PROTEÇÃO DE DADOS NAS ELEIÇÕES

democracia e privacidade

Heloisa Massaro (**coord.**)
Bruna Santos
Bruno Bioni
Francisco Brito Cruz
Mariana Rielli
Rafael Sonda Vieira

Grupo de Estudos em Proteção de Dados e Eleições | 2020

SETEMBRO/2020

APOIO

INTERNETLAB
pesquisa em direito e tecnologia

DataPrivacyBR RESEARCH

INSTITUTO LIBERDADE DIGITAL

PROTEÇÃO DE DADOS NAS ELEIÇÕES

democracia e privacidade

INTEGRANTES DO
GRUPO DE ESTUDOS EM PROTEÇÃO DE DADOS E ELEIÇÕES 2020

Bruno Bioni
Bruna Santos
Clarice Tavares
Diogo Rais
Ester Borges
Francisco Brito Cruz
Jacqueline Abreu
Heloisa Massaro
Mariana Rielli
Rafael Sonda Vieira

COMO CITAR

Massaro, Heloisa; Santos, Bruna; Bioni, Bruno; Brito Cruz, Francisco; Rielli, Mariana; Vieira, Rafael. **Proteção de Dados nas Eleições: democracia e privacidade.** Grupo de Estudos em Proteção de Dados e Eleições, 2020.

APOIO

INTERNETLAB pesquisa em direito e tecnologia
DataPrivacyBR RESEARCH
INSTITUTO LIBERDADE DIGITAL

ÍNDICE

1 APRESENTAÇÃO

SOBRE OS AUTORES

Este documento é o produto do Grupo de Estudos em Proteção de Dados e Eleições, que reuniu, ao longo de sete meses, membros de diferentes organizações, como InternetLab, Data Privacy Brasil e Instituto Liberdade Digital, além de pesquisadores independentes.

O objetivo do grupo foi discutir, a partir das diferentes perspectivas trazidas pelos participantes, questões sensíveis sobre a proteção de dados pessoais no contexto eleitoral, considerando elementos como a aprovação e eventual vigência da Lei Geral de Proteção de Dados (LGPD) e sua menção explícita pela Resolução nº 23.610/2019.

Os seguintes temas foram debatidos ao longo dos meses pelo grupo: competência para apreciar violações a dados pessoais nas eleições, a extensão da aplicação da LGPD ao contexto eleitoral, e *compliance* e *accountability* eleitoral diante das normas de proteção de dados pessoais.

OBJETIVO DESTE DOCUMENTO

O nosso objetivo é organizar a discussão sobre proteção de dados pessoais em períodos eleitorais, demonstrando, a partir de situações concretas, a importância de se pensar de forma responsável e pragmática sobre o uso massivo de dados pessoais nesse contexto e a necessidade de se resguardar os direitos dos eleitores.

Assim, não queremos oferecer respostas prontas para cada uma das questões que permeiam a proteção de dados nas eleições deste ano, até porque muitos desses questionamentos seguem em aberto e dependem de interpretações que escapam às nossas pretensões no momento. Em vez disso, buscamos organizar o ferramental necessário para que decisões sejam realizadas em seu devido contexto, avaliando os seus custos e riscos.

Os atores envolvidos nesse ecossistema precisam tomar decisões informadas sobre como se adequar às exigências de uma sociedade cada vez mais preocupada com a proteção dos seus dados pessoais.

2 DADOS PESSOAIS E CAMPANHAS POLÍTICO-ELEITORAIS

2.1. O USO DE DADOS PESSOAIS POR CAMPANHAS ELEITORAIS: UMA REALIDADE CRESCENTE

É comum ouvir que vivemos em uma sociedade e uma economia movida a dados e que os dados pessoais "são o novo petróleo". Circulando no senso comum, essas colocações revelam uma percepção generalizada de que os dados pessoais (aqueles que nos identificam diretamente ou que têm o potencial de nos identificar) estão cada vez mais presentes em todos os campos da vida social e econômica.

