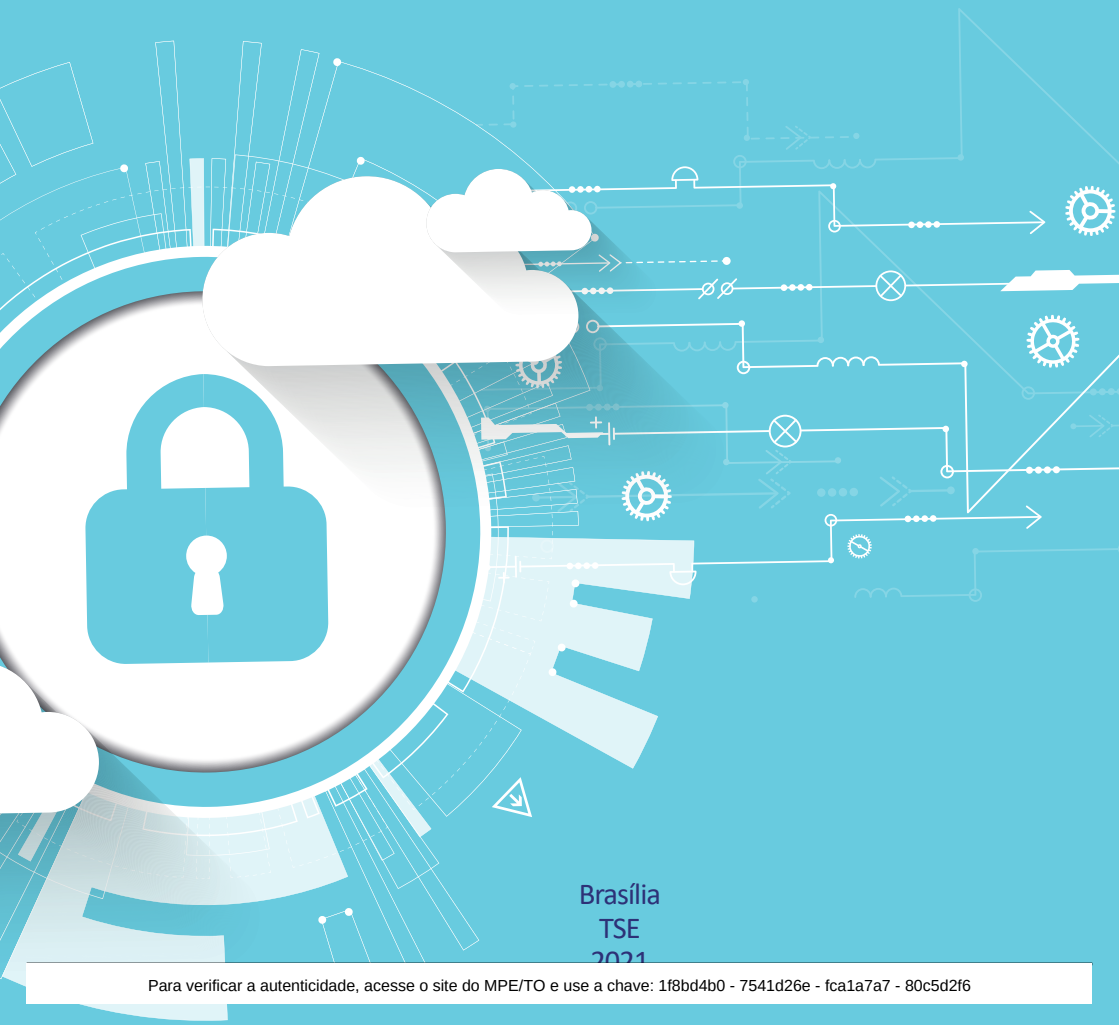
ANPD

Tribunal Superior Eleitoral

GUIA ORIENTATIVO
APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)
por agentes de tratamento no contexto eleitoral

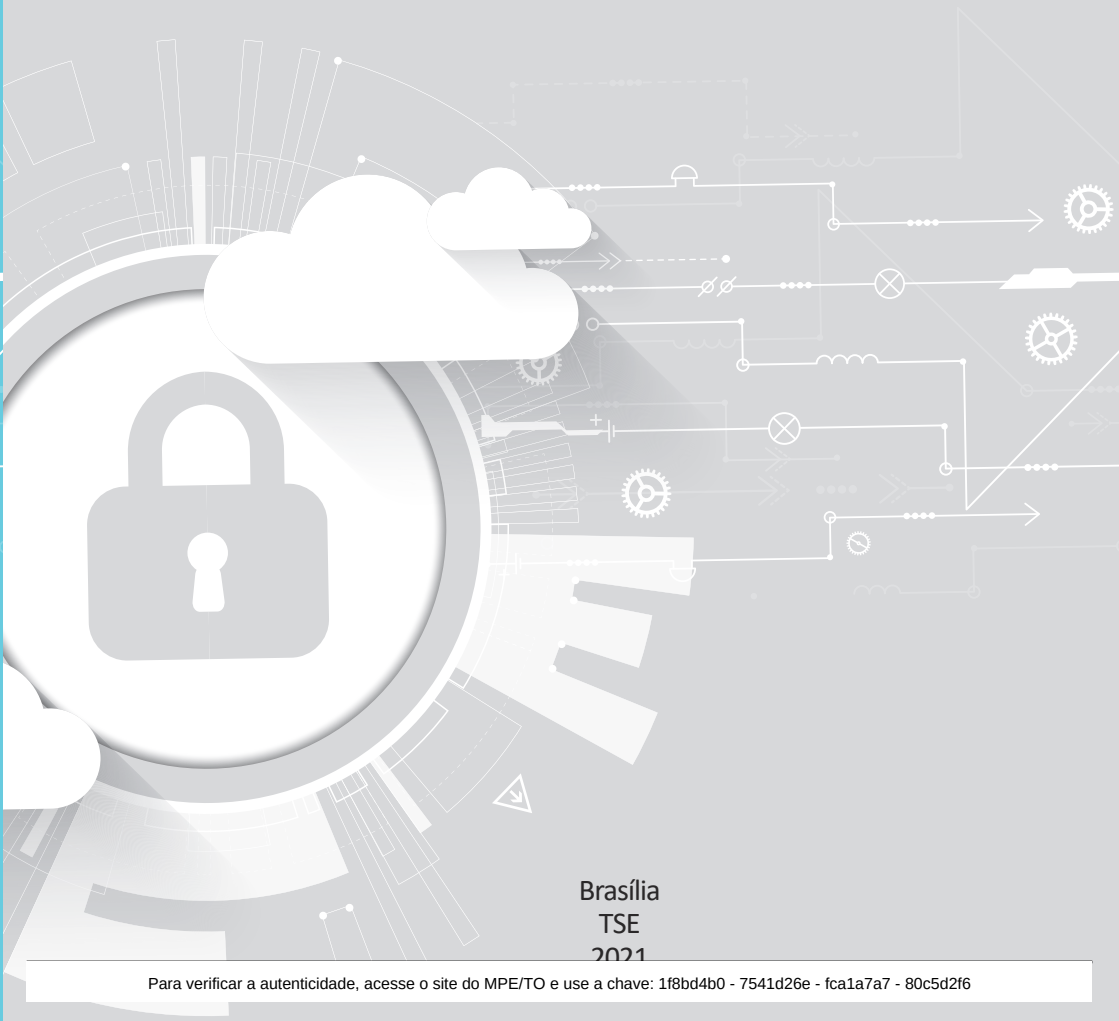


Brasília
TSE
2021

ANPD

Tribunal Superior Eleitoral

GUIA ORIENTATIVO
APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)
por agentes de tratamento no contexto eleitoral



Brasília
TSE
2021

TRIBUNAL SUPERIOR ELEITORAL

Presidente
Ministro Luís Roberto Barroso

Vice-Presidente
Ministro Edson Fachin

Ministros
Ministro Alexandre de Moraes
Ministro Mauro Campbell Marques
Ministro Benedito Gonçalves
Ministro Sérgio Banhos
Ministro Carlos Horbach

Procurador-Geral Eleitoral
Augusto Aras

PRESIDENTE DA REPÚBLICA
Jair Messias Bolsonaro

DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Waldemar Gonçalves Ortunho Júnior

MINISTRO PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL
Luís Roberto Barroso

CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Arthur Sabbat
Joacil Rael
Nairane Rabelo
Miriam Wimmer

EQUIPE DE ELABORAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Alexandra Krastins Lopes
Andressa Girotto Vargas
Diego Vasconcelos Costa
Isabela Maiolino
Jeferson Dias Barbosa
Lucas Borges de Carvalho
Lucas Costa dos Anjos
Luiz Octavio de Souza Pereira Gomes
Marcelo Santiago Guedes
Sabrina Fernandes Maciel Favero
Thiago Guimaraes Moraes

EQUIPE DE ELABORAÇÃO DO TRIBUNAL SUPERIOR ELEITORAL
Bruno Cezar Andrade de Souza
Luísa Lacerda
Simone Trento

Secretaria de Gestão da Informação
SAFS, Quadra 7, Lotes 1/2, 1º andar
Brasília/DF – 70070-600
Telefone: (61) 3030-9225

Secretária-Geral da Presidência
Aline Rezende Peres Osorio

Diretor-Geral da Secretaria do Tribunal
Rui Moreira de Oliveira

Secretário de Gestão da Informação
Cleber Schumann

Coordenador de Editoração e Publicações
Washington Luiz de Oliveira

Capa
Bruna Pagy

Projeto gráfico e diagramação
Verônica Estácio
Seção de Editoração e Programação Visual (Seprov/Cedip/SGI)

Revisão
Paula Lins e Valéria Carneiro
Seção de Preparação e Revisão de Conteúdos (Seprev/Cedip/SGI)

Dados Internacionais de Catalogação na Publicação (CIP)
Tribunal Superior Eleitoral – Biblioteca Professor Alysson Darowish Mitraud

Guia orientativo : aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral [recurso eletrônico]. – Dados eletrônicos (65 páginas). – Brasília : Tribunal Superior Eleitoral, 2021.

Guia elaborado em parceria entre a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e o Tribunal Superior Eleitoral (TSE).
Versão eletrônica (PDF).
Modo de acesso: Internet.
<https://www.tse.jus.br/o-tse/catalogo-de-publicacoes/lista-do-catalogo-de-publicacoes>

1. Brasil. Lei geral de proteção de dados (2018). 2. Proteção de dados pessoais – Brasil. 3. Processo eleitoral – Brasil. I. Brasil. Presidência da República. Autoridade Nacional de Proteção de Dados Pessoais. II. Brasil. Tribunal Superior Eleitoral.

CDD 342.810 858
CDU 342.721(81)

Bibliotecária: Sabrina Ruas Lopes – CRB-1/1865

Sumário

APRESENTAÇÃO

1. O processo político-eleitoral envolve a circulação de um grande volume de dados pessoais: candidatas, candidatos e partidos políticos querem fazer suas propostas chegar ao eleitorado e, para isso, é muito valioso conhecer seus hábitos e suas opiniões e pretensões.

2. A atual capacidade de processamento das informações e a adaptação da sociedade a novos hábitos digitais – com forte adesão a redes sociais e aplicativos de mensagens privadas e em grupos – aumentam a preocupação com a tutela de dados pessoais das cidadãs e dos cidadãos. No contexto eleitoral, a observância das regras de proteção de dados é essencial não apenas do ponto de vista individual, mas também para a defesa da democracia e integridade do pleito.

3. A Lei Geral de Proteção de Dados Pessoais (LGPD) especificou uma série de direitos das pessoas titulares de dados pessoais e, em contrapartida, trouxe obrigações para agentes que tratam dados pessoais. Ao mesmo tempo, a legislação eleitoral regula diversos aspectos da atividade político-partidária que guardam pontos de contato com a proteção de dados pessoais.

4. Diante desse cenário, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e o Tribunal Superior Eleitoral (TSE) apresentam este *Guia Orientativo*, destinado a agentes de tratamento que participam do processo eleitoral.

5. O propósito deste guia é, a partir de uma leitura sistemática das normas de proteção de dados pessoais e das normas eleitorais, apresentar os principais aspectos a serem considerados por candidatas, candidatos, coligações, federações e partidos políticos para o tratamento de dados pessoais das pessoas titulares, eleitoras ou eleitores em potencial. As orientações constantes desta publicação buscam garantir a proteção de dados, a privacidade das pessoas titulares e a lisura do processo eleitoral, sem obstruir a comunicação entre candidato e cidadão, necessária ao processo democrático.

6. Nessa tentativa, este guia é acompanhado de exemplos, que procuram ser ilustrativos, da aplicabilidade dos preceitos que devem reger as relações sociais que permeiam as eleições. Ao lado de esclarecimentos sobre normas impositivas no contexto eleitoral, este documento traz importantes recomendações de boas práticas a serem seguidas por candidatas, candidatos, partidos, coligações e federações partidárias.

7. As orientações apresentadas constituem um primeiro passo no processo de delimitação das interpretações sobre a LGPD aplicáveis ao contexto eleitoral. Por isso, a versão publicada ficará aberta a comentários e sugestões de forma contínua, pelo *e-mail* normatizacao@anpd.gov.br ou pelo contato com a Ouvidoria do TSE[1], com o fim de atualizar o guia oportunamente, à medida que novas regulamentações e entendimentos forem estabelecidos, a critério da ANPD e do TSE.

8. Desejamos contribuir com a consolidação de uma democracia atenta à proteção de dados pessoais. Boa leitura!

[1] A Ouvidoria do TSE pode ser contatada mediante preenchimento de formulário eletrônico disponível em: https://www.tse.jus.br/eleitor/servicos/ouvidoria.

DADOS PESSOAIS, DADOS SENSÌVEIS E APLICAÇÃO DA LGPD AO CONTEXTO ELEITORAL

9. O conceito de *dado pessoal* é amplo, sendo definido, no art. 5º, I, da LGPD, como a informação relacionada à pessoa natural identificada ou identificável. Assim, um dado é considerado pessoal quando permite a identificação, direta ou indireta, de uma pessoa natural.

10. A forma mais simples de identificação direta é pelo nome completo, por meio do qual é possível, em regra, distinguir uma pessoa de outra. Em algumas situações, no entanto, o nome pode não ser um identificador suficiente, como no caso de homônimos. Nessas hipóteses, a identificação da pessoa ocorre de forma indireta, pela combinação de outras informações, como o nome da mãe e a data de nascimento.

11. Dados pessoais também podem ser inferidos de outras informações para prever, avaliar e influenciar comportamentos e orientar processos decisórios automatizados. A título de exemplo, a formação de perfis pessoais e de consumo para fins de anúncios individualizados – como aqueles realizados em redes sociais – ocorre de forma automatizada, com base em uma série de informações coletadas das pessoas usuárias. Nesses casos, mesmo dados aparentemente irrelevantes ou sem um vínculo direto com uma pessoa, como curtidas em determinada postagem e vídeos assistidos, podem ser úteis à identificação de traços de sua personalidade. Como esse tipo de informação permite a identificação indireta de uma pessoa natural, com potencial impacto

sobre seus direitos e interesses, ele também se insere no conceito legal de dado pessoal.

12. Considerando a definição de dado pessoal, pode-se afirmar que *as disposições da LGPD são aplicáveis ao contexto eleitoral e devem ser observadas sempre que um partido político, uma candidata, um candidato ou qualquer outro(a) agente de tratamento realize uma operação com dados pessoais.* É o que a lei denomina de "tratamento", o qual inclui, entre outras, as atividades de coleta, classificação, armazenamento, transferência, transmissão e eliminação de dados pessoais.

13. Por sua vez, *dados pessoais sensíveis* são uma categoria de dados pessoais especialmente protegida pela LGPD, devido à sua maior vinculação a direitos fundamentais e ao maior risco relacionado ao seu uso. A definição legal está prevista no art. 5º, II, da LGPD:

> Art. 5º [...]
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

14. A LGPD determinou que os dados sensíveis sejam tratados com maior cautela, observadas regras mais restritivas do que aquelas que se aplicam a outros dados pessoais. A lei presumiu que a utilização indevida dessas informações tem o potencial de gerar restrições significativas ao exercício de direitos fundamentais, como atos de discriminação racial, étnica ou em razão de orientação sexual, considerando a pessoa titular de dados em posição mais vulnerável em relação a agentes de tratamento.

15. No âmbito das campanhas políticas, que recorrem, cada vez mais, a processos automatizados de tratamento de dados pessoais para apresentar propostas e se aproximar de seus(suas)potenciais eleitoras e eleitores, *o respeito às disposições da LGPD desempenha papel crucial para o estabelecimento de uma relação de confiança entre candidatas ou candidatos e eleitoras ou eleitores*, bem como para assegurar a estes *as condições necessárias para uma escolha autônoma e bem-informada*. O tratamento irregular de dados pessoais e, em particular, de dados sensíveis, no âmbito das campanhas políticas, pode gerar impactos negativos sobre a lisura do processo eleitoral e sobre a igualdade de oportunidades entre candidatas e candidatos.

16. Entre as categorias indicadas na lei, são especialmente relevantes para o contexto eleitoral os dados pessoais sensíveis sobre *opinião política* e *filiação a organização de caráter político*. Isso porque, em muitas ocasiões, agentes que realizam tratamento de dados pessoais para fins eleitorais irão lidar diretamente com dados desse tipo, a exemplo de dados pessoais de *indivíduos filiados a partidos políticos* ou da *formação de perfis que incluem a classificação da pessoa titular conforme sua opinião política*, os quais constituem dados sensíveis para fins da LGPD.

17. Dados pessoais sensíveis também podem ser revelados a partir do tratamento de inferência ou de cruzamento de bases de dados. Por isso, quando há revelação ou identificação indireta de aspectos sensíveis relacionados à personalidade da pessoa titular, com o potencial de prejudicar ou restringir seus direitos e interesses, expondo 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, dado genético ou biométrico, também se aplica o regime jurídico especial previsto na LGPD para os dados sensíveis.

18. É o caso da identificação de convicção religiosa, origem racial ou opinião política de pessoa titular de dados a partir de outras informações não

sensíveis, como o nome, o endereço e o perfil de consumo. Da mesma forma, um banco de dados de pessoas doadoras e voluntárias engajadas em uma campanha eleitoral, ainda que contenha apenas informações cadastrais e de contato da pessoa titular, pode revelar sua opinião política e ser considerado dado sensível, por exemplo, ao ser associado ao partido ou a candidata ou candidato responsável pela coleta das informações.

19. O tratamento de dados pessoais sensíveis somente pode ocorrer nas hipóteses legais específicas estipuladas no art. 11 da LGPD – em menor número e mais restritivas do que as previstas no art. 7º da lei, aplicáveis aos demais dados pessoais. Além de identificar a base legal adequada à hipótese, pode ser necessário elaborar relatório de impacto à proteção de dados pessoais, haja vista os prováveis riscos às liberdades civis e aos direitos fundamentais decorrentes do tratamento (art. 5º, XVII; art. 38). Finalmente, é importante observar os princípios aplicáveis (art. 6º), as medidas de prevenção e segurança e as regras específicas válidas para a hipótese, conforme as orientações disponibilizadas neste guia.

20. É importante considerar, também, que dados pessoais tornados manifestamente públicos pela pessoa titular não deixam de ser protegidos pela LGPD. O tratamento desses dados deve respeitar os direitos e as legítimas expectativas da pessoa titular, além de observar os princípios previstos na LGPD, tais como finalidade, adequação, necessidade e transparência.

Exemplo 1 – Aplicativo disponibilizado por partido político

Partido político disponibiliza aplicativo gratuito a pessoas filiadas e a eleitoras e eleitores em geral. Com o consentimento da pessoa usuária, o aplicativo coleta, entre outros, dados básicos de identificação, biometria facial e informações de localização. Os dados coletados constituem informação

relacionada a pessoa natural identificada ou identificável, razão pela qual todo o processo de tratamento dos dados pessoais deve ser efetuado em conformidade com as disposições da LGPD, sujeito à fiscalização pela ANPD e pela Justiça Eleitoral, conforme suas respectivas esferas de atuação. Além disso, as biometrias faciais coletadas, que são incorporadas em um banco de dados e utilizadas para a identificação da pessoa usuária, constituem dados pessoais sensíveis, cujo tratamento deve ser efetuado com maior cautela, observadas as hipóteses legais previstas no art. 11 da LGPD. A depender do contexto em que forem utilizados, todos os dados pessoais coletados pelo aplicativo poderão ser considerados dados sensíveis, caso sejam tratados com o propósito de inferir informações tais como opinião política, filiação a partido ou convicção religiosa.

AGENTES DE TRATAMENTO NO CONTEXTO ELEITORAL

21. Segundo a Lei nº 13.709, de 14 de agosto de 2018 LGPD, são agentes de tratamento o controlador e o operador de dados pessoais.

22. *O controlador*, nos termos do art. 5º, VI, da LGPD, é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade desse tratamento.

23. *O operador*, conforme definição do art. 5º, X, da LGPD, é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. O operador somente poderá tratar os dados para a finalidade previamente estabelecida pelo controlador.

24. Portanto, controladores e operadores podem ser pessoas naturais ou jurídicas, de direito público ou privado, definidos a partir de seu caráter institucional. No caso de uma pessoa jurídica, a organização é a agente de tratamento para os fins da LGPD, uma vez que é esta que estabelece as regras para o tratamento de dados pessoais, a serem executadas por seus(suas) representantes ou prepostos(as).

25. *Não são considerados controladores ou operadores os indivíduos subordinados*, tais como as pessoas funcionárias, as servidoras ou os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do(a) agente de tratamento.

26. Uma pessoa natural poderá ser controlador nas situações em que é a responsável pelas principais decisões referentes ao tratamento de dados pessoais. Nessa hipótese, a pessoa natural age de forma independente e em nome próprio, e não de forma subordinada a uma pessoa jurídica ou como membra ou membro de um órgão desta.

27. No contexto político-eleitoral, partidos políticos, coligações e candidatas e candidatos poderão ser considerados agentes de tratamento, bem como organizações contratadas para a realização de campanhas envolvendo o tratamento de dados pessoais. *Importa aqui observar a vedação do art. 31 da Resolução-TSE nº 23.610, de 18 de dezembro de 2019, às pessoas relacionadas no art. 24 da Lei nº 9.504/1997*[2]*, bem como às pessoas jurídicas de direito privado da utilização, doação ou cessão de dados pessoais de seus(suas) clientes em favor de candidatas ou de candidatos, de partidos políticos ou de coligações*. Em razão dos diferentes arranjos possíveis em uma campanha eleitoral, é importante compreender as responsabilidades de cada agente de tratamento de forma a se adequar à LGPD.

28. Constata-se, portanto, que, muito embora o controlador também trate dados pessoais, o elemento distintivo é o poder de decisão, admitindo-se que o controlador forneça instruções para que terceira ou terceiro ("operador") realize o tratamento em seu nome (art. 5º, VII; art. 39), no limite das finalidades determinadas por ele.

29. Ainda que a LGPD não determine expressamente que o controlador e o operador devam firmar contrato sobre o tratamento de dados, tal

[2] São elas: (i) entidade ou governo estrangeiro; (ii) órgão da administração pública direta e indireta ou fundação mantida com recursos provenientes do poder público; (iii) concessionário ou permissionário de serviço público; (iv) entidade de direito privado que receba, na condição de beneficiária, contribuição compulsória em virtude de disposição legal; (v) entidade de utilidade pública; (vi) entidade de classe ou sindical; (vii) pessoa jurídica sem fins lucrativos que receba recursos do exterior; (viii) entidades beneficentes e religiosas; (ix) entidades esportivas; (x) organizações não governamentais que recebam recursos públicos; (xi) organizações da sociedade civil de interesse público.

ajuste se mostra uma boa prática, uma vez que as cláusulas contratuais impõem limites à atuação do operador, fixam parâmetros objetivos para a alocação de responsabilidades entre as partes e reduzem os riscos e as incertezas decorrentes da operação. Os pontos que podem ser definidos contratualmente são o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos, as obrigações e as responsabilidades relacionados ao cumprimento da LGPD.

30. Quando há a contratação de um operador, é usual e legítimo que parte das decisões a respeito do tratamento, limitadas aos seus elementos não essenciais, fique sob sua alçada. A título de exemplo, podem ser mencionados a *escolha dos* softwares *e equipamentos* que serão utilizados e o detalhamento de *medidas de prevenção e segurança*.

31. Dentre os elementos decisórios essenciais, usualmente pelo controlador, destaca-se a definição *da finalidade do tratamento*, dos *objetivos que justificam a realização do tratamento*, e de sua respectiva *base legal*.

32. O controlador também é responsável por estabelecer outros elementos essenciais relativos ao tratamento, tais como a *definição da natureza dos dados pessoais tratados* (por exemplo, dados de pessoas filiadas a um partido político) e da *duração do tratamento*, isto é, do período durante o qual será realizada a operação, incluindo o estabelecimento de prazo para a eliminação dos dados. Vale ressaltar que outros elementos podem ser considerados essenciais a depender do contexto e das peculiaridades do caso concreto.

33. É importante observar que o(a) agente de tratamento é definido para cada operação de tratamento de dados pessoais, portanto a mesma organização poderá ser controlador e operador, de acordo com sua atuação em diferentes operações de tratamento.

Exemplo 2 – Contratação de empresa para desenvolvimento de aplicativo de partido

O partido político Sigma decide contratar a empresa Alpha para o desenvolvimento de um aplicativo para a agremiação. Ao firmar contrato com a empresa, o partido Sigma define o conteúdo a ser incorporado, o leiaute do aplicativo, bem como a política de privacidade. A empresa Alpha, por sua vez, trabalhará diretamente com a programação e a operação do *software* do aplicativo, incluindo manutenção e atualização periódicas e inserção do conteúdo previamente definido pelo partido.

Neste exemplo, o partido Sigma atuará como controlador ao determinar o tratamento de dados e definir os seus elementos essenciais. Enquanto isso, a empresa Alpha atuará como operadora ao tratar dados, conforme a finalidade definida pelo controlador. Cabe destacar que, caso a empresa contrate serviços de terceiras ou de terceiros, por exemplo, essa empresa prestadora de serviços será caracterizada como suboperadora.

34. É possível, ainda, que uma mesma operação de tratamento de dados pessoais envolva mais de um controlador com poder de decisão sobre elementos essenciais de tratamento. Nessa hipótese, há uma *controladoria conjunta*.

35. Conforme a LGPD, art. 42, § 1º, II, há responsabilidade solidária quando mais de um controlador estiver diretamente envolvido no tratamento, à exceção das hipóteses previstas no art. 43. Assim, embora a LGPD não explicite o conceito de controladoria conjunta, é possível inferir que ele está contemplado no sistema jurídico de proteção de dados.

36. Em resumo, verifica-se a existência de controladoria conjunta quando os seguintes critérios forem observados:

1. mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais;
2. há interesse mútuo de dois ou mais controladores, com base em finalidades próprias, sobre um mesmo tratamento; e
3. dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e os elementos essenciais do tratamento.

37. Grande parte dos casos de uso de mídia social para campanhas políticas podem configurar controladoria conjunta, visto que tanto a candidata ou o candidato quanto a plataforma podem tomar decisões sobre a forma e a finalidade do tratamento de dados pessoais, observadas as limitações previstas na legislação eleitoral.

38. A identificação da controladoria conjunta será contextual e apenas o caso concreto permitirá identificar em que casos a controladoria conjunta foi estabelecida. Uma vez que se configure, a responsabilidade dos controladores será solidária, o que reforça a importância de que todos estejam em conformidade com a LGPD.

Exemplo 3 – Contratação de empresa para elaboração de campanha eleitoral

O partido Delta contrata a empresa Gamma para desenvolver a campanha eleitoral da agremiação. Ao firmarem o contrato de prestação de serviços, a empresa Gamma propõe que seja realizado: impulsionamento de conteúdo a partir de perfis levantados em redes sociais, pesquisas de intenção de voto, bem como comícios presenciais e virtuais.

Ainda que, em parte, esteja tratando dados pessoais em nome do partido Delta, a empresa Gamma tem poder de decisão sobre elementos essenciais

do tratamento, tais como quais informações serão coletadas e de que forma será realizado o tratamento, inclusive quanto ao armazenamento, ao tempo de retenção e à eliminação dos dados pessoais.

Nesse sentido, considera-se que o partido Delta e a empresa Gamma atuarão em controladoria conjunta, uma vez que ambos serão responsáveis pela definição quanto aos elementos essenciais do tratamento.

39. Para informações mais detalhadas sobre agentes de tratamento, veja o *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, elaborado pela ANPD[3].

[3] Acessível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

PRINCIPAIS BASES LEGAIS

40. O uso de dados pessoais por candidatas, candidatos, partidos políticos ou coligações, independentemente da finalidade pretendida, somente poderá ocorrer se estiver amparado em alguma das hipóteses autorizativas estabelecidas na LGPD. Essas hipóteses são conhecidas como bases legais para o tratamento de dados pessoais, e estão previstas nos arts. 7º e 11 da LGPD.

41. O art. 7º da lei enumera dez hipóteses que justificam a utilização de dados pessoais não sensíveis, ao passo que o art. 11 prevê oito circunstâncias em que é permitida a realização de atividades de tratamento envolvendo dados pessoais de natureza sensível.

42. A avaliação a ser realizada pelo controlador para a definição da base legal mais adequada e segura para que um dado pessoal possa ser coletado, armazenado e processado deve considerar a finalidade específica a ser alcançada por meio do tratamento, além do contexto do caso concreto.

43. Dessa forma, para que as operações de tratamento de dados pessoais sejam consideradas lícitas e legítimas, além do respeito aos princípios estabelecidos na LGPD, o(a) agente de tratamento deve confirmar, antes de qualquer utilização do dado pessoal, a existência de alguma das hipóteses previstas na legislação (art. 7º ou, no caso de dados sensíveis, art. 11 da LGPD).

44. A seguir, serão abordadas as principais bases legais que podem dar amparo ao tratamento de dados pessoais para o exercício de atividades de natureza político-eleitoral. Vale ressaltar que não serão avaliadas todas as bases legais previstas na LGPD, mas apenas aquelas mais relevantes para o contexto avaliado.

Consentimento (art. 7º, I, e art. 11, I, da LGPD)

45. A primeira base legal estabelecida pela LGPD para fundamentar o tratamento de dados pessoais é o consentimento da pessoa titular de dados. Como já exposto, o consentimento não é a única nem a principal base legal possível para viabilizar o tratamento de dados pessoais.

46. Nos termos do art. 5º, XII, da LGPD[4], adotar o consentimento como base legal para uma determinada operação de tratamento pressupõe um processo de tomada de decisão livre, bem informado e inequívoco pela pessoa titular do dado pessoal acerca da sua utilização para uma finalidade específica.

47. No contexto eleitoral, o consentimento é necessário, por exemplo, para o recebimento de mensagens instantâneas com conteúdo de propaganda, por meio de disparo em massa (art. 34 da Res.-TSE nº 23.610/2019). Isso quer dizer que a realização de propaganda por meio de disparo em massa de mensagens instantâneas é, em regra, vedada, salvo anuência da pessoa destinatária.

48. O consentimento será livre quando a pessoa titular de dados puder escolher entre aceitar ou recusar a realização do tratamento pretendido sem consequências negativas ou intervenções do controlador de dados que possam vir a viciar ou prejudicar sua manifestação de vontade.

---

[4] Art. 5º [...]
XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

49. O consentimento será informado quando todas as informações necessárias para uma avaliação consciente pela pessoa titular forem apresentadas pelo(a) agente de tratamento. Assim, a pessoa titular deve ter conhecimento prévio a respeito da forma e do prazo pelo qual seu dado pessoal será tratado, bem como das finalidades pretendidas pelo controlador[5], sendo importante expor que essas informações se vinculam à própria utilização do dado. Qualquer alteração das premissas adotadas para a obtenção do consentimento macula a base legal adotada, exigindo novo consentimento pelo titular de dados, ou a utilização de outra base legal, de acordo com as novas premissas estabelecidas e com todas as informações necessárias para tanto.

50. Além disso, o consentimento deve ser inequívoco, o que significa dizer que o(a) agente responsável pelo tratamento deve obter uma manifestação de vontade clara da pessoa titular do dado, *não se permitindo sua inferência ou obtenção de forma tácita ou a partir de uma omissão do titular*. Importante observar que compete ao controlador do dado a responsabilidade de comprovar que o consentimento do titular foi obtido com respeito a todos os parâmetros estabelecidos pela LGPD. Dessa forma, é uma boa prática o registro e a documentação de todos os requisitos necessários para a comprovação de que o consentimento da pessoa titular não possui vícios e contou com todas as informações necessárias.

51. Caso o dado a ser tratado pelo controlador se enquadre na definição de dado pessoal sensível, alguma das bases legais constantes no art. 11 da LGPD deverá ser adotada. Na hipótese de ser utilizado o consentimento, este deverá *ser obtido por forma específica e destacada, conforme preconiza o art. 11, I, da LGPD*. Em relação à forma destacada,

[5] Pela relevância do assunto, é importante expor que a finalidade declarada pelo controlador de dados para a realização de operações de tratamento não poderá ser genérica ou ampla, sendo imprescindível a apresentação de informações pormenorizadas, claras e em linguagem acessível, de forma que a pessoa titular possa consentir ou não com o tratamento desejado de forma consciente.

recomenda-se que o consentimento conste separadamente do texto principal ou, ainda, que se usem recursos para evidenciá-lo, de modo a indicar quais dados serão coletados e de que forma serão utilizados pelo controlador. A finalidade do consentimento deverá ter objeto específico, sendo, portanto, determinada e restrita àquela atividade para a qual se deu o consentimento. Uma maneira de fazer isso seria utilizar formulário que coletaria separadamente o consentimento para a coleta e o tratamento de dados sensíveis para uma finalidade específica.

52. Dessa forma, além dos requisitos previstos no art. 7º da LGPD, que exigem que o consentimento para a utilização de dados pessoais não sensíveis deve ser livre, informado e inequívoco, *para dados pessoais sensíveis, o(a) agente deve comprovar que o consentimento foi obtido de forma específica e destacada em relação a outras comunicações mantidas com a pessoa titular do dado*.

53. Ainda, quando o tratamento de dados for realizado tendo o consentimento como base legal, independentemente da natureza do dado, se sensível ou não, é importante garantir o *direito à revogação do consentimento*, previsto pelo art. 8º, § 5º, da LGPD. O controlador de dados deve fornecer mecanismo gratuito e facilitado de exercício de revogação do consentimento pela pessoa titular para cessar a atividade de tratamento, seja por meio de formulário eletrônico, seja por *e-mail* com solicitação de descadastramento, por exemplo. O ato de revogação é unilateral e deverá ser atendido sempre que requisitado pela pessoa titular de dados.

Exemplo 4 – Constituição de banco de dados por partido político após a vigência da LGPD

Partido Ômega, que teve seu estatuto registrado no TSE em setembro de 2021, busca constituir uma base de dados pessoais apenas com

nome, endereço de *e-mail* e telefone de eleitoras e de eleitores com a finalidade específica de envio do programa eleitoral da agremiação para as eleições de 2022. Para tanto, o partido adotou a base legal do consentimento prevista no art. 7º, I, da LGPD.

Para ser considerado adequado e lícito o tratamento pretendido, o partido Ômega deve observar e respeitar todos os princípios constantes no art. 6º da LGPD, devendo, ainda, obter o consentimento das eleitoras e dos eleitores de forma livre, informada e inequívoca, sempre observando, durante toda a cadeia de tratamento, a finalidade específica indicada no momento da coleta dos dados, no caso, o envio do programa eleitoral para as eleições de 2022.

Conforme preconiza o art. 9º da LGPD, a eleitora e o eleitor deverão receber, de forma clara, adequada e ostensiva, todas as informações necessárias para compreender as finalidades que justificam a coleta de seus dados. Para tanto, deverão ter acesso à identidade do controlador responsável pelas operações de tratamento e às suas informações de contato, ao tipo de dado que será coletado, ao uso pretendido pelo partido político e à sua duração e deverá, ainda, ser informado sobre seus direitos constantes na LGPD.

Por fim, o partido Ômega deve ser capaz de demonstrar que a pessoa titular de dados efetivamente manifestou sua vontade no sentido de consentir com o tratamento pretendido. Assim, para ser considerado válido, o consentimento deve resultar de uma ação clara da pessoa titular, que pode ocorrer por meio de um "clique" em um botão destacado, pela marcação em uma caixa de texto em branco contida em formulário eletrônico, pela assinatura em formulário impresso ou por formas similares disponibilizadas pelo partido. Vale destacar que deve ser conferida à pessoa titular a efetiva possibilidade de aceitar ou recusar o tratamento, de modo que o fornecimento de uma única opção, o silêncio ou a continuidade de acesso à página do partido político, sem ações concretas no sentido de concordar com o tratamento pretendido, não pode ser considerado como consentimento válido.

Exemplo 5 – Tratamento de dados sensíveis mediante o consentimento da pessoa titular e mudança posterior da finalidade do tratamento de dados

João, cidadão brasileiro, animado com a proximidade das eleições em seu município, acessa o sítio eletrônico do partido Alpha e preenche formulário a fim de que possa participar de uma reunião ordinária do partido, que ocorrerá remotamente. No sítio eletrônico, havia expressamente a informação de que a base legal adotada para o tratamento dos dados pessoais era o consentimento com a finalidade específica de registro de sua participação em reunião ordinária do partido Alpha.

Caso o tratamento a ser realizado envolva dados pessoais de natureza sensível, conforme previsto no art. 11, I, da LGPD, o consentimento deve ser obtido de forma *específica, destacada e para finalidades específicas*, sendo nulas as autorizações genéricas, nos termos do art. 8º, § 4º, da lei. Em relação à forma destacada, recomenda-se que o consentimento conste separadamente do texto principal ou, ainda, que se usem recursos para evidenciá-lo, de modo a indicar quais dados serão coletados e de que forma serão utilizados pelo controlador. A finalidade do consentimento deverá ter objeto específico, sendo, portanto, determinada e restrita àquela atividade para a qual se deu o consentimento. Vale dizer, ainda, que o consentimento é revogável a qualquer tempo, mediante procedimento gratuito e facilitado. Além disso, para que seja válido, o consentimento deverá ocorrer de forma *livre, informada e inequívoca*.

No exemplo em questão, considerando que a finalidade do tratamento se destinava ao registro de participação em evento do partido Alpha, esses dados não poderão ser utilizados para encaminhamento de mensagens eletrônicas, por exemplo, sem a obtenção de novo consentimento específico ou sem outra base legal eventualmente aplicável para a nova finalidade almejada, tendo em vista a falta de anuência da pessoa titular de dados em relação à segunda operação de tratamento.

Obrigação legal (art. 7º, II, e art. 11, II, *a*, da LGPD)

54. A base legal da obrigação legal ou regulatória pode ser utilizada tanto para dados pessoais sensíveis quanto para dados não sensíveis ou ordinários e autoriza o tratamento de dados pessoais pelo controlador para o cumprimento de obrigações legais ou regulatórias.

55. Nessa hipótese, o controlador precisa tratar apenas os dados pessoais da pessoa titular que sejam essenciais para garantir a execução de obrigações legais ou regulatórias. Dessa forma, apenas os dados pessoais necessários para o cumprimento da obrigação devem ser objeto de tratamento e utilizados exclusivamente para essa finalidade.

56. Um exemplo de utilização da hipótese da obrigação legal para o tratamento de dados pessoais no contexto político-eleitoral pode ser observado a partir da obrigação estabelecida na Lei dos Partidos Políticos (Lei nº 9.096/1995), que, em seu art. 19,[6] dispõe que o partido deverá inserir os dados de suas filiadas e de seus filiados no sistema eletrônico da Justiça Eleitoral. Também por previsão legal, os partidos políticos têm pleno acesso às informações de suas filiadas e de seus filiados constantes do Cadastro Eleitoral, devendo a Justiça Eleitoral disponibilizar acesso eletrônico a esses dados (art. 19, §§ 3º e 4º, da Lei nº 9.096/1995).

57. Outra situação que exige o tratamento de dados pessoais em decorrência de obrigações legais pode ser observada quando do cumprimento de obrigações de ordem trabalhista ou previdenciária, como no caso

[6] Art. 19. Deferido internamente o pedido de filiação, o partido político, por seus órgãos de direção municipais, regionais ou nacional, deverá inserir os dados do filiado no sistema eletrônico da Justiça Eleitoral, que automaticamente enviará aos juízes eleitorais, para arquivamento, publicação e cumprimento dos prazos de filiação partidária para efeito de candidatura a cargos eletivos, a relação dos nomes de todos os seus filiados, da qual constará a data de filiação, o número dos títulos eleitorais e das seções em que estão inscritos.

de compartilhamento de dados de funcionárias e de funcionários do partido político com órgãos públicos, como o Instituto Nacional do Seguro Social (INSS) ou a Receita Federal.

Legítimo interesse (art. 7º, IX, da LGPD)

58. 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 pessoas terceiras, "exceto no caso de prevalecerem direitos e liberdades fundamentais da pessoa titular que exijam a proteção dos dados pessoais" (art. 7º, IX). *Trata-se, portanto, de base legal não aplicável ao tratamento de dados pessoais sensíveis*.

59. O interesse do controlador será considerado legítimo quando não encontrar óbices legais, isto é, quando não for contrário às disposições da lei. Por exemplo, não há legítimo interesse das candidatas e dos candidatos, dos partidos políticos, das coligações e das federações na obtenção de dados custodiados pela administração pública ou por pessoa jurídica de direito privado, tendo em vista se tratar de prática vedada pela legislação eleitoral (art. 57-E, *caput*, da Lei nº 9.504/1997 e art. 31 da Res.-TSE nº 23.610/2019). Do mesmo modo, é vedada a venda, por pessoas físicas e jurídicas, de cadastros eletrônicos (art. 57-E, § 1º, da Lei nº 9.504/1997 e art. 31, § 1º, da Res.-TSE nº 23.610/2019), o que impede a caracterização do legítimo interesse. Tampouco há legítimo interesse na utilização de dados pessoais para envio de propaganda eleitoral por *telemarketing*, tendo em vista que é prática vedada pelo art. 34 da Res.-TSE n° 23.610/2019 e pelo Supremo Tribunal Federal (STF) na ADI nº 5.122.

60. Além disso, o controlador deverá avaliar, em momento anterior à realização de qualquer operação baseada em seu legítimo interesse ou de pessoa terceira, a proporcionalidade entre, de um lado, os interesses

que legitimam o tratamento e, de outro, os direitos e as legítimas expectativas das pessoas titulares. Deverá, ainda, comprovar a adoção de medidas técnicas e administrativas capazes de salvaguardar a operação e os dados utilizados, garantindo a segurança do tratamento e a transparência para as pessoas titulares.

61. A avaliação a ser realizada pelo controlador acerca das legítimas expectativas da pessoa titular de dados deve considerar o respeito aos seus direitos e liberdades individuais. Para ser adequado o tratamento, o controlador deve se certificar de que a utilização pretendida, além de não ferir direitos e liberdades, poderia ser razoavelmente prevista pela pessoa titular de dados, isto é, que seria possível à pessoa titular supor que aquela utilização poderia ocorrer com seus dados pessoais a partir das informações prestadas pelo controlador no momento da coleta do dado pessoal.

62. Ressalta-se que, caso o partido político, candidata ou candidato faça uso dessa base legal, as regras do art. 10 da LGPD deverão ser observadas, tais como os destaques conferidos aos princípios da necessidade, da finalidade (§ 1º) e da transparência (§ 2º). Além disso, segundo o § 3º desse artigo, a ANPD poderá solicitar a elaboração de relatório de impacto à proteção de dados pessoais, por meio do qual o controlador deverá comprovar a observância dos requisitos estabelecidos pela LGPD para o tratamento.

Exemplo 6 – Coleta de dados de navegação para melhoria da experiência durante a navegação

Partido Alpha coleta dados de navegação a partir do acesso de pessoas usuárias a seu *site* na internet com a finalidade de desenvolver ações de *melhoria da experiência durante a navegação*. Para tanto, serão coletados

dados pessoais mediante a utilização de *cookies*, que serão utilizados para gerar informações sobre a navegação das pessoas usuárias.

No exemplo, o partido deverá, em momento anterior à coleta, avaliar: a legitimidade do seu interesse; a proporcionalidade entre o interesse declarado e as legítimas expectativas da pessoa titular do dado; e a eventual existência de violação aos direitos e liberdades individuais da pessoa titular do dado, devendo, ainda, adotar salvaguardas para garantir o respeito aos direitos da pessoa titular.

Além disso, o partido Alpha deve limitar a utilização dos dados pessoais à finalidade declarada, não podendo utilizá-los para outras finalidades, como o desenvolvimento de perfis de pessoas usuárias a partir dos hábitos de navegação. Caso o partido pretenda utilizar os dados pessoais para essa segunda finalidade, deverá, necessariamente, fazê-lo com fundamento em outra base legal, como o consentimento, ou realizar nova avaliação de legítimo interesse. Além disso, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados e o controlador deverá adotar medidas para garantir a transparência do tratamento.

PRINCÌPIOS DA FINALIDADE, DA ADEQUAÇÃO E DA NECESSIDADE

63. Toda operação de tratamento de dados pessoais deve estar associada a uma *finalidade*[7] que atenda a esse princípio. Para isso, a finalidade deve cumprir quatro requisitos:

    1. ser legítima, isto é, deve ser lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal que autorize o tratamento de dados pessoais;
    2. ser específica, isto é, a partir da finalidade, deve ser possível delimitar o escopo do tratamento e estabelecer quais as garantias necessárias para a proteção dos dados pessoais;
    3. ser explícita, isto é, deve ser expressa de maneira clara e precisa; e
    4. ser informada, isto é, deve ser disponibilizada em linguagem simples e de fácil acesso para a pessoa titular de dados.

64. O princípio da *adequação*[8] está diretamente relacionado ao da finalidade. As operações de tratamento de dados raramente ocorrem de forma isolada. O simples ato de coletar dados implica que eles serão

[7] Art. 6º [...]
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

[8] Art. 6º [...]
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

transportados e armazenados em algum lugar. Outras operações, como compartilhamento e eliminação de dados também costumam ocorrer a partir de atividades preliminares. Assim, sempre que uma operação de tratamento for realizada em seguida a outra, é preciso analisar se esse conjunto de operações é compatível com a finalidade inicial. Caso contrário, será necessário identificar uma nova finalidade que atenda aos requisitos desse princípio, providenciando-se a informação à pessoa titular do dado.

65. Além disso, o princípio da *necessidade*[9] orienta que todo tratamento deve se limitar ao mínimo necessário para a realização de suas finalidades. O(a) agente de tratamento de dados deve refletir sobre quais categorias de dados pessoais necessitam ser tratadas para o alcance de uma determinada finalidade, devendo se restringir a tratar somente esses dados pessoais. Ou seja, conforme o art. 6º, III, da LGPD, o tratamento deve abranger apenas os dados pertinentes, proporcionais e não excessivos em relação às suas finalidades.

Desvio de finalidade - como evitar

66. Ao cumprir sua finalidade, o tratamento de dados pessoais é finalizado. Realizados os registros das operações de tratamento, os(as) agentes de tratamento devem efetuar o controle de uso dos dados em relação às finalidades que lhe tenham sido atribuídas especificamente. Ou seja, o(a) agente de tratamento não deve permitir que os dados sejam utilizados para finalidades incompatíveis com as originalmente definidas, que não possuam bases legais que legitimem o tratamento e que desrespeitem os princípios do art. 6º da LGPD.

[9] Art. 6º [...]
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

67. Em regra, os dados pessoais devem ser excluídos ou anonimizados ao término do tratamento, o que ocorre, por exemplo, quando a finalidade for alcançada ou quando os dados não forem mais necessários ou pertinentes para o seu alcance, conforme o art. 15, I, da LGPD. Os dados poderão ser conservados mesmo após o término do tratamento nas hipóteses previstas no art. 16 dessa lei.

68. Vale enfatizar que os dados pessoais coletados somente podem ser utilizados para uma nova finalidade se ela for compatível com a finalidade original. Caso contrário, será necessário verificar novamente qual a base legal adequada, o que pode ensejar a obtenção de novo consentimento ou, ainda, fundamentar o tratamento por meio de outras bases legais, tais como a necessidade de cumprimento de uma obrigação legal ou o legítimo interesse.

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS (*ACCOUNTABILITY*)

69. O princípio da responsabilização e prestação de contas (*accountability*) estabelece que os(as) agentes de tratamento devem ser capazes de demonstrar o cumprimento e o respeito à LGPD, apresentando as medidas adotadas e a eficácia delas. Para isso, a lei apresenta uma série de instrumentos que podem ser utilizados.

70. Em primeiro lugar, cabe destacar a importância de se implementar um *Programa de Governança em Privacidade (PGP)* (art. 50, § 2º, I). Embora a lei indique ao controlador a possibilidade de elaborar esse programa, o operador, enquanto agente de tratamento, também pode produzir o seu próprio programa.

71. O PGP deve ser capaz de demonstrar a integridade e o comprometimento do(a) agente de tratamento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais. Nesse sentido, cabe destacar alguns processos e políticas importantes para a governança dos dados pessoais.

72. Uma atividade importante é o mapeamento dos dados pessoais tratados pelo(a) agente de tratamento, que pode ser consolidado em um inventário de dados pessoais. Esse inventário irá descrever todos os processos que tratam dados pessoais, informando, *por exemplo*:

    - as finalidades do tratamento;

- as bases legais para o tratamento (arts. 7º e 11 da LGPD);
- as categorias de dados pessoais tratados;
- a existência de decisões tomadas com base em tratamento automatizado e suas características;
- a ocorrência de compartilhamento de dados incluindo, se for o caso, a transferência internacional de dados, quem são os destinatários, que dados são compartilhados e as hipóteses legais para o compartilhamento;
- o tempo de retenção dos dados e os locais onde são armazenados;
- as práticas de eliminação e descarte dos dados pessoais;
- os meios pelos quais os direitos das pessoas titulares de dados podem ser exercidos;
- as medidas de segurança técnicas e administrativas implementadas.

73. É importante que as políticas informem às pessoas titulares de dados como os dados pessoais são tratados, estabeleçam orientações internas para o tratamento de dados pessoais, definam as medidas de segurança técnicas e administrativas que devem ser adotadas e informem sobre a utilização de *cookies* ou outros rastreadores eletrônicos.

74. O PGP também deve conter planos de resposta a incidentes e remediação para orientar o(a) agente a lidar com cenários de incidentes de segurança.

75. As políticas e salvaguardas adotadas devem ser implementadas de acordo com um processo de avaliação sistemática de impactos e riscos à privacidade. Esta abordagem orientada a riscos deve ter como foco a pessoa titular de dados. Um importante instrumento para essa avaliação de riscos é o *Relatório de Impacto à Proteção de Dados Pessoais (RIPD)*. De acordo com o art. 5º, XVII, esse documento contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, proteções e mecanismos de mitigação de risco.

76. Embora a LGPD não determine os contextos em que a elaboração de um RIPD é obrigatória, sua elaboração, principalmente em cenários de alto risco, como os que envolvam tratamento de dados sensíveis e em larga escala, *é altamente recomendável*. Como no contexto eleitoral pode ocorrer o tratamento de um grande volume de dados sensíveis relacionados a opiniões e filiações políticas, o RIPD se torna um instrumento importante de *accountability*.

77. O PGP deve ser aplicável a todo o conjunto de dados pessoais que sejam tratados pelo(a) agente, independentemente do modo como a coleta foi realizada. A coleta de dados pessoais pode ser realizada diretamente com as pessoas titulares ou intermediada por diferentes agentes de tratamento, por exemplo, por meio de atividades de corretagem. As corretoras de dados agregam informações e segmentam titulares de acordo com características que consideram relevantes em cada contexto. As organizações que estejam envolvidas nessas relações devem definir claramente seus papéis, sejam elas controladoras ou operadoras de dados, e, consequentemente, a atribuição de obrigações e responsabilidades decorrentes de cada uma dessas funções de tratamento, em particular no respeito aos princípios da LGPD, aos direitos das pessoas titulares de dados e à legislação eleitoral.

78. Além disso, o programa deve ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados. Desse modo, a complexidade do programa poderá variar não apenas de acordo com o porte do(a) agente de tratamento, como também com relação à natureza dos dados pessoais.

79. O programa deve privilegiar a comunicação transparente com a pessoa titular, com o objetivo de estabelecer relação de confiança com esta, assegurando, inclusive, mecanismos para sua participação nas atividades de tratamento.

80. Por fim, o PGP deve estar integrado à estrutura geral de governança de agentes de tratamento e deve estabelecer e aplicar mecanismos de supervisão internos e externos. É essencial que ele seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

81. Além disso, a LGPD determina, no art. 37, que agentes de tratamento devem manter *registro das operações de tratamento de dados pessoais* que realizar. Embora seja dado destaque para essas atividades de registro no caso de uso da hipótese legal do legítimo interesse, é importante frisar que a manutenção desses registros é obrigatória para qualquer atividade de tratamento de dados.

82. Os registros são especialmente importantes para implementar trilhas de auditorias que auxiliam a compreender a cadeia de compartilhamento de dados pessoais, ao mesmo tempo que facilitam a investigação forense de incidentes de segurança que envolvam a exfiltração de dados pessoais (vazamento de dados).

83. Para garantir a correta implementação das práticas supramencionadas, é recomendável que sejam realizados planos de *capacitação e treinamento em proteção de dados e segurança da informação*. A conscientização das pessoas funcionárias de agentes de tratamento é essencial para que as políticas e salvaguardas estabelecidas no PGP sejam concretizadas, assim como o princípio da responsabilização e prestação de contas.

84. Outros(as) importantes protagonistas para a efetividade das boas práticas em privacidade são *a encarregada ou o encarregado de dados pessoais* (art. 5º, VIII, da LGPD). A encarregada ou o encarregado é o canal de comunicação de agentes de tratamento com as pessoas titulares e com a ANPD. Além disso, ele(a) pode auxiliar no processo de elaboração e implementação do PGP, bem como nas atividades de conscientização internas e externas. As atribuições do encarregado

estão elencadas no § 2º do art. 41 da LGPD e, por agir como um ponto de contato com as pessoas titulares de dados e com a ANPD, é importante que os detalhes de contato da encarregada ou do encarregado de dados estejam facilmente acessíveis, nos termos do § 1º do art. 41 da LGPD.

85. Para mais orientações a respeito da encarregada ou do encarregado, sugere-se a leitura do *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, publicado pela ANPD[10].

[10] *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado* disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

DIREITOS DA PESSOA TITULAR, TRANSPARÊNCIA E LIVRE ACESSO

86. A autodeterminação informativa, um dos fundamentos da LGPD com previsão no inciso II do art. 2º, confere à pessoa titular de dados o direito de controlar seus próprios dados pessoais, com base nos preceitos da boa-fé e da transparência. Nesse contexto, a lei estabeleceu, nos incisos do art. 18, alguns direitos que podem ser exercidos pelas pessoas titulares de dados, permitindo, entre outros, a confirmação da existência de operações de tratamento envolvendo seus dados pessoais, a possibilidade de correção de dados eventualmente incorretos e, ainda, a revogação do consentimento concedido para uma determinada operação.

87. Considera-se que o rol de direitos dispostos no art. 18 é exemplificativo, tendo em vista a previsão de direitos em outros dispositivos da LGPD, como o constante no art. 20[11]. Esses direitos podem ser exercidos pelas pessoas titulares mediante requerimento expresso dirigido a agente de tratamento ou ao(à) seu(sua) encarregado(a), conforme o caso. Em regra, nos termos do art. 18, § 4º, o requerimento somente poderá ser negado nas hipóteses em que: (i) o controlador não é o(a) agente de tratamento, devendo indicar, sempre que possível, o(a) agente responsável pelo tratamento; ou (ii) o(a) agente de tratamento apontar as razões de fato e de direito que o(a) impedem de adotar a medida requerida pela pessoa titular. Entretanto, ainda assim, nessas hipóteses,

[11] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

existe a obrigação, prevista no § 4º do art. 18 da LGPD, de o controlador enviar comunicação à pessoa titular de dados, informando-lhe sobre a negativa do requerimento

88. A revogação do consentimento é um dos direitos da pessoa titular listados no art. 18, IX. Para as demais bases legais, a pessoa titular poderá se opor ao tratamento realizado, em caso de descumprimento ao disposto na LGPD, conforme art. 18, § 2º.

89. Em qualquer hipótese, o controlador deverá fornecer à pessoa titular o acesso às informações referentes ao tratamento de seus dados, nos termos do art. 9º da LGPD, de maneira facilitada, de forma a viabilizar o exercício dos direitos estabelecidos na legislação e possibilitar, caso necessário, a apresentação de requerimentos, diante de possíveis violações às disposições da LGPD.

90. Conforme o art. 18, § 5º, da LGPD, o requerimento será atendido pelo controlador sem custos à pessoa titular, observados os prazos de atendimento previstos em regulamento a ser editado pela ANPD. Caso o controlador não atenda o requerimento apresentado pela pessoa titular, este(a) poderá peticionar contra o controlador na ANPD (art. 18, § 1º e art. 55-J, V).

91. Vale ressaltar que a LGPD, em linha com o princípio constitucional do acesso à Justiça (art. 5º, XXXV, da CF/1988)[12], indica a possibilidade de defesa dos interesses e direitos das pessoas titulares em juízo, individual ou coletivamente, conforme preconiza o art. 22. Caso haja violação a obrigações previstas na legislação eleitoral, a Justiça Eleitoral poderá ser acionada pelas legitimadas e pelos legitimados, como o Ministério Público, partidos políticos, candidatas e candidatos.

[12] Art. 5º [...]
XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;

Canais para exercício dos direitos da pessoa titular

92. Conforme exposto, a adequada aplicação da LGPD por partidos políticos, candidatas e candidatos na condição de agentes de tratamento pressupõe a disponibilização de canais de comunicação que sejam eficientes e facilmente acessíveis às pessoas titulares de dados. Tal conduta, além de conferir maior transparência à relação e gerar benefícios relacionados à confiança entre a pessoa titular e o(a) controlador(a) de dados, possibilita a efetiva implementação dos direitos elencados na LGPD, minimizando riscos de questionamentos administrativos e judiciais envolvendo violações aos direitos das pessoas titulares de dados.

93. Portanto, é importante que agentes de tratamento forneçam canais adequados de contato para receber as demandas da pessoa titular de dados. Recomenda-se o uso de canal no mesmo ambiente em que serviços e produtos são oferecidos à pessoa titular, seja o sítio eletrônico, aplicativo, *e-mail* ou qualquer outra plataforma digital. Serviços de comunicação postal ou telefônica são bem-vindos como canal subsidiário para garantir acesso às pessoas titulares que, por algum motivo, não estejam conseguindo enviar seu requerimento por meios digitais. Independentemente do canal utilizado, o acesso gratuito deve ser garantido por agentes de tratamento. Além disso, destaca-se novamente o papel da encarregada ou do encarregado como ponto de contato entre a pessoa titular e o controlador, sendo elemento importante para facilitar essa comunicação.

94. Recomenda-se que controladores e operadores possuam canais de comunicação direta entre si para que possam informar uns aos outros sobre petições de pessoas titulares, garantindo que os direitos destas sejam atendidos tempestivamente. A mesma recomendação é válida para as hipóteses de controladoria conjunta.

PREVENÇÃO E SEGURANÇA

95. O art. 46 da LGPD estabelece que agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Destacamos, a seguir, algumas medidas de segurança da informação que devem ser observadas no tratamento de dados pessoais no contexto eleitoral e que podem ser encontradas também no *Guia Orientativo Segurança da Informação para Agentes de Tratamento de Pequeno Porte* editado pela ANPD[13].

Política de segurança da informação

96. A ANPD sugere que seja estabelecida pelo(a) agente de tratamento envolvido(a) no processo eleitoral uma política de segurança da informação, ainda que simplificada, contemplando controles relacionados ao tratamento de dados pessoais, por exemplo, controle de acesso à informação; coleta, compartilhamento, armazenamento e descarte de dados pessoais; uso de correio eletrônico e de outras plataformas de comunicação.

[13] *Guia Orientativo Segurança da Informação para Agentes de Tratamento de Pequeno Porte* disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte.

Conscientização e treinamento

97. Os recursos humanos no contexto do tratamento de dados pessoais durante o processo eleitoral são o fator preponderante para o sucesso das medidas que se referem à segurança da informação e à proteção de dados pessoais, uma vez que efetivamente são as pessoas que trabalham para agentes de tratamento que realizarão as atividades de tratamento. Assim, sugere-se que agentes de tratamento conscientizem suas funcionárias e seus funcionários sobre suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais.

98. Essa conscientização implica informar e sensibilizar todas as colaboradoras e todos os colaboradores, especialmente aqueles(as) diretamente envolvidos(as) na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD.

99. Algumas dicas úteis devem ser passadas às colaboradoras e aos colaboradores envolvidos(as) nas campanhas eleitorais, a fim de evitar ou minimizar os efeitos dos incidentes de segurança relacionados a dados pessoais. Tais dicas podem ser encontradas no *Guia de Segurança da Informação* elaborado pela ANPD, já mencionado.

Gerenciamento de contratos

100. Durante o estabelecimento dos contratos e termos de serviço, sugere-se que termos de confidencialidade sejam assinados com funcionárias, funcionários e empresas contratadas para que se comprometam a não divulgar informações confidenciais que envolvam dados pessoais, a fim de evitar exposições indevidas ou abusos de privilégio.

101. É indicado que seja realizado o gerenciamento de contratos e aquisições para atenção à segregação de funções e responsabilidades

entre as partes, com observância à LGPD e ao tratamento adequado dos dados pessoais.

102. No caso de terceirização de serviços de Tecnologia da Informação (TI), recomenda-se que sejam firmados com as fornecedoras ou com os fornecedores contratos que incluam, dentre outras, cláusulas de segurança da informação que assegurem a adequada proteção de dados pessoais.

103. Tais instrumentos poderão conter, por exemplo, cláusulas que tratam de:

- regras para fornecedoras ou fornecedores e parceiras ou parceiros;
- regras sobre compartilhamentos;
- relações entre controlador e operador;
- orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador.

Controle de acesso e gerenciamento de senhas

104. O controle de acesso consiste em uma medida de segurança para garantir que os dados sejam acessados somente por pessoas autorizadas. Ele consiste em processos de autenticação, autorização e auditoria.

- A autenticação identifica quem acessa o sistema ou os dados.
- A autorização determina o que a pessoa usuária identificada pode fazer.
- A auditoria registra o que foi feito pela pessoa usuária.

105. Sobre esse aspecto, a ANPD sugere que, caso o(a) agente de tratamento possua rede interna de computadores, seja implementado sistema de

controle de acesso aplicável a todas as pessoas usuárias, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais.

106. A premissa que deve ser aplicada é a do princípio do menor privilégio – necessidade de conhecer (*need to know*), ou seja, as pessoas usuárias de um sistema terão somente o nível de acesso necessário para a realização de suas atividades. Funções de alto nível, tais como as de administrador(a) de sistema, devem ser restringidas apenas àquelas pessoas funcionárias que necessitem exercer esse papel e sejam capazes de assumir essa responsabilidade.

107. Além disso, sugere-se que o sistema de controle de acesso seja configurado com funcionalidades que possam detectar e não permitir o uso de senhas que não respeitem certo nível de complexidade, como tamanho mínimo e uso de caracteres especiais. O uso de fatores múltiplos de autenticação (MFA/2FA) também é recomendado.

108. É importante, ainda, na implementação de sistemas de segurança, utilizar um adequado gerenciamento de senhas, evitando o uso de senhas padrão disponibilizadas pelos fornecedores de *software* ou *hardware* adquiridos, tendo em vista que geralmente os(as) atacantes utilizam essas senhas padronizadas (*default*) para tentativas de conexão e realização de ataques. As senhas precisam ser alteradas por outras com requisitos mais seguros.

109. Outra medida sugerida é que agentes de tratamento não permitam o compartilhamento de contas ou de senhas entre pessoas funcionárias, visto que isso é um vetor crítico de vulnerabilidade de segurança da informação.

Segurança dos dados pessoais armazenados

110. Inicialmente, para se evitar riscos de incidentes de segurança e outros comprometimentos, e em atenção ao princípio da necessidade previsto no art. 6º, III, da LGPD, agentes de tratamento devem coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, dentro do contexto eleitoral a que se referem, considerando sua utilidade imediata e concreta.

111. Além disso, sugere-se que agentes de tratamento que armazenam dados sensíveis implementem soluções que dificultem a identificação da pessoa titular, como as técnicas de pseudonimização[14]. Um exemplo dessa técnica é a criptografia.

112. Em relação às estações de trabalho, sugere-se que as pessoas funcionárias os funcionários sejam orientados acerca da importância das configurações de segurança, a fim de que não as desativem ou ignorem, inclusive quanto a restrições de acesso de determinados tipos de *sites*.

113. Um importante ponto a ser considerado é evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como *pendrives*, discos rígidos externos, dentre outros.

[14] Art. 13. [...]
§ 4º [...] pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Segurança das comunicações

114. No que se relaciona à segurança das comunicações, destaca-se a relevância de se utilizar conexões cifradas, com uso de protocolos seguros, como TLS/HTTPS, ou aplicativos com criptografia fim a fim. Isso se aplica também ao uso de *e-mails*, de dispositivos de trocas de mensagens e de redes sociais.

115. Recomenda-se, também, a utilização de sistemas de proteção de perímetro que monitorem, detectem, bloqueiem e previnam ameaças cibernéticas, incluindo *firewalls* de aplicação, sistemas de proteção a serviços de *e-mail*, com antivírus, *anti-spam* e filtros de *e-mail* integrados.

Manutenção de programa de gerenciamento de vulnerabilidades

116. Um dos pontos centrais na prevenção a vulnerabilidades é a manutenção de sistemas e aplicativos sempre atualizados, bem como a instalação de todas as correções de segurança disponíveis lançadas pelos desenvolvedores do sistema operacional e de aplicativos.

117. Uma medida adicional de segurança e detecção de comprometimentos consiste na adoção e atualização de *softwares* de antivírus ou *antimalwares*, que detectam, impedem e atuam na remoção de programas maliciosos, como vírus.

118. Além disso, é importante que esses mecanismos sejam mantidos em funcionamento e atualizados, que realizem varreduras periódicas nos dispositivos e que não possam ser desativados ou alterados pelas pessoas usuárias.

Medidas relacionadas ao uso de dispositivos móveis

119. Em relação aos dispositivos móveis, como *smartphones* e *laptops*, caso seu uso seja necessário para fins de tratamento de dados no contexto eleitoral, sugere-se que estejam sujeitos aos mesmos procedimentos de controle de acesso que os outros equipamentos de TI, como o uso da autenticação multifator (MFA) para acesso aos dispositivos e sistemas de informação, além de que sejam guardados em locais seguros quando não estiverem em uso.

120. Caso não seja possível implementar as medidas de segurança equivalentes às fornecidas pelos comitês de campanha ou congêneres, recomenda-se que dispositivos móveis pessoais não sejam utilizados no contexto eleitoral.

121. Tendo em vista que dispositivos móveis podem ser comprometidos mais facilmente em eventual perda ou roubo e que isso pode colocar em risco a guarda dos dados pessoais, sugere-se também que os(as) agentes avaliem e implementem funcionalidades que permitam apagar remotamente os dados pessoais relacionados à sua atividade de tratamento, devendo tal procedimento estar descrito no plano de resposta a incidentes.

Medidas relacionadas ao serviço em nuvem

122. Com relação à prestação de serviços de computação em nuvem, sugere-se que o(a) agente de tratamento tenha, em seu contrato, cláusula que contemple a segurança dos dados armazenados.

123. Além disso, a partir dos requisitos de segurança da informação definidos pelo(a) agente de tratamento, sugere-se que seja avaliado se o serviço oferecido pelo provedor do serviço em nuvem atende aos requisitos estabelecidos e se está em conformidade com requisitos da LGPD e orientações da ANPD.

124. Por fim, sugere-se que sejam especificados os requisitos para o acesso da pessoa usuária a cada serviço em nuvem utilizado, bem como que sejam usadas técnicas de autenticação multifator (MFA), por exemplo, aplicativos autenticadores ou *short message service* (SMS) para acesso aos serviços em nuvem relacionados a dados pessoais.

Tratamento de incidentes de segurança com dados pessoais

125. A ANPD disponibiliza, em sua página na internet, orientações sobre a comunicações de incidentes de segurança com dados pessoais[15], que também são aplicáveis ao tratamento de dados pessoais no contexto eleitoral.

126. No caso de um incidente de segurança da informação com dados pessoais, recomenda-se executar imediatamente o plano de resposta a incidentes[16], empreendendo as medidas imediatas para fazer cessar o incidente e empreender as medidas reativas ao restabelecimento seguro dos serviços.

127. Em seguida, recomenda-se avaliar internamente o incidente e os aspectos nele envolvidos, como natureza, categoria e quantidade de titulares de dados afetados, consequências concretas e prováveis. A partir daí, sugere-se elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (art. 6º, X, da LGPD).

128. Quanto à encarregada ou ao encarregado de dados pessoais, é importante que ele(a) seja comunicado(a) sobre o incidente o quanto

[15] Informações sobre incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD, disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

[16] O plano de resposta a incidentes faz parte do programa de governança em privacidade, conforme o art. 50, § 2º, I, da LGPD.

antes. Além disso, se o(a) agente de tratamento for operador, o controlador deverá ser comunicado(a).

129. O controlador deverá comunicar à ANPD e à pessoa titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante às pessoas titulares (LGPD, art. 48). Até o momento de publicação deste guia, não há distinções entre situações em que um(a) ou outro(a) deve ser comunicado(a), por isso tanto a ANPD quanto a pessoa titular devem receber comunicações quanto ao incidente. Contudo, o teor dessa comunicação poderá se distinguir, uma vez que para a ANPD são necessárias informações mais técnicas para que esta analise a gravidade do incidente (art. 48, § 2º), enquanto, para a pessoa titular, o mais importante é informar-lhe como se proteger contra eventuais consequências danosas, quais soluções estão sendo disponibilizadas para remediar danos já concretizados e como exercer seus direitos de titular. A comunicação à ANPD deve seguir as orientações[17] na seção Comunicação de incidentes de segurança e no formulário[18] de comunicação de incidente de segurança com dados pessoais à ANPD.

[17] Orientações disponíveis em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

[18] Formulário disponível em: https://www.gov.br/anpd/pt-br/assuntos/atual-formulario-de-comunicacao-de-incidentes-de-seguranca-com-dados-pessoais_01-03-2021-4.docx.

Atuação coordenada entre a ANPD e o TSE

130. A ANPD é o *órgão central de interpretação da LGPD* e do estabelecimento de normas e diretrizes para sua implementação, no que se inclui a deliberação administrativa, em caráter terminativo, sobre a interpretação da lei e suas próprias competências e casos omissos (art. 55-K, parágrafo único; art. 55-J, XX). Além disso, a autoridade nacional detém *competência exclusiva para aplicar as sanções administrativas previstas na LGPD*, com prevalência de suas competências sobre outras correlatas de entidades e órgãos da administração pública no que se refere à proteção de dados pessoais (art. 55-K).

131. Assim, a ANPD possui competência originária, específica e uniformizadora no que concerne à proteção de dados pessoais e à aplicação da LGPD, previsão legal que deve ser *interpretada de forma a se compatibilizar com a atuação de outros entes públicos* que possam eventualmente tratar sobre o tema.

132. O ponto central a ser considerado é *que um mesmo fato pode gerar repercussões em esferas jurídicas diferentes*. Por exemplo, o art. 18, § 8º, da LGPD deixa claro que, além de se dirigir à ANPD, as pessoas titulares de dados também poderão reclamar de controladores nos órgãos de defesa da consumidora e do consumidor. Já o art. 52, § 2º,

estabelece que as sanções da LGPD não substituem as previstas no Código de Defesa do Consumidor (CDC) e em legislação específica. Da mesma forma, o art. 22 enfatiza a possibilidade de defesa de interesses e direitos das pessoas titulares também no Poder Judiciário.

133. Esse mesmo princípio deve ser aplicado à seara eleitoral. Dessa forma, um mesmo fato poderá eventualmente ser objeto de fiscalização, orientação e aplicação de sanções tanto pela ANPD como pela Justiça Eleitoral, observados o contexto fático e as disposições jurídicas aplicáveis à hipótese.

134. A esse respeito, a LGPD (art. 55-J, § 3º) estabelece que *a ANPD deve atuar em coordenação e articulação com outros órgãos e entidades públicas*, visando assegurar o cumprimento de suas atribuições com maior eficiência e promover o adequado funcionamento dos setores regulados. O presente guia é fruto, justamente, da cooperação estabelecida entre a ANPD e o TSE, com o fim de fornecer orientações uniformes aos agentes de tratamento que atuam no campo eleitoral.

135. Outro parâmetro importante é o da *exigência de mínima intervenção* da ANPD ao impor condicionantes administrativas ao tratamento de dados pessoais por agente privado (art. 55-J, § 1º). No contexto eleitoral, essa determinação legal pode ser interpretada, de forma mais específica, como a necessidade de evitar a imposição de restrições que afetem a igualdade de oportunidades no processo eleitoral ou, ainda, como a exigência de menor interferência possível no debate democrático[19].

[19] Conforme preceito análogo previsto na legislação eleitoral (art. 38, Res.-TSE nº 23.610/2019), "a atuação da Justiça Eleitoral em relação a conteúdos divulgados na internet deve ser realizada com a menor interferência possível no debate democrático (Lei nº 9.504/1997, art. 57-J)".

136. A ANPD deve, ainda, atuar *de forma proporcional aos riscos e danos envolvidos em um determinado caso*. A título de exemplo, as sanções administrativas mais graves, que implicam suspensão ou proibição da atividade de tratamento de dados pessoais, somente podem ser aplicadas de forma gradativa, isto é, após ter sido aplicada, no mesmo caso concreto, uma sanção mais leve, como multa ou publicização da infração (art. 52, § 6º, da LGPD), observados, ainda, os demais critérios previstos no art. 52, § 1º, dessa lei.

137. Por fim, *a ANPD não possui competência para atuar em matérias submetidas à competência exclusiva da Justiça Eleitoral*, tais como: (i) a aplicação de sanções previstas na legislação eleitoral; (ii) a moderação de conteúdos com finalidade político-eleitoral; (iii) a fiscalização sobre a propaganda eleitoral; e (iv) a concessão de direito de resposta.

138. Nos tópicos seguintes, serão analisadas obrigações específicas previstas na legislação eleitoral que possuem uma interface próxima com princípios e direitos previstos na LGPD. Além de recomendações baseadas na legislação de proteção de dados, serão também apresentados exemplos hipotéticos com o fim de auxiliar a compreensão do tema e da atuação coordenada entre a ANPD e o TSE.

Utilização de base de dados coletada previamente à vigência da LGPD

139. Toda operação de tratamento de dados sujeita à LGPD deve ser realizada com respeito às suas regras e princípios. O mesmo ocorre com bases de dados legadas, isto é, aquelas constituídas antes da vigência da LGPD, que podem estar em desconformidade com seus dispositivos. Nesse caso, ainda que o art. 63 da lei preveja a possível

regulamentação futura dessas bases, *recomenda-se que elas sejam progressivamente adequadas às obrigações estabelecidas pela LGPD*.

140. Assim, agentes de tratamento que possuem dados pessoais coletados em momento anterior à vigência da LGPD devem avaliar, para novos tratamentos, qual a base legal mais adequada para a operação pretendida, a depender do contexto, da finalidade e da natureza do dado a ser tratado. Devem ser observados, ainda, os direitos das pessoas titulares e os princípios estipulados na lei, tais como finalidade, necessidade, adequação e transparência, conforme as orientações apresentadas neste guia.

141. Em todos os casos, o registro das operações e a adoção de outras medidas de transparência e prestação de contas assumem relevante função durante a adequação das bases de dados legadas e para a realização de operações de tratamento envolvendo dados coletados antes da vigência da LGPD.

Exemplo 7 – Utilização de base de dados obtida em eleições anteriores

Candidata constituiu uma base de dados pessoais (nome, telefone celular, endereço e *e-mail*) para fins de *marketing* eleitoral nas eleições de 2016, antes da vigência da LGPD.

Para uso dessa base de dados nas eleições de 2022, deverá ser identificada a base legal mais apropriada à hipótese, nos termos dos arts. 7º ou 11 da LGPD, assim como os direitos das pessoas titulares e os princípios constantes no art. 6º da LGPD.

Cessão, doação e venda de bases de dados

142. A legislação eleitoral (art. 57-E, § 1º, da Lei 9.504/1997; art. 31, § 1º, Res.-TSE nº 23.610/2019) proíbe a venda de cadastro de endereços

eletrônicos em favor de candidatas, candidatos, partidos políticos, coligações e federações, por pessoas físicas ou jurídicas. Proíbe também a doação, cessão e utilização de dados pessoais em favor de candidatas, candidatos, partidos políticos, coligações e federações pela administração pública e por pessoa jurídica de direito privado[20].

143. Eventual infração pode ser penalizada pela Justiça Eleitoral com multa de até R$30.000,00[21], bem como a cassação do registro ou diploma, caso caracterizado o abuso do poder político ou econômico e o uso indevido dos meios de comunicação[22].

144. Ao regulamentar a matéria, o art. 31, § 3º, da Res.-TSE nº 23.610/2019 estabelece que a violação a essa regra eleitoral não afasta a aplicação de outras sanções previstas em lei, com expressa referência à LGPD. Destaca-se, ainda, a previsão do § 4º do mesmo artigo de que "[...] o tratamento de dados pessoais, inclusive a utilização, doação ou

---

[20] Para ver o rol completo, verificar o art. 24 da Lei 9.504/1997 ou, ainda, a nota de rodapé 1 deste guia.

[21] Art. 57-E, § 2º, da Lei nº 9.504/1997 e art. 31, § 2º, da Res.-TSE nº 23.610/2019.

[22] Lei Complementar nº 64/1990, art. 22:
Art. 22. Qualquer partido político, coligação, candidato ou Ministério Público Eleitoral poderá representar à Justiça Eleitoral, diretamente ao Corregedor-Geral ou Regional, relatando fatos e indicando provas, indícios e circunstâncias e pedir abertura de investigação judicial para apurar uso indevido, desvio ou abuso do poder econômico ou do poder de autoridade, ou utilização indevida de veículos ou meios de comunicação social, em benefício de candidato ou de partido político, obedecido o seguinte rito:
[...] XIV - julgada procedente a representação, ainda que após a proclamação dos eleitos, o Tribunal declarará a inelegibilidade do representado e de quantos hajam contribuído para a prática do ato, cominando-lhes sanção de inelegibilidade para as eleições a se realizarem nos 8 (oito) anos subsequentes à eleição em que se verificou, além da cassação do registro ou diploma do candidato diretamente beneficiado pela interferência do poder econômico ou pelo desvio ou abuso do poder de autoridade ou dos meios de comunicação, determinando a remessa dos autos ao Ministério Público Eleitoral, para instauração de processo disciplinar, se for o caso, e de ação penal, ordenando quaisquer outras providências que a espécie comportar. (Redação dada pela Lei Complementar nº 135, de 2010).

cessão destes por pessoa jurídica ou por pessoa natural, observará as disposições da Lei nº 13.709/2018".

145. Assim, para além da fiscalização exercida pela Justiça Eleitoral, agentes de tratamento devem observar as disposições da LGPD. Por isso, também se submetem às determinações da ANPD, seja no caso específico de venda, utilização, doação ou cessão de dados pessoais, seja, de forma mais geral, nas demais hipóteses de tratamento de dados pessoais.

Exemplo 8 – Banco de dados de pessoa jurídica de direito público

Órgão público cede dados pessoais de pessoas beneficiárias de programa social para candidato, que os utiliza para fins de formação de perfis e de propaganda eleitoral enviada por aplicativos de mensagens instantâneas e impulsionada em redes sociais.

Entre outras medidas, a Justiça Eleitoral poderá determinar a suspensão de acesso ao conteúdo veiculado, além de aplicar multa de até R$30.000,00 (arts. 57-I e 57-E, § 2º, Lei 9.504/1997). A ANPD também poderá investigar o fato, a fim de apurar a compatibilidade do tratamento com a LGPD, considerando, entre outros pontos, a base legal utilizada, a observância dos princípios da finalidade, da necessidade e da transparência no caso, bem como o respeito aos direitos das pessoas titulares. Conforme o caso, pode emitir orientações ao controlador ou aplicar alguma das sanções administrativas previstas no art. 52 da LGPD.

Envio de mensagens eletrônicas e instantâneas

146. A propaganda eleitoral pode ser realizada, entre outras formas, pelo envio de "mensagem eletrônica para endereços cadastrados gratuitamente pelo candidato, pelo partido político ou pela coligação,

observadas as disposições da Lei Geral de Proteção de Dados quanto ao consentimento do titular" (Res.-TSE nº 23.610/2019, art. 28, III).

147. A propaganda também pode ser enviada por aplicativos de mensagens instantâneas, vedada a contratação de disparo em massa "*sem anuência do destinatário*". Em qualquer caso, deve ser assegurada a possibilidade de "*descadastramento*" (Res.-TSE nº 23.610/2019, art. 28, IV; arts. 33 e 34)[23].

148. A atividade de coletar dados pessoais, visando ao posterior envio de mensagens publicitárias às interessadas ou aos interessados, é uma espécie de tratamento de dados pessoais, sujeito às disposições da LGPD, incluindo, em particular, a necessidade de identificação da base legal apropriada para o caso. Os dispositivos citados da legislação eleitoral indicam a necessidade de observância às disposições da LGPD quanto ao consentimento, estabelecendo a obtenção de "anuência" do destinatário das mensagens como condição de validade para o disparo em massa de mensagens instantâneas. Também é conferida à pessoa titular a prerrogativa de revogar o consentimento a qualquer tempo, mediante a solicitação de "descadastramento". Note-se que as mensagens eletrônicas e as mensagens instantâneas enviadas consensualmente por pessoa natural diversa da candidata ou do candidato, de forma privada ou em grupos restritos de participantes, não se submetem à obrigação de descadastramento, tampouco às normas eleitorais sobre propaganda (art. 33, § 2º, da Res.-TSE nº 23.610/2019).

149. Portanto, em atendimento à legislação eleitoral vigente, o tratamento de dados pessoais visando ao *envio de mensagens eletrônicas e instantâneas com conteúdo de propaganda eleitoral* deve ser realizado com fundamento *em alguma das bases legais previstas*

[23] Não estão submetidas a esse regramento "as mensagens eletrônicas e as mensagens instantâneas enviadas consensualmente por pessoa natural, de forma privada ou em grupos restritos de participantes [...]" (art. 33, § 2º, Res.-TSE nº 23.610/2019).

nos arts. 7º e 11 da LGPD. Caso, no entanto, a atividade pretendida envolva o *disparo em massa de mensagens instantâneas, a base legal será necessariamente o consentimento*.

150. Nesse caso, o(a) agente de tratamento deve sempre respeitar a manifestação de vontade da pessoa titular, seja no momento de obtenção do consentimento ou de sua revogação. Ademais, salvo nas hipóteses previstas na legislação, o tratamento dos dados não deve ser ampliado para além dos termos e finalidades consentidos pela pessoa titular.

151. Como demonstrado neste guia, para ser válido, o consentimento deve ser livre, informado e inequívoco. Adicionalmente, caso o tratamento envolva dados sensíveis, o consentimento deverá ser fornecido de forma específica e destacada. Em qualquer hipótese, devem ser apresentadas à pessoa titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, conforme o art. 9º da LGPD.

152. Caso essas informações não sejam apresentadas à pessoa titular previamente e com transparência ou, ainda, se forem apresentadas informações com conteúdo enganoso ou abusivo, o consentimento eventualmente concedido será considerado nulo (art. 9º, § 1º, da LGPD). Por essa razão, o tratamento dos dados padecerá de irregularidade (art. 8º, § 3º, da LGPD), o que poderá ser objeto de fiscalização e sanção pela ANPD e pela Justiça Eleitoral no âmbito de suas respectivas esferas de competência.

153. O consentimento pode ser revogado a qualquer momento (art. 8º, § 5º, da LGPD). Para assegurar o exercício desse direito, o(a) agente de tratamento deve disponibilizar procedimento gratuito e facilitado, por meio do qual a pessoa titular possa manifestar sua vontade (art. 8º, § 5º, da LGPD). Efetuada a solicitação, o tratamento deve ser encerrado

e os dados da pessoa titular, eliminados, ressalvadas as hipóteses de conservação previstas no art. 16 da LGPD. Essas disposições da LGPD são complementadas e reforçadas por normas eleitorais específicas, que conferem à destinatária ou ao destinatário de mensagens publicitárias o direito de solicitar o seu "descadastramento", a ser providenciado pelo(a) remetente, no prazo de até 48 horas (art. 57-G, Lei nº 9.504/1997).

154. Para atender a essas determinações legais, *recomenda-se incluir, na própria mensagem encaminhada, orientações de fácil visibilidade sobre como a pessoa titular pode revogar o consentimento* e ter os seus dados excluídos da lista de envio de mensagens. O exercício dessa opção deve ser efetuado *sempre de modo facilitado e gratuito*, por exemplo, mediante simples "clique" em *link* disponibilizado na mensagem.

Exemplo 9 – Envio de mensagens eletrônicas a eleitores(as)

Candidato realiza evento de campanha eleitoral. Voluntárias e voluntários convidam as pessoas interessadas a preencher formulário e fornecer dados pessoais de identificação e contato com vistas a participar de sorteio de brindes. Nenhuma outra informação é apresentada. Os dados coletados são compartilhados com agência de marketing *e, alguns dias depois, as eleitoras e os eleitores passam a receber mensagens eletrônicas com conteúdo de propaganda eleitoral. As mensagens esclarecem que o descadastramento poderá ser efetuado, porém sem indicar o procedimento para tanto.*

A atividade de coletar dados pessoais visando ao posterior envio de mensagens publicitárias às pessoas interessadas constitui tratamento de dados pessoais, sujeito às disposições da LGPD. Por isso, caso o tratamento pretendido tenha por base legal o consentimento, é preciso atentar para que este seja obtido de forma livre, informada e inequívoca, devendo ser apresentadas à pessoa titular informações claras, precisas e facilmente

acessíveis sobre a realização do tratamento, incluindo aquelas sobre sua finalidade específica e o compartilhamento realizado.

No caso concreto, conforme o art. 9º, § 1º, da LGPD, o consentimento deve ser considerado nulo, visto que as informações fornecidas tinham conteúdo enganoso ou incompleto, induzindo as pessoas interessadas a preencher o formulário sem informar os usos secundários para a campanha eleitoral. Além disso, não foram apresentadas, previamente e com transparência, outras informações exigidas pela lei.

Cabe destacar ainda que, em desacordo com a LGPD e com a legislação eleitoral, não foi fornecido à pessoa titular procedimento gratuito e facilitado para revogar o consentimento e se descadastrar.

Por fim, é de se notar que, ainda que se pretendesse invocar outra base legal para o tratamento, igualmente seria necessário prestar informações às pessoas titulares dos dados pessoais sobre a finalidade da coleta, até mesmo para poder avaliar se o tratamento que efetivamente venha a ser dado será ou não compatível com a finalidade informada à pessoa titular.

Impulsionamento de conteúdo

155. Partidos políticos, coligações, candidatas e candidatos também podem realizar propaganda eleitoral mediante "impulsionamento de conteúdo" na internet (art. 57-C da Lei nº 9.504/1997). Trata-se de mecanismo que permite publicar e promover um anúncio em serviços de aplicações de internet, especialmente em redes sociais e serviços de busca[24]. O impulsionamento deve observar uma série de

[24] De acordo com a Res.-TSE nº 23.610/2019 (art. 37, XIV), impulsionamento de conteúdo é "o mecanismo ou serviço que, mediante contratação com os provedores de aplicação de internet, potencializem o alcance e a divulgação da informação para atingir usuários que, normalmente, não teriam acesso ao seu conteúdo, incluída entre as formas de impulsionamento a priorização paga de conteúdos resultantes de aplicações de busca na internet, nos termos do art. 26, § 2º, da Lei nº 9.504/1997".

regras previstas na legislação eleitoral, entre as quais a contratação com provedor com sede e foro no país, a finalidade exclusiva de promover ou beneficiar candidatas ou candidatos ou suas agremiações e a identificação inequívoca como propaganda eleitoral.

156. Além disso, *é necessária a observância das disposições aplicáveis da LGPD*, tendo em vista que *o impulsionamento de conteúdo é sempre realizado mediante o tratamento de dados pessoais*. De fato, a propaganda em redes sociais e serviços de busca é segmentada, no sentido de que pressupõe a seleção do público-alvo a partir de determinados perfis, formados com elevado índice de precisão com base na combinação de dados pessoais detidos por partidos, candidatas, candidatos e prestadoras ou prestadores de serviço, como as plataformas digitais.[25]

157. É possível, por exemplo, direcionar um anúncio especificamente para eleitoras com elevado padrão de renda e escolaridade, residentes em uma dada região, com um ou dois filhos. Esse tipo de perfil comportamental, que está na base do microdirecionamento da publicidade *on-line*, constitui dado pessoal, já que associado a uma pessoa natural identificada, no caso, uma usuária ou um usuário de um provedor de aplicação de internet.[26]

158. Entre outros aspectos que devem ser observados, conforme o exposto neste guia, destacam-se aqui quatro pontos essenciais para se avaliar a conformidade do impulsionamento de conteúdo com a LGPD.

---

[25] CRUZ, F. B. *et al*. *Direito eleitoral na era digital*. Belo Horizonte: Letramento, 2018, p. 172; Information Commissioner's Office. *Democracy disrupted? Personal information and political influence*, 2018, p. 27-28. Disponível em: https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf. Acesso: 7 out. 2021.

[26] Conforme o art. 12, § 2º, da LGPD: "poderão ser igualmente considerados como dados pessoais, para os fins desta lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada".

159. O primeiro é a necessidade *de identificar a base legal aplicável*, efetuando-se o devido registro da análise e da operação realizadas. Considerando que a legislação eleitoral não definiu a base legal que autoriza o impulsionamento de conteúdo, a análise deve ser feita de acordo com o contexto e o caso concreto, tendo em vista as categorias de dados utilizadas, a forma de coleta e os(as) agentes envolvidos(as) na operação, entre outros elementos relevantes.

160. De forma geral, *o impulsionamento de conteúdo poderá ser realizado com fundamento nas bases legais do consentimento ou do legítimo interesse*, observados o contexto fático e os requisitos legais aplicáveis à hipótese. A título de exemplo, um partido político pode disponibilizar em seu sítio eletrônico um cadastro para as pessoas interessadas, do qual consta a opção de consentir ou não com a utilização de suas informações para a promoção de anúncios em uma rede social. O mesmo partido político pode recorrer ao legítimo interesse para fundamentar o direcionamento de anúncios a pessoas que interagiram com sua página em uma rede social. Caso se opte por esta última base legal, que é admitida somente quando não abrangidos dados sensíveis, atenção especial deve ser dada às regras previstas no art. 10 da LGPD, sempre respeitando as legítimas expectativas e os direitos e liberdades fundamentais da pessoa titular. A esta também deve ser assegurado o direito de se opor ao tratamento (art. 18, § 2º), hipótese na qual a exibição do anúncio e o tratamento de seus dados pessoais devem ser interrompidos.

161. O segundo ponto é a *transparência* do tratamento. Avisos e políticas de privacidade devem ser disponibilizados por partidos, candidatas, candidatos, coligações e plataformas digitais em locais de fácil acesso, além de elaborados com linguagem simples e com informações claras e precisas, conforme as orientações apresentadas neste guia.

É importante considerar que o funcionamento da publicidade *on-line* e a correlata utilização de dados pessoais é de difícil compreensão para a cidadã ou o cidadão comum, razão pela qual constitui uma boa prática a utilização de recursos visuais que simplifiquem e facilitem o seu entendimento.

162. A terceira observação é quanto às práticas de formação e utilização de *perfil comportamental*. Caso a criação desses perfis seja realizada a partir da tomada de decisões baseadas unicamente em tratamento automatizado de dados pessoais, a pessoa titular de dados terá direito a solicitar a revisão dessas decisões (art. 20 da LGPD). Além disso, sempre que solicitado, o controlador deverá fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados o segredo comercial e o industrial. Caso esses segredos sejam alegados como fundamentação de recusa em fornecer as informações solicitadas, a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios no tratamento automatizado de dados pessoais (art. 20, § 2º, da LGPD).

163. Por fim, os *direitos das pessoas titulares* devem ser respeitados. Os(as) agentes de tratamento, incluindo partidos, candidatas, candidatos, coligações, federações e plataformas digitais, devem dar preferência a mecanismos intuitivos e de fácil acesso, que confiram à pessoa titular a efetiva possibilidade de controlar o uso de seus dados. Nessa linha, podem ser disponibilizadas ferramentas simplificadas que viabilizem, entre outras funcionalidades, o bloqueio de anúncios indesejados e a apresentação de requerimentos diversos, como nos casos de descadastramento, eliminação de dados, revogação de consentimento ou de oposição ao tratamento.

Exemplo 10 – Impulsionamento de conteúdo e formação de perfis de eleitores

Candidata contrata serviço de provedor de aplicação de internet visando ao impulsionamento de conteúdo em rede social. Para tanto, utiliza banco de dados pessoais próprio, coletados em eventos da campanha ou em razão de interações em sua página na rede social. Também utiliza cadastro de endereços eletrônicos vendido por uma consultoria de análise de dados. Essa lista inicial, com nome, e-mail *e números de telefone, é fornecida ao provedor, que, por sua vez, identifica as contas dessas pessoas titulares em redes sociais. A partir daí, são criados "perfis de eleitoras e de eleitores" baseados nas informações identificadas nessas redes, considerando aspectos demográficos, de gênero, interesses, opiniões políticas, crenças religiosas e localização, entre outros.*

A venda de cadastro de endereços eletrônicos é prática vedada pela legislação eleitoral, razão pela qual os dados em questão não poderiam ser utilizados pelo partido político.

Quanto aos demais dados pessoais, o tratamento pelo partido político ou pelo provedor de aplicação será legítimo desde que observados os direitos das pessoas titulares, os princípios da LGPD e identificada a base legal apropriada, o que deve ser objeto de justificativa documentada. Em regra, na hipótese de impulsionamento de conteúdo, o tratamento de dados pessoais pode ser realizado com base no consentimento ou no legítimo interesse.

Já no caso específico da formação de perfis de eleitoras e de eleitores, o consentimento seria mais apropriado, tendo em vista a impossibilidade de utilização do legítimo interesse quando o tratamento abrange dados sensíveis. É o que ocorre no exemplo citado, haja vista o tratamento de informações relativas a crenças religiosas e opiniões políticas das pessoas titulares.

CONSIDERAÇÕES FINAIS

164. Com esta primeira versão do *Guia Orientativo*, pretendemos reunir esforços iniciais do TSE e da ANPD no sentido de sistematizar os impactos da LGPD no processo eleitoral, para que partidos, candidatas, candidatos, coligações e federações estejam em melhores condições de efetuar tratamento adequado, responsável e seguro de dados pessoais, bem como para que a pessoa titular de dados tenha informações mais facilitadas sobre seus direitos.

165. Não é propósito deste guia obstar legítimas ações de agentes de tratamento no exercício de direitos político-eleitorais, mas sim elucidar como essas ações podem ser empreendidas com responsabilidade, transparência e de forma a serem respeitadas as disposições trazidas pela LGPD.

166. Além das exigências legais e regulamentares que já se apresentam de forma mais clara e impositiva, procuramos traçar recomendações de boas práticas que serão capazes de traduzir a boa-fé de candidatas, candidatos, partidos, coligações e federações partidárias no tratamento de dados pessoais.

167. Eventual imprecisão ou omissão poderá ser sanada em próximas versões deste guia, com a colaboração dos partícipes do processo eleitoral, no que se incluem as próprias pessoas titulares de dados pessoais.

168. Ademais, novas leis e regulamentos poderão induzir necessárias reinterpretações de preceitos normativos hoje em vigor. Também

o Poder Judiciário, na interpretação desse novo quadro normativo, poderá chegar a conclusões diversas quanto a determinados aspectos do tema. Por ora, este guia pretende responder algumas das perguntas que inquietam agentes eleitorais e conferir maior segurança jurídica na aplicação de normas legais protetivas de dados pessoais.

169. Esperamos ter sido capazes de contribuir com o manejo seguro de dados pessoais pelos(as) agentes de tratamento no contexto eleitoral, bem como com a construção de uma democracia saudável e respeitadora dos dados pessoais de suas cidadãs e de seus cidadãos.

Esta obra foi composta nas fontes George Rounded Semibold, corpo 16
e Calibri (Regular, Bold e Italic), corpo 12, entrelinhas de 14,4 pontos.