ao exercício de prerrogativas estatais típicas, é possível fundamentá-lo na base legal do legítimo interesse. Para isso, é imprescindível atender aos requisitos estabelecidos na LGPD, especialmente a necessidade de realizar uma ponderação entre os interesses da entidade pública e os direitos e as legítimas expectativas dos titulares dos dados. Além disso, é fundamental adotar medidas para assegurar a transparência do tratamento, garantindo que os titulares sejam devidamente informados sobre a finalidade e os procedimentos envolvidos.

c) Execução de políticas públicas

O inciso III do art. 7º da LGPD estabelece que a administração pública pode realizar "o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres". Por sua vez, em relação aos dados sensíveis, o art. 11, II, b, refere-se ao "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos".

FIQUE ATENTO!

O art. 11, I, b, da LGPD, não faz referência às políticas públicas instituídas em ajustes contratuais. Por isso, no caso de tratamento de **dados sensíveis** pelo Poder Público, a base legal é mais restrita, uma vez que limitada a políticas públicas previstas em "leis e regulamentos", sem incluir contratos, convênios ou instrumentos congêneres.

Essa base legal é aplicável não apenas ao Poder Executivo, mas também os Poderes Legislativo e Judiciário, desde que estejam atuando no exercício de funções administrativas.

Em suas funções administrativas, o STF poderá tratar dados pessoais necessários à execução de políticas públicas, por exemplo, quando coleta informações referentes a pessoas com deficiência ou mobilidade reduzida, para fins de cumprimento da Lei nº 13.146/2015 (Lei Brasileira de Inclusão).

2.3 O interesse público no tratamento de dados pessoais?

O interesse público refere-se a ações e decisões que têm como objetivo atender às necessidades e promover os benefícios da coletividade, garantindo o bem-estar social. O art. 23 da LGPD estabelece que o tratamento de dados pessoais por pessoas jurídicas de direito público deve ser direcionado ao cumprimento de sua finalidade pública, sempre alinhado à persecução do interesse público e voltado para a execução de competências legais ou o desempenho de atribuições do serviço público. Para isso, o Poder Público deverá obedecer aos seguintes requisitos:

- Informar as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.
- Nomear um encarregado de dados pessoais.

3. BASES LEGADAS: COMO GERENCIAR O PASSADO?

Bases legadas são os dados pessoais coletados antes da entrada em vigor da LGPD, quando ainda não estavam sujeitos às condições de legitimidade para o tratamento de dados previstas pela lei. O art. 63 da LGPD estabelece que: *"A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados"*. No entanto, a ANPD ainda não publicou diretrizes específicas sobre a adequação das bases legadas.

Embora não seja necessário descartar todos os dados recolhidos antes da nova legislação, é recomendável que as organizações promovam ajustes em suas bases de dados para assegurar a conformidade com a legislação atual. Esse processo deve incluir:

- **Revisão das finalidades originais:** À luz do princípio da finalidade, é importante verificar se os dados coletados antes da vigência da LGPD ainda atendem a um propósito legítimo e válido. Caso contrário, a manutenção desses dados deve ser reconsiderada.
- **Avaliação da necessidade:** Com base no princípio da necessidade, a organização deve identificar quais dados legados são indispensáveis para seus objetivos atuais. Dados que não são mais relevantes devem ser eliminados, reduzindo riscos e garantindo o respeito à privacidade dos titulares.

4. ARMAZENAMENTO E ELIMINAÇÃO DE DADOS COM SEGURANÇA

Os princípios de proteção de dados estabelecidos no art. 6º da LGPD são parâmetros essenciais que devem orientar todo o processo de tratamento de dados pessoais. Esses princípios devem ser observados em todas as etapas, desde a coleta até o armazenamento e eventual eliminação das informações.

Após a definição inicial sobre como os dados serão coletados e a identificação da base legal que fundamenta seu tratamento, é imprescindível implementar processos internos para garantir a manutenção contínua das condições de legitimidade dos dados coletados. Esses processos devem assegurar que os dados sejam armazenados de forma segura, utilizados de maneira adequada e eliminados quando não forem mais necessários, em conformidade com os princípios da finalidade, necessidade e segurança.

O armazenamento de dados pessoais deve observar os seguintes parâmetros:

- **PRINCÍPIO DA FINALIDADE E DA PRESTAÇÃO DE CONTAS**: Todas a unidades do STF devem saber quais dados possui, por quanto tempo eles serão necessários e para qual(is) finalidade(s) é utilizado, devendo o agente de tratamento ser capaz de apresentar uma justificativa para seu armazenamento.
- **PRINCÍPIO DA FINALIDADE**: O tratamento de dados deve ter propósitos legítimos, específicos e explícitos ao longo de todo o ciclo de vida dos dados. Não é permitido armazenar dados sem um objetivo claro e legítimo.
- **PRINCÍPIO DA NECESSIDADE**: Deve haver uma supervisão permanente das atividades de tratamento que permita identificar quando a coleta de determinados dados deixa de ser necessária e quando eles devem ser excluídos.
- **PRINCÍPIO DA NECESSIDADE**: Dados coletados inicialmente que não são estritamente necessários para o desempenho daquela atividade devem ter sua utilização reduzida ao máximo. Quando possível, deve-se adotar técnicas como anonimização ou pseudonimização.
- **PRINCÍPIO DA ADEQUAÇÃO E DA TRANSPARÊNCIA**: Se a finalidade do tratamento for alterada durante o período de armazenamento, e os dados não puderem ser excluídos, o titular deve ser informado sobre a mudança ou ter acesso fácil a essas informações.
- **PRINCÍPIO DA NECESSIDADE E DA QUALIDADE DOS DADOS**: Dados armazenados por longos períodos devem ser revisados para garantir que permaneçam atualizados e confiáveis. Telefone e endereço, por exemplo, são dados que podem ficar desatualizados com rapidez. deve-se solicitar a atualização ao titular ou reavaliar a necessidade de mantê-los.
- **PRINCÍPIO DA SEGURANÇA**: Devem ser adotadas medidas de segurança adequadas para proteger os dados contra acessos não autorizados e possíveis vazamentos.

Alguns dos mecanismos que podem ser utilizados para garantir a segurança da informação durante o processo de armazenamento de dados são:

- **Controles de acesso:** Implementação de autenticação robusta, como senhas fortes e autenticação multifator, para limitar o acesso apenas a pessoas autorizadas.
- **Criptografia:** Uso de técnicas de criptografia para proteger dados sensíveis tanto no armazenamento quanto durante a transmissão.
- **Monitoria e auditoria:** Estabelecimento de processos de monitoramento contínuo e auditorias regulares para identificar vulnerabilidades e mitigar riscos de segurança de forma proativa.

Já a **eliminação** refere-se à exclusão de um dado ou de um conjunto de dados armazenados em banco de dados. É o encerramento do ciclo de vida do dado.

Os dados devem ser eliminados nas seguintes situações:

- **Finalidade atingida:** Quando os dados não forem mais necessários para os fins específicos que motivaram sua coleta.
- **Solicitação do titular:** O titular dos dados tem o direito de solicitar sua eliminação, conforme previsto no art. 18, IV e VI, da LGPD.
- **Cessação de obrigações legais:** Quando não houver mais necessidade de retenção dos dados para atender a obrigações legais ou regulatórias.

5. INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS: COMO EVITAR E COMO AGIR?

Em primeiro lugar, é importante considerar que nem todo incidente de segurança envolve dados pessoais. De acordo com a ANPD, um incidente de segurança com dados pessoais é "qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais" (art. 3º, XII, do Regulamento de Comunicação de Incidente de Segurança da ANPD).

5.1 Medidas preventivas

Para mitigar os riscos e reduzir impactos de incidentes de segurança com dados pessoais, é essencial adotar medidas preventivas, entre as quais destacamos:

- **Políticas e capacitação:** criar, revisar e comunicar diretrizes considerando melhores práticas para assegurar a proteção dos dados pessoais, bem como promover capacitação contínua dos colaboradores sobre práticas de segurança e de proteção de dados.
- **Gestão de acessos:** restringir acessos a pessoas autorizadas e revogá-los quando desnecessários.
- **Autenticação forte:** utilizar senhas complexas, autenticação multifator (MFA) e segregação de funções.
- **Criptografia, anonimização e pseudonimização:** avaliar a utilização de recursos de criptografia, anonimização e pseudonimização quando necessário.
- **Minimização e ciclo de vida dos dados:** coletar apenas as informações estritamente necessárias, revisando e eliminando dados desatualizados ou desnecessários periodicamente.
- **Metodologia *privacy by design* e *by default*:** incorporar a preocupação com a privacidade e com a proteção de dados em todas as fases dos projetos desenvolvidos pela organização, desde a concepção até a sua implementação.
- **Manutenção e atualização contínua:** manter sistemas, aplicativos e ferramentas de segurança sempre atualizados, bem como realizar testes de intrusão e auditorias internas regulares.

5.2 Avaliação do incidente de segurança

Mesmo com a adoção de medidas preventivas, incidentes de segurança envolvendo dados pessoais podem ocorrer. O vazamento de dados é uma das ocorrências mais conhecidas, sendo caracterizado pela exposição indevida de informações do titular a terceiros. Esse tipo de incidente pode resultar em fraudes, tentativas de golpes, uso indevido dos dados e até mesmo sua comercialização ilegal.

De acordo com o art. 48 da LGPD, o controlador deverá comunicar a ANPD e os titulares de dados quando o incidente de segurança puder acarretar **risco ou dano relevante** aos titulares. Nesse contexto, a identificação do risco é uma etapa essencial: ao tomar ciência de um incidente, o agente de tratamento deve avaliar internamente a extensão do problema, a natureza, a categoria e a quantidade de dados pessoais afetados, bem como as consequências concretas e prováveis do incidente.

O art. 5º do Regulamento de Comunicação de Incidente de Segurança da ANPD estabelece que "o incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios":

- dados pessoais sensíveis;
- dados de crianças, de adolescentes ou de idosos;
- dados financeiros;
- dados de autenticação em sistemas;
- dados protegidos por sigilo legal, judicial ou profissional; ou
- dados em larga escala.

Além disso, o art. 5º, § 1º, do Regulamento da ANPD indica que "o incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade".

A elaboração de documentação contendo a avaliação interna do incidente, as medidas tomadas e a análise de risco é essencial, à luz do princípio de responsabilização e prestação de contas.

5.3 Comunicação à ANPD e aos titulares de dados

Dada a gravidade de cenários envolvendo incidentes de segurança, a ANPD recomenda que os controladores comuniquem os eventos mesmo quando houver dúvida sobre a relevância dos riscos e danos. Subavaliações comprovadas podem ser interpretadas como descumprimento da legislação de proteção de dados pessoais.

A comunicação à ANPD deverá ocorrer no prazo de até três dias úteis, contendo informações detalhadas e documentos, como o relatório do incidente de segurança, que auxiliem na análise do evento, dos riscos e das medidas adotadas. O art. 6º do Regulamento de Comunicação de Incidente de Segurança da ANPD especifica quais informações e documentos deverão estar contidas na comunicação do incidente.

A comunicação aos titulares também deve ocorrer no prazo de até três dias úteis, contados do conhecimento pelo controlador de que o incidente afetou dados pessoais. A comunicação deve ser feita em linguagem simples e acessível e, sempre que possível, deve ser individualizada. Quando não for possível a comunicação direta e individualizada aos titulares de dados, o controlador deverá comunicar a ocorrência do incidente pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.

A ANPD disponibiliza um passo a passo para a comunicação desses incidentes.

5.4 Gestão de incidentes de segurança no STF

No STF, a IN nº 267/2022 institui o Processo de Gestão de Incidentes de Segurança da Informação, que se aplica também a incidentes de segurança relacionados à proteção de dados. A Coordenadoria de Segurança Cibernética da Secretaria de Tecnologia e Inovação (CSEC/STI) é responsável por receber, analisar, classificar, tratar e reportar os incidentes, além de fornecer subsídios para o Comitê de Segurança da Informação e para o Comitê Executivo de Proteção de Dados (CEPD) para tomada de ações ou decisões gerenciais.

O CEPD e o Encarregado pelo Tratamento de Dados Pessoais devem ser prontamente informados sobre incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais. Compete ao CEPD, conforme o art. 6º-A da IN nº 267/2022, comunicar os incidentes à ANPD e aos titulares, seguindo as diretrizes da Instrução Normativa e do Regulamento de Comunicação de Incidente de Segurança da ANPD.

Assim, ao detectar ou suspeitar de um incidente de segurança envolvendo dados pessoais, a unidade do Tribunal deve notificar a CSEC/STI, detalhando o ocorrido. Em

seguida, a área técnica deve informar o incidente ao CEPD e ao encarregado, conduzindo uma análise criteriosa para avaliar o alcance da falha, o impacto potencial sobre os titulares e as possíveis causas.

Com base nessa avaliação, devem ser implementadas medidas corretivas para conter a exposição, reforçar controles e eliminar vulnerabilidades. Caso a análise interna conclua que o incidente apresenta risco ou dano relevante aos titulares, o CEPD procederá à comunicação imediata à ANPD e aos titulares afetados.

5.5 Passo a passo: como agir em caso de incidente de segurança com dados pessoais

1. Identificação e notificação inicial:

- Ao detectar ou suspeitar de um incidente de segurança, o gestor da unidade, qualquer servidor ou colaborador deverá notificar a CSEC/STI com os detalhes iniciais.

2. Análise preliminar e comunicação ao CEPD e ao encarregado:

- A CSEC/STI deve comunicar, imediatamente, o CEPD e o encarregado de dados.
- A CSEC/STI deve iniciar a análise sobre o alcance do incidente e seu impacto potencial, além de identificar as causas e vulnerabilidades envolvidas.
- A CSEC/STI deve identificar o grau de severidade do evento ocorrido. Caso a severidade do incidente seja classificada como crítica ou elevada, o CSI deve ser comunicado, para apoio e recomendações de tratamento.

3. Comunicação à ANPD e aos titulares (se aplicável):

- Caso identificado que o incidente pode acarretar risco ou dano relevante aos titulares, o CEPD deverá comunicar a ANPD e os titulares de dados, em até três dias úteis.

4. Plano de ação após a comunicação do incidente

- Elaboração de um plano de ação para corrigir possíveis falhas e evitar que novos incidentes venham a ocorrer.
- Análise das medidas técnicas adotadas no âmbito da tecnologia da informação.
- Atualizar políticas e processos de trabalho para prevenir novos incidentes.

6. COMPARTILHAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

O compartilhamento de dados pessoais ocorre quando órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas. Esse compartilhamento deve sempre respeitar os princípios de proteção de dados pessoais e destinar-se a finalidades específicas de execução de políticas públicas ou cumprimento de atribuições legais, conforme disposto no art. 26 da LGPD.

Em geral, o compartilhamento de dados pelo STF deverá atender aos seguintes requisitos:

- **Formalização e registro:** a Autoridade Nacional de Proteção de Dados (ANPD) recomenda a instauração de processo administrativo que documente a motivação para o compartilhamento. É importante que o compartilhamento seja formalizado por meio de instrumentos como contratos, convênios ou atos equivalentes, nos quais deve constar a base legal que autoriza a operação.
- **Objeto e finalidade:** os dados pessoais a serem compartilhados devem ser claramente definidos, limitando-se ao mínimo necessário para atender à finalidade pretendida, em conformidade com o princípio da necessidade. A finalidade deve ser específica e detalhada, indicando com precisão a iniciativa, ação ou programa a ser executado, ou a atribuição legal que será cumprida por meio do compartilhamento. Deve haver compatibilidade entre a finalidade original da coleta e a finalidade do compartilhamento.
- **Duração do tratamento:** o instrumento que formaliza o compartilhamento deve especificar o período de duração do uso compartilhado dos dados. Deve-se também indicar se há a possibilidade de conservação dos dados após o término do tratamento ou se eles devem ser eliminado.
- **Transparência e direitos dos titulares:** é fundamental garantir que os titulares dos dados tenham acesso a informações claras, precisas e de fácil compreensão sobre o compartilhamento realizado, incluindo orientações sobre como exercer seus direitos.

A LGPD veda ao Poder Público a transferência de dados pessoais a entidades privadas, exceto nas seguintes situações:

- **Execução descentralizada de atividade pública:** Quando a transferência for necessária para a execução descentralizada de uma atividade pública, exclusivamente para esse fim específico e determinado, em conformidade com a Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI).
- **Dados acessíveis publicamente:** Quando os dados forem de acesso público, respeitando as disposições da LGPD.
- **Previsão legal ou respaldo contratual:** Quando houver previsão legal para a transferência ou se a operação for respaldada por contratos, convênios ou instrumentos similares.
- **Prevenção de fraudes e proteção da segurança:** Para a prevenção de fraudes e irregularidades, ou para proteger a segurança e a integridade do titular dos dados, desde que o tratamento para outras finalidades seja vedado.

7. COMO ADEQUAR CONTRATOS À LGPD?

Com a entrada em vigor da LGPD, é essencial revisar e adequar todos os contratos e aditivos contratuais para assegurar conformidade com as novas exigências legais.

A definição do papel de cada pessoa envolvida em um determinado processo é feita a partir da avaliação de cada atividade, analisando quem tem o poder de decisão sobre os tratamentos realizados. A inclusão de cláusulas contratuais é importante para estabelecer as obrigações de cada parte e definir as instruções sobre procedimentos a serem adotados, como em casos de incidentes de segurança.

Além disso, a definição contratual dos papéis dos agentes de tratamento pode ser importante aspecto para a redução da exposição do controlador. Tal fato decorre da maior carga de responsabilidade que o controlador possui em relação à comprovação do cumprimento com os termos da legislação, assim como na garantia dos direitos dos titulares. Por esse motivo, o controlador tem papel estratégico na definição do operador, sendo o contrato um instrumento importante para a definição das obrigações dos operadores e os limites da atuação dos subcontroladores.

FIQUE ATENTO!

A definição do papel ocupado por cada pessoa envolvida naquele determinado processo é feita a partir da avaliação de cada atividade. Ou seja, uma organização pode desenvolver o papel de operador em determinado tratamento que envolve outra organização e, em outro processo, esses papéis podem ser invertidos.

A relação entre os agentes de tratamento de cada tratamento, muitas vezes, é definida contratualmente, mas a efetiva identificação de cada agente será determinada pelas funções desempenhadas por cada um. O que é essencial para determinar se uma organização está atuando como controladora dos dados é o poder de decisão sobre os elementos essenciais do tratamento, como a definição da finalidade do tratamento, da natureza dos dados pessoais tratados e a duração do processo.

Se o operador agir além das determinações do controlador quanto aos elementos essenciais do tratamento, ele passa a atuar como verdadeiro controlador. Dessa forma, as responsabilidades do controlador inicial são transferidas para o operador, que deverá cumprir todas as obrigações previstas para o controlador (art. 42, § 1º, I, da LGPD).

Nesse sentido, destacamos os deveres de cada um dos agentes de tratamento, assim como aqueles comuns aos dois:

Deveres comuns aos agentes de tratamento

- Conformidade com os princípios da LGPD.
- Implementação de medidas de segurança técnicas e organizacionais.
- Registro de operações de tratamento de dados pessoais.
- Observância das regras de transferências internacionais.

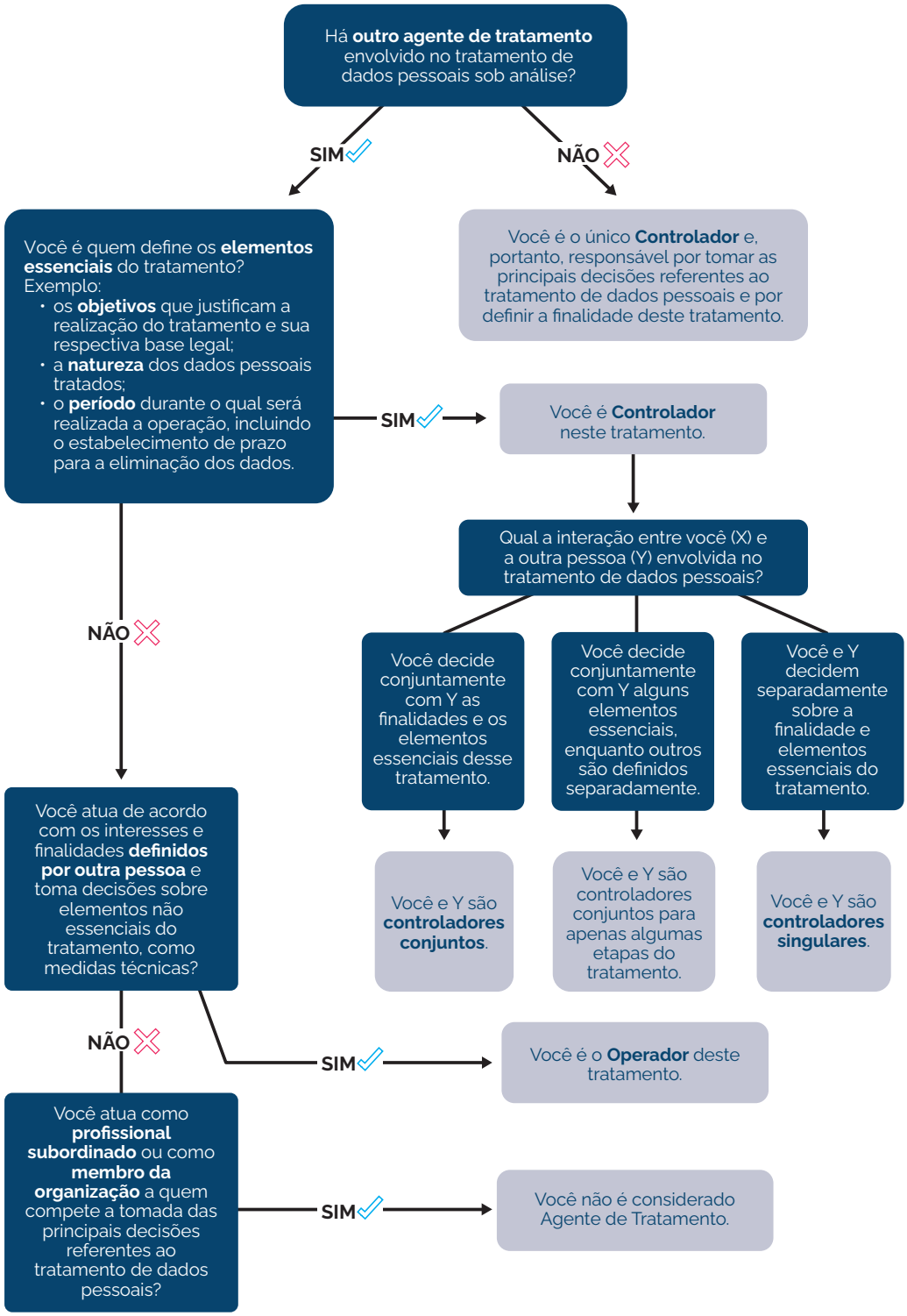
Obrigações dos operadores

- Cumprir as instruções do controlador sobre o tratamento de dados.
- Notificar incidentes de segurança ou possível violação de proteção de dados ao controlador.
- Reparar os danos causados em razão do exercício de atividade de tratamento de dados pessoais, quando este descumprir com suas obrigações ou não seguir as orientações do controlador.

Obrigações dos controladores

- Manutenção do ônus da prova de que o consentimento do titular foi obtido em conformidade com a LGPD.
- Observância dos direitos dos titulares.
- Comunicação de incidentes de segurança que possam acarretar risco ou dano relevante à ANPD e aos titulares afetados.
- Elaboração de Relatório de Impacto à Proteção de Dados.
- Nomeação de encarregado de dados.
- Implementação de programa de governança em privacidade com os requisitos previstos no art. 50, § 2º.

Para auxiliar a aplicação dos conceitos de controlador e operador, a ANPD divulgou o seguinte fluxograma no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado:



Fonte: Autoridade Nacional de Proteção de Dados, Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, Brasília, 2022, p. 25.

Embora a responsabilização dos agentes de tratamento seja avaliada contextualmente pela ANPD, a elaboração de cláusulas contratuais pode auxiliar a definir o regime das atividades e as responsabilidades de cada parte. De acordo com o Guia da ANPD, os pontos que podem ser definidos contratualmente incluem: o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos, e os direitos, obrigações e responsabilidades relacionadas ao cumprimento da LGPD.

Recomenda-se que os contratos incluam cláusulas que proíbam a contratação de suboperadores sem a prévia autorização do controlador, além de vedar o compartilhamento de dados pessoais com terceiros que não estejam diretamente envolvidos na relação contratual. Caso seja necessário contratar outro operador de dados, é essencial garantir que este agente esteja sujeito às mesmas condições acordadas para o operador original, incluindo a possibilidade de auditorias para assegurar o cumprimento dos termos contratuais.

Assim, sugerimos que a elaboração de cláusulas contratuais considere os seguintes tópicos:

- Duração das atividades de tratamento.
- Indicação de agentes de tratamento.
- Finalidades específicas do tratamento de dados.
- Vedação à utilização de dados pessoais sem ciência ou autorização da controladora.
- Exigência de adequação das partes do contrato à LGPD.
- Vedação ao compartilhamento de dados pessoais e obrigatoriedade de notificação à parte caso o compartilhamento seja necessário.
- Obrigação de registro de informações.
- Obrigação de implementação de medidas técnicas e administrativas que garantam a segurança dos dados tratados.
- Possibilidade de realização de auditorias para demonstração de cumprimento da legislação.
- Deveres de confidencialidade.
- Periodicidade de atualização de informações do contrato.
- Hipóteses de transferência de dados.
- Obrigatoriedade de elaboração de plano de incidentes envolvendo dados pessoais.
- Procedimentos de destruição e devolução de dados pessoais.
- Obrigatoriedade de notificação em caso de determinações oficiais que obriguem o fornecimento de dados pessoais.

8. COMO GARANTIR OS DIREITOS DOS TITULARES?

A LGPD assegura uma série de direitos para os titulares de dados. O exercício desses direitos é feito pelo **FalaBR da Ouvidoria do Supremo. A Secretaria de Relações com a Sociedade (SRS)**, como unidade encarregada responsável pelo tratamento de dados pessoais, é quem responde a essas solicitações. Para garantir respostas completas, precisas e adequadas ao titular de dados, a SRS poderá requisitar informações e documentos de diferentes unidades do Tribunal. Além disso, quando necessário, a solicitação poderá ser encaminhada a outras unidades especializadas para o devido tratamento.

A Resolução STF nº 838/2024 estabelece os procedimentos para o recebimento e tratamento dessas solicitações de dados pessoais no Supremo Tribunal Federal. Para mais detalhes, **acesse a Resolução**[7].

Confira os direitos previstos nos arts. 8º, 18 e 20 da LGPD:

- **Acesso** facilitado aos dados são tratados e para quais finalidades.
- **Confirmação** da existência de tratamento.
- **Correção** de dados incompletos, inexatos ou desatualizados.
- **Anonimização, bloqueio** ou **eliminação** de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
- **Eliminação** dados pessoais tratados com consentimento, salvo exceções legais.
- **Portabilidade** dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com regulamentação da ANPD, observados os segredos comercial e industrial.
- **Revogação do consentimento** concedido anteriormente para o tratamento dos dados.
- **Informação** das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
- **Informação** sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- **Revisão** de decisões automatizadas.

[7] https://api-atosnormativosprd.azurewebsites.net/api/normativo/apresentacao/E7fpbpABvUtUZJHiGUQ1

9. LEI DE ACESSO À INFORMAÇÃO E LEI GERAL DE PROTEÇÃO DE DADOS: COMO COMPATIBILIZAR?

O direito à informação e o direito à proteção de dados pessoais são direitos fundamentais expressamente previstos na Constituição Federal de 1988, regulamentados, respectivamente, pela Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI) e pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

No setor público, o processo de adequação à LGPD tem suscitado muitas dúvidas sobre como equilibrar a disponibilização pública de informações pessoais. Enquanto a LGPD exige cautela e análise de riscos antes da divulgação de dados pessoais, a LAI estabelece que a publicidade é a regra, permitindo o sigilo apenas em situações excepcionais. A análise dessas situações envolve uma ponderação entre, de um lado, o direito à privacidade e o direito à proteção de dados pessoais e, de outro, o direito à informação sobre as atividades do Poder Público.

A própria LAI já traz caminhos para essa ponderação. Isso porque o art. 31 contempla a proteção de informações pessoais, atribuindo a elas acesso restrito, independentemente de classificação de sigilo, pelo prazo de até 100 anos. A sua divulgação poderá ser autorizada nas seguintes hipóteses:

- consentimento expresso da pessoa a que elas se referirem; e
- quando as informações forem necessárias para:
  - prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
  - realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
  - cumprimento de ordem judicial;
  - defesa de direitos humanos; ou
  - proteção do interesse público e geral preponderante.

Nesse contexto, a ANPD recomenda que a análise sobre a disponibilização de informações ao público leve em consideração também os princípios da proteção de dados. Em termos práticos, é necessário realizar uma avaliação sobre os riscos e os impactos para os titulares dos dados pessoais bem como sobre as medidas mais adequadas para mitigar possíveis danos decorrentes do tratamento de dados pessoais.

O princípio da necessidade também é um guia importante nessa análise. De um lado, deve-se exigir o mínimo de dados pessoais do requerente para atender à sua solicitação, conforme o art. 10, § 1º da LAI. Por outro lado, a administração pública deve avaliar quais dados pessoais devem ser disponibilizados para o cumprimento do pedido de acesso à informação[8].

Nesse sentido, a ANPD indica que uma possível salvaguarda a ser adotada é a limitação da divulgação àqueles dados efetivamente necessários para se alcançar os propósitos legítimos e específicos em causa, observados o contexto do tratamento e as expectativas legítimas dos titulares. A título de exemplo, em cumprimento à decisão proferida pelo STF, a divulgação da remuneração individualizada de servidores públicos federais é realizada sem a apresentação completa de números como o CPF e a matrícula do servidor. A restrição de acesso a essas informações mitiga os riscos aos titulares de dados pessoais, sem, no entanto, comprometer a finalidade de garantia de transparência e de controle social sobre as despesas públicas.

O **princípio da finalidade** também desempenha um papel essencial na compatibilização entre proteção de dados e direito à informação. Esse princípio visa garantir que a disponibilização de informações públicas não seja usada para finalidades diferentes daquelas que fundamentaram sua disponibilização. Do mesmo modo, ele reforça a segurança do requerente, garantindo que os dados pessoais fornecidos em um pedido de acesso à informação não sejam utilizados para outros fins que não os necessários para atender ao pedido[9].

[8] Bioni, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. In: Cadernos Técnicos da CGU, vol. 1. pp. 8-19, 2022

[9] Bioni, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. In: Cadernos Técnicos da CGU, vol. 1. pp. 8-19, 2022

10. ORIENTAÇÕES PRÁTICAS E PRINCIPAIS DÚVIDAS

Cada área do Tribunal possui um contexto específico de tratamentos de dados pessoais. Entretanto, na Roda de Conversas realizada pelo Grupo de Trabalho com unidades do STF, algumas dúvidas sobre como agir em conformidade legal surgiram em mais de uma ocasião.

O presente capítulo deve ser lido em conjunto com o restante do Guia para melhor compreensão das orientações.

10.1 A coleta do consentimento para utilizar dados pessoais

Um dos pontos mais abordados por diversas áreas foi acerca da necessidade de coletar consentimento para uso de dados pessoais, seja de servidores, terceirizados ou cidadãos no geral. Conforme destacado no item 2.2, o consentimento é uma entre várias bases legais e possui aplicabilidade restrita para casos específicos que comportam os requisitos legais.

Nesse contexto, muitas vezes o consentimento não é necessário, e o servidor deve procurar o seu gestor e/ou o Encarregado do Tribunal para que seja avaliada a necessidade da coleta do consentimento, que pode já estar prevista no registro das atividades de tratamento de dados pessoais da sua secretaria.

Outras bases legais estão enumeradas nos arts. 7° e 11 da LGPD. Para auxiliar na identificação da base legal mais adequada, recomenda-se consultar o item 2.2, no qual são apresentados exemplos das bases legais previstas na legislação.

10.2 Dados pessoais em pedidos de acesso à informação

Muitas unidades do STF são responsáveis por receber e responder pedidos de acesso à informação com base na LAI que demandam a divulgação de dados pessoais de ministros, servidores, partes de processos judiciais em curso e/ou arquivados, etc.

Não é possível, no presente momento, criar uma regra geral que possa ser aplicada a todos os possíveis contextos de pedidos de acesso à informação, uma vez que os pedidos podem variar nos tipos, origem e utilizações possíveis.

Assim, é recomendado que exista uma análise junto à Assessoria Jurídica e ao Encarregado sobre os pedidos que envolvam dados pessoais para mapear todos os possíveis riscos e medidas de mitigação.

10.3 Contratação de sistemas e empresas com acessos a dados pessoais

Muitas áreas realizam suas atividades com sistemas de suporte e/ou parte dos processos é realizada por empresas contratadas, resultando em acessos a dados pessoais de servidores, partes dos processos, advogados, entre outros.

Para evitar o uso indevido desses dados pelas empresas contratadas, é necessário que todos os contratos possuam cláusulas contratuais específicas para a relação de agentes de tratamento, que podem ser: entre dois controladores OU entre um Controlador (o Tribunal) e um Operador (a empresa).

No processo SEI nº 007163/2024, foram disponibilizados modelos de cláusulas a serem inseridas nos contratos celebrados pelo Tribunal. Os modelos foram elaborados pela Secretaria de Relações com a Sociedade e pelo Grupo de Trabalho de Adequação à LGPD (Portaria nº 105/2024).

Além disso, é importante que existam processos internos para a verificação da adequação à LGPD dessas empresas antes da sua contratação, a fim de mitigar riscos.

CONCLUSÃO

A proteção de dados pessoais no STF é uma responsabilidade compartilhada entre todas as unidades do Tribunal, sendo essencial garantir que cada etapa do tratamento esteja em conformidade com a LGPD. A implementação das práticas recomendadas neste guia visa não apenas a adequação às exigências legais, mas também a construção de uma cultura de respeito à autodeterminação informativa. A conscientização e o treinamento contínuo dos servidores são fundamentais para que o STF seja um exemplo de conformidade e boas práticas no tratamento de dados pessoais.

Ao adotar as medidas descritas neste guia, o Tribunal também fortalece a confiança da sociedade na transparência das suas atividades, respeitando os direitos dos titulares e promovendo a segurança das informações.

Por fim, é imprescindível que o STF continue a revisar e aprimorar seus processos e práticas relacionadas à proteção de dados pessoais, adaptando-se às mudanças legais e tecnológicas. A adequação contínua à LGPD e o comprometimento com a proteção de dados pessoais são essenciais para garantir um ambiente mais seguro e ético para todos os cidadãos. O STF, como instituição pública, tem um papel fundamental na construção de uma sociedade mais consciente e responsável no uso e proteção de dados pessoais.

Secretária-Geral da Presidência
Aline Osorio

Equipe técnica de elaboração
Representantes do Supremo Tribunal Federal:
Luísa Lacerda
Polyane Wercelens da Silva
Teresa Cristina de Melo Costa

Especialistas externos:
Alisson Alexsandro Possa
Bruno Ricardo Bioni
Fabricio da Mota Alves
Laura Schertel Mendes
Maria Cecilia Oliveira Gomes
Tainá Aguiar Junquilho

Projeto gráfico e diagramação
SCO/ Coordenadoria de Multimeios / Gerência de Design Integrado

Brasília, 2025

SUPREMO TRIBUNAL FEDERAL

JANEIRO DE 2025


STF
SUPREMO TRIBUNAL FEDERAL