Não é surpresa que, no caso das campanhas eleitorais, isso também seja verdade. Se campanhas têm a necessidade pragmática de se comunicar com eleitores nos meios em que eles podem ser encontrados, informações sobre tais eleitores sempre foram peças-chave para estes esforços, o que dá especial importância ao desenvolvimento e uso de tecnologias que lhes garantam vantagens estratégicas. Este movimento na direção de agregar tecnologias cada vez mais complexas de tratamento de dados pessoais às campanhas foi significativamente notado pela literatura especializada já há algum tempo.[1]

Nas últimas décadas, mudanças no cenário de produção, circulação e consumo de informação foram decisivas para que o uso de dados se tornasse mais relevante.[2] Isto ocorre a partir da adoção massiva da internet e de suas plataformas de comunicação digital, de um lado, e do aumento exponencial da capacidade de coleta, armazenamento e processamento de dados, de outro.

Neste movimento, a dinâmica da comunicação da TV e do rádio - de um para muitos - deu lugar a outras possibilidades de interação entre usuários em rede. A abertura dessas possibilidades de maior direcionamento de conteúdo com base em tecnologias de tratamento de dados pessoais não ocorre apenas por conta do uso de plataformas de redes sociais, mas de uma ampla gama de novos serviços e fornecedores disponíveis a campanhas. Como são fenômenos marcados por uma dinâmica competitiva, vantagens de uma campanha em um processo

1 Nickerson, David W.; Rodgers, Todd. Political Campaigns and Big Data. *The Journal of Economic Perspectives*, v. 28, n. 2, p. 51-74, 2014; Chester Jeff.; Montgomery, Kathryn. C. The role of digital marketing in political campaigns. Internet Policy Review, vol. 6, n. 4, 2017; Bennett, Colin. J.; LYON, David. Data-driven elections : implications and challenges for democratic societies. *Internet Policy Review*, v. 8, n. 4, 2019.

2 Brito Cruz, Francisco (coord.); Massaro, Heloisa; Oliva, Thiago; Borges, Ester. *Internet e eleições no Brasil: diagnósticos e recomendações*. InternetLab, São Paulo, 2019.

eleitoral são observadas de perto por seus adversários, o que acentua a busca por novas ferramentas e tecnologias.

Nesta nova fase da comunicação política o tratamento de dados pessoais é cada vez mais essencial. Informações como endereço, por exemplo, permitem uma comunicação voltada para o trabalho de um candidato em uma determinada região; "likes" em uma rede social, por sua vez, demonstram interesses de um indivíduo. Estabelecidas capacidades de coleta e tratamento cada vez melhores, dados pessoais são um insumo estratégico para que campanhas e candidatos conheçam seu eleitorado e cheguem mais perto dele. Usando tais informações as campanhas conseguem planejar o uso mais eficiente de seus recursos, ganhar poder de convencimento sobre determinados nichos de eleitores ou, ainda, entender movimentos de comportamento do eleitorado decisivos para mudanças de estratégia.

Todo esse cenário de digitalização e recurso aos dados pessoais como alimento de campanhas e da relação entre eleitores e eleitos é acentuado em um contexto de pandemia, que restringe as interações sociais e as atividades de campanha presenciais. Com isso, o papel da internet e das redes sociais como ferramenta de campanha é reforçado.

Por um lado, essa comunicação mais personalizada pode favorecer o engajamento do eleitor com pautas que lhe são mais relevantes, facilitando uma maior aproximação entre o eleitor e a campanha, que passa a contar com a possibilidade de se dirigir à uma parcela do eleitorado que tenha maior afinidade com seu projeto político, estabelecendo uma comunicação mais relevante para estes eleitores. As potencialidades de uma comunicação mais direcionada já foram, inclusive, uma promessa de maior eficiência na comunicação para campanhas menores com recursos limitados.

No entanto, isso não ocorre sem problemas, evidentemente. O tratamento de dados pessoais, por essência, implica riscos para o indivíduo a que eles se referem (o chamado "titular"), o que tem como contrapartida a criação de dispositivos legais que visam protegê-los contra o uso indevido e abusivo de suas informações. Além disso, a depender de como essas ferramentas e capacidades de uso de dados pessoais são incorporadas às estratégias de campanha, elas podem fomentar divisões e polarização no eleitorado, além de possibilitar que mensagens contraditórias sejam veiculadas de modo a enganar o eleitor e reduzir a transparência sobre a totalidade das campanhas.

Casos como o da empresa *Cambridge Analytica* são bastante ilustrativos de como dados pessoais podem ser coletados por vias inadequadas e utilizados com a finalidade de manipular eleitores e a opinião pública, prejudicando a própria democracia. É essencial entender que as vantagens estratégicas buscadas por campanhas não podem estar fundamentadas em práticas pouco transparentes ou enganosas. Isso evidencia o caráter bastante sensível do contexto eleitoral, especificamente, quando se fala da proteção de dados pessoais.

2.2. A IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS: GARANTIA AO ELEITOR E SEGURANÇA PARA AS CAMPANHAS

Uma maior atenção dedicada à proteção dos dados pessoais no contexto eleitoral representa um ganho tanto para os eleitores quanto para as próprias campanhas e candidatos. Mais do que uma questão de respeito a leis em vigor, ela é fundamental para que a integridade do processo eleitoral seja garantida e para que a representação política seja fruto de um processo democrático em forma e em conteúdo.

De um lado, eleitores se beneficiam quando seus dados são protegidos e tutelados por regras e princípios que regulam o poder que emerge do uso de suas informações pessoais. Isto significa garantir que quem os utiliza tenha uma justificativa adequada para tanto, que haja salvaguardas contra usos inadequados e incidentes de segurança e que direitos como acesso aos dados, retificação, dentre outros, sejam plenamente assegurados. Em suma, regras de proteção de dados pessoais ***regulam o poder que se tem sobre alguém que advém do tratamento de informações pessoais de sua titularidade***.
Este regime deve ser visto como uma decorrência da proteção constitucional da privacidade e de uma série de outras garantias fundamentais, como a liberdade de associação e de informação.

Por outro lado, as próprias campanhas e candidatos também devem se beneficiar de um emprego mais responsável dos dados pessoais em suas atividades. Isso porque a proteção de dados não significa uma proibição do seu uso, mas sim a criação de diretrizes que coloquem todos - quem usa os dados e quem é o titular dos dados - na mesma página, tornando esse fluxo mais fácil e seguro. Nesse sentido, um regime de proteção de dados garante às campanhas um caminho seguro para estratégias que envolvam o uso de dados pessoais de eleitores, possibilitando

que se busque uma comunicação mais eficiente e relevante de forma transparente e com a mitigação dos riscos que podem advir dessas práticas. Regras de proteção de dados pessoais reforçam, assim, a ***igualdade de chances*** entre as candidaturas - princípio basilar na gestão de processos eleitorais - e a segurança jurídica das atividades por elas empreendidas.

2.3. A LEI GERAL DE PROTEÇÃO DE DADOS SERÁ APLICADA NAS ELEIÇÕES DE 2020?

No Brasil, é a LGPD que define um regime geral de proteção de dados, trazendo princípios e regras para o tratamento de dados pessoais. Aprovada em 2018, a lei entrou em vigor neste ano. No entanto, ainda há alguma controvérsia quanto à sua aplicabilidade para as eleições municipais de 2020. No momento em que este documento foi organizado, o cenário para a vigência da LGPD era o seguinte: em 26 de agosto de 2020, o Senado Federal analisou a Medida Provisória nº 959, que, dentre outras coisas, adiava a vigência da LGPD para 2021, e entendeu que esse tema já havia sido apreciado anteriormente e, portanto, que estava prejudicado. Em 17 de setembro de 2020, a Presidência da República sancionou a Medida Provisória nº 959, dando vigência para a LGPD a partir de 18 de setembro de 2020.

Mas isso significa que ela se aplicará às próximas eleições?

Há argumentos para se defender que a LGPD estaria sujeita ao princípio da anualidade eleitoral, estabelecido no artigo 16 da Constituição Federal, e não se aplicaria para estas eleições. Como forma de proteger a integridade do processo eleitoral contra tentativas de alterar as regras do jogo que beneficiem ou prejudiquem candidatos, a Constituição estabelece que a "lei que alterar o processo eleitoral" não se aplica à eleição que ocorra até um ano da data de sua vigência. Como a vigência da LGPD se iniciou em 18 de setembro de 2020, muito menos do que um ano até as eleições marcadas para 15 de novembro, as normas da LGPD não seriam aplicáveis aos candidatos, partidos e coligações nestas eleições.

Por outro lado, enquadrar a LGPD como uma lei que altera o "processo eleitoral" seria distorcer o escopo da lei, que, na verdade, estabelece um regime geral para a proteção de dados pessoais no país. A legislação não traz alterações para o processo eleitoral em si, mas define regras para tratamento de dados pessoais que também incidem sobre atividades de campanha que envolvam o tratamento de dados pessoais.

Além disso, o Tribunal Superior Eleitoral já decidiu sobre a aplicação da LGPD nas eleições de 2020 quando da edição das resoluções aplicáveis a estas eleições. Em dezembro de 2019, quando o início da vigência da LGPD estava previsto para agosto de 2020, o Tribunal Superior Eleitoral decidiu, por unanimidade, incorporar dispositivos de proteção de dados pessoais e da própria LGPD à Resolução do TSE n° 23.610/2019, aplicável para as eleições de 2020, superando o possível óbice do artigo 16 da Constituição Federal quanto a estes pontos, especificamente.

Independente da aplicabilidade da LGPD, é importante pontuar que a privacidade e a proteção de dados continuam válidas no ordenamento jurídico brasileiro e que as campanhas e candidatos devem se atentar a elas em todas as suas atividades nas eleições de 2020. Um exemplo contundente dessa realidade é o recente julgamento, pelo Supremo Tribunal Federal, da ADI 6387, em que se reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais e que a própria Constituição já garante o direito à privacidade dos indivíduos.

Diante desse cenário, o presente documento apresenta base principiológica, isto é, ele parte do pressuposto de que as normas em vigor no Brasil no momento são suficientes para justificar a incorporação de mecanismos de proteção de dados pessoais às campanhas e atividades políticas, independente da aplicabilidade ou não da LGPD para as eleições de 2020.

3 ELEIÇÕES E O REGIME DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Garantir a privacidade e a proteção dos dados pessoais de eleitores durante campanhas eleitorais envolve percorrer um caminho de considerações a respeito do tipo do dado pessoal em questão, as condições da coleta e tratamento, a finalidade para a qual ele foi obtido e utilizado, a necessidade do tratamento daquele dado, se esses dados serão compartilhados, dentre outras.

A LGPD consolida um regime de proteção de dados pessoais que uniformiza conceitos e estabelece regras, deveres e direitos que fornecem balizas para que esse caminho seja percorrido. Isso não significa, no entanto, que a LGPD seja o único diploma jurídico que regulamente o uso de dados pessoais. Como o próprio nome da lei sugere, ela estabelece um regime geral, fundamentado em uma racionalidade própria de proteção de dados, que passa a conviver e interagir com regras setoriais de proteção de dados previamente existentes. No caso de processos eleitorais, esse regime se entrelaça ainda com a legislação eleitoral, fundamentada em uma racionalidade própria, com princípios e valores que visam garantir a integridade democrática.

Isso significa que a compreensão do regime de proteção de dados pessoais que se aplica em processos eleitorais envolve um olhar mais abrangente. Tanto a LGPD quanto o Marco Civil da Internet e a legislação eleitoral estabelecem princípios e regras que vão guiar a interpretação de questões envolvendo o uso de dados pessoais, trazendo pontos que merecem ser colocados em discussão. Nesta seção nós percorremos esse caminho de considerações, mapeando o conjunto de regras e princípios que perfazem um regime de proteção de dados aplicável em processos eleitorais.

3.1. CONCEITOS FUNDAMENTAIS

A discussão das condições e dos limites para o uso de dados pessoais por campanhas passa, primeiro, por uma compreensão a respeito do que é um dado pessoal, o que é um dado pessoal

sensível, e o que é tratamento de dados. A LGPD consolida esse aparato conceitual. Essas definições vão informar não apenas a aplicação da própria lei, mas se tornam referência também para outros dispositivos em legislações setoriais que mobilizam esses conceitos, inclusive a legislação eleitoral.

O QUE É DADO PESSOAL?

O conceito de dado pessoal é central para a definição do escopo e do alcance de um regime de proteção de dados pessoais. A forma como essa definição é construída define os contornos desse regime, limitando ou expandindo o leque de informações que serão consideradas dados pessoais e, portanto, submetidas à regulação.

Existem duas formas principais de definir dados pessoais: a reducionista e a expansionista. A primeira, mais restrita, considera como dado pessoal apenas a informação relacionada a uma pessoa identificada, exigindo um vínculo direto entre o dado e uma pessoa determinada e identificada. Trata-se do RG, do CPF e de outros números únicos, por exemplo. A segunda forma, mais abrangente, considera como dado pessoal qualquer informação relacionada a uma pessoa identificada ou identificável, englobando no conceito dados que, apesar de não estarem imediatamente relacionados a um indivíduo específico, possuem um vínculo indireto com um indivíduo que pode ser identificado. Em ambos os casos, a análise da relação entre a informação e um indivíduo deve ser feita contextualmente. No caso de uma definição expansionista, deve ser levada em consideração a possibilidade de, naquele contexto e a partir do conjunto de informações, se identificar o indivíduo relacionado àquela informação - a partir de um cruzamento de outros dados e informações, por exemplo.[3]

A LGPD, em harmonia com o que já havia sido definido no âmbito do Decreto n. 8771/16 que regulamentou o Marco Civil da Internet,[4] adota uma definição expansionista de dado pessoal, caracterizando como dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável." Neste caso, vale ressaltar que "informação" pode incluir uma ampla gama de dados e conteúdos - números, fotos, vídeos, informações subjetivas ou objetivas, dentre outras, podem vir a serem consideradas dados pessoais se puderem ser relacionadas, de forma direta ou indireta, a uma pessoa natural identificada ou identificável. Ainda, a informação não precisa corresponder necessariamente a um fato - suposições, informações erradas ou imprecisas, bem como inferências podem ser consideradas dados pessoais.

3 Sobre o conceito de dado pessoal ver: BIONI, B. Xeque-Mate: o tripé da proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. GPoPAI/USP, 2015; ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 4/2007 on the concept of personal data. 2007. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>

4 O decreto 8771/16 define, em seu art. 14, I, dado pessoal como "o dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa."

O QUE É DADO PESSOAL SENSÍVEL?

Dentro da categoria de dados pessoais, existe uma categoria mais restrita, os chamados dados pessoais sensíveis. A definição de dado pessoal sensível é importante porque ela delimita uma categoria de dados pessoais aos quais se impõe um regime mais protetivo, por revelarem informações mais intrusivas à privacidade do indivíduo, com potencial discriminatório e mais riscos a direitos e garantias individuais.[5]

A LGPD define dados pessoais sensíveis a partir de um rol taxativo de categorias de informações. São considerados como dados pessoais sensíveis os dados pessoais sobre origem racial ou étnica; sobre convicção religiosa; sobre opinião política; sobre filiação a sindicato ou a organização de caráter religioso, filosófico ou político; referente à saúde ou à vida sexual; além de dados genéticos ou biométricos. Assim como o conceito de dado pessoal, a definição de dado pessoal sensível também não é nova no ordenamento jurídico nacional. A Lei do Cadastro Positivo (Lei 12.414/11) já trazia conceito similar ao definir informações sensíveis como aquelas relacionadas à origem racial e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Essa categorização tem relevância na medida em que o reconhecimento de um dado como sensível traz implicações a respeito das condições e limites do seu uso por campanhas político-eleitorais. Pela LGPD, dados sensíveis só podem ser tratados, em regra, mediante o fornecimento de consentimento específico (art. 11, I). É uma categoria à qual é conferido um grau de proteção maior, o que pode trazer ***implicações quanto às possibilidades de uso desses dados para atividades de campanha, quanto ao impedimento de reuso destes dados para finalidades secundárias e compatíveis, e quanto à mensuração de violações e eventuais sanções no âmbito da justiça eleitoral***.

No limite, parte significativa das estratégias de marketing de uma determinada campanha pode envolver o tratamento de dados sensíveis. Listas de filiados são os exemplos mais evidentes de dados pessoais sensíveis em contextos político-eleitorais, por revelarem claramente orientação política de um indivíduo. No entanto, outras situações menos óbvias também podem envolver o tratamento de dados pessoais sensíveis. Sobretudo, porque a LGPD submete a esse regime mais restritivo não apenas os dados sensíveis em si, mas qualquer tratamento de dados pessoais, inclusive os chamados ''triviais'', que ***revele*** dados pessoais sensíveis e que possa causar dano ao titular (art. 11 §1º). Uma lista de emails com dados de eleitores que concordaram em receber propaganda

5 Sobre dados sensíveis ver: MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159–180, 2018.

de um determinado partido, ou uma lista de seguidores de uma páginas ou perfil político, poderia eventualmente revelar dados sensíveis, na medida em que esses eleitores teriam revelado uma opinião política ao curtirem uma página ou concordarem com o recebimento dessa propaganda.

O mesmo pode ser dito de uma lista com dados de moradores de um bairro, a priori sem qualquer dado sensível, mas que seja utilizada para segmentar propaganda eleitoral a partir de uma inferência sobre a origem racial ou étnica dos moradores daquele bairro. Neste último caso, vale relembrar que a inferência não precisa se referir necessariamente a uma informação verdadeira; ainda que a inferência seja falsa, aquela informação será considerada como dado pessoal.

O QUE É TRATAMENTO DE DADOS?

Um regime de proteção de dados pessoais estabelece regras para o tratamento de informações pessoais. Assim como o conceito de dado pessoal é relevante para definir o escopo desse regime, entender o que é o tratamento de dados pessoais é central para a compreensão do âmbito de aplicação desse regime. Tratamento de dados é, na verdade, um conceito bem amplo, que vai envolver desde a coleta de dados pessoais, até seu uso, armazenamento, análise ou compartilhamento. A LGPD define tratamento como toda operação realizada com dados pessoais, trazendo uma lista exemplificativa de atividades como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados pessoais.

Entender que qualquer atividade que envolva dados pessoais, inclusive o recebimento de dados, pode caracterizar tratamento de dados pessoais é importante porque revela o amplo escopo de práticas que devem estar atentas ao regime de proteção de dados pessoais. Não é apenas a coleta de dados de eleitores ou a análise deste dados que configuram tratamento de dados, mas ***o simples fato da campanha receber um banco de dados de uma pessoa física, por exemplo, já configura tratamento de dados***.

3.2. LGPD E ELEIÇÕES: PRIMEIROS PASSOS

Identificada uma operação de tratamento de dados pessoais (ou de dados pessoais sensíveis), é a LGPD que definirá um regime geral de regras que essa atividade de tratamento deve respeitar.

A lei traz desde princípios gerais que devem guiar o tratamento de dados, até obrigações mais específicas para operadores e controladores. Muitas destas regras e obrigações mais específicas ainda dependem da atuação da Autoridade Nacional de Proteção de Dados e podem, de fato, se mostrar de difícil adequação para as eleições deste ano, como a efetivação do direito de acesso ou correção de dados. No entanto, isso não invalida a adoção da lei como guia para um tratamento de dados protetivo e seguro por campanhas políticas, através de um caminho principiológico e da adequação às bases legais da LGPD.

Para os propósitos deste documento, portanto, ***o foco principal são os princípios da lei, que devem nortear as operações de tratamento, e as bases legais que definem as hipóteses nas quais é autorizado o tratamento de dados pessoais***.

PRINCÍPIOS DA LGPD

Os princípios da LGPD são o principal ponto de partida no caminho de considerações a ser percorrido quando se está diante de uma operação de tratamento de dados pessoais. A LGPD traz um total de dez princípios que devem ser seguidos em atividades de tratamento de dados pessoais (art.6º): finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, e responsabilização e prestação de contas. Esses princípios vão aparecer e ser concretizados em diversos dispositivos da lei, em regras mais específicas para o tratamento de dados, além de se relacionarem com dispositivos presentes em outras normas, como o Marco Civil da Internet. Mas, sobretudo, eles oferecem um guia principiológico para o tratamento de dados pessoais e são um dos principais parâmetros interpretativos para questões envolvendo o uso de dados pessoais por campanhas político-eleitorais. Neste estudo, iremos olhar mais detidamente para sete desses princípios, divididos em 5 grupos. Juntos, ***eles constroem um caminho seguro para campanhas se comunicarem com os eleitores***. O objetivo é oferecer uma referência principiológica que ilumine questões jurídico-regulatórias e auxilie na tomada de decisões.

Finalidade

A finalidade do tratamento de dados pessoais é um dos eixos centrais da proteção de dados. De modo geral, o princípio busca garantir a legitimidade do propósito para o qual se realiza o tratamento de dados pessoais e restringir a reutilização de dados para tratamento posterior incompatível com esse propósito. Pela LGPD, o princípio da finalidade é a “realização

do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades."

Isso significa que, ao se realizar qualquer atividade de tratamento de dados pessoais, deve-se assegurar que a finalidade para a qual esses dados estão sendo tratados é legítima e específica - ou seja, a finalidade não pode ser vedada pela lei (a exemplo das restrições da legislação eleitoral sobre doação de banco de dados), nem pode ser ampla e genérica. Coletar dados pessoais de eleitores indicando que os dados serão usados para "finalidades político-eleitorais" amplas e genéricas, por exemplo, não respeita o princípio da finalidade.

Essa finalidade deve, ainda, ser explícita e informada ao titular dos dados - isto é, é necessário deixar claro ao titular para qual finalidade específica seus dados serão tratados. Retomando o exemplo, se uma campanha estiver coletando dados de eleitores através de um formulário na internet para fins de propaganda, é necessário informar de forma explícita ao eleitor que aqueles dados serão utilizados especificamente para envio de propaganda eleitoral.

O princípio da finalidade assegura também que estes dados não sejam tratados posteriormente para finalidades incompatíveis. Ou seja, se um partido coletou dados para um abaixo-assinado, ou, até mesmo, se uma campanha realizou coleta de dados para uma pesquisa de opinião interna, informando especificamente essas finalidades aos titulares, não é possível que esses dados sejam utilizados, posteriormente, para envio de propaganda eleitoral. Ainda, se um determinado parlamentar lançou, no curso do seu mandato, uma plataforma para informar os eleitores das ações do mandato, não poderá reutilizar para a sua campanha eleitoral. ***Faz-se necessária sempre uma análise contextual, isto é, compreender se o uso secundário detêm uma relação conexão bastante próxima com uso primário. Se a resposta for negativa, então o uso não será compatível***.

Dados de acesso público são um dos casos em que é especialmente importante estar atento ao princípio da finalidade. Cadastro de eleitores acessíveis em cartórios eleitorais, listas de filiados de partidos, e, até mesmo, informações publicadas por usuários em seus perfis de redes sociais são todos exemplos de dados de acesso público e, no último caso, dados tornados manifestamente públicos pelo titular. O fato de um dado ser público, no entanto, não significa que ele pode ser tratado livremente. Em todos estes casos, os dados foram coletados ou disponibilizados pelos usuários

para finalidades específicas - seja para exercício do direito de votar ou para participar em uma rede social e expressar suas opiniões (artigo 7o, §4º, §6º e §7º). A coleta, reutilização ou tratamento destes dados por campanhas políticas para construção de bancos de dados, pesquisas internas, ou envio de propaganda eleitoral, portanto, configuram um tratamento de dados pessoais em violação ao princípio da finalidade. Em todo caso, é necessário se certificar de que há uma base legal para o tratamento de dados pessoais, ainda que públicos.

Adequação e Necessidade

Adequação e necessidade são dois princípios intimamente ligados ao princípio da finalidade. O princípio da adequação busca garantir que a atividade de tratamento realizada seja compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento. Reaproveitamento de bases de dados de eleições anteriores é uma das hipóteses que pode levantar questões sobre adequação.

Já o princípio da necessidade busca garantir que o tratamento de dados seja limitado ao mínimo necessário, abrangendo apenas os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. De modo geral, o princípio segue a lógica de que menos é mais, isto é, ele busca equacionar como usar a menor quantidade possível de dados para atingir uma determinada finalidade. Em contextos eleitorais, a incidência desse princípio se complexifica, pois a balança nestes casos não é entre a proteção de dados e atividade econômica, mas envolve o próprio processo democrático.

Há, assim, uma difícil equação, que ainda está longe de ser resolvida, em torno de quais são os limites de informações que partidos políticos e candidatos devem observar para realizar uma comunicação efetiva com o eleitorado. No caso de países em que o voto é obrigatório, como no Brasil, a equação deve levar ainda em consideração que tal diálogo facilita o exercício da cidadania. Ainda assim, o pretexto de realizar uma comunicação efetiva com o eleitor não justifica qualquer tratamento de dados pessoais, em detrimento do princípio da necessidade. A coleta de dados para elaboração de perfis psicométricos detalhados de eleitores para micro direcionamento de mensagens - a exemplo do realizado pela ***Cambridge Analytica*** - tende a ser um caso claro de tratamento excessivo de dados, colidindo com o princípio da necessidade.

Transparência

A transparência sobre atividades de tratamento de dados é essencial para garantir ao titular a autonomia sobre suas informações. O princípio da transparência busca garantir que titulares tenham acesso a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. ***O princípio reflete uma racionalidade comum que há, historicamente, entre normas de proteção de dados e normas de direito eleitoral: a redução de assimetria de poder e informação.***

Em um cenário de uso de dados pessoais em processos eleitorais, essa racionalidade implica que partidos políticos e campanhas eleitorais sejam transparentes a respeito das atividades de tratamento de dados realizadas. Um primeiro passo é a transparência para com o eleitor titular de dados, através da formulação de políticas de privacidade claras, precisas e acessíveis, que tragam informações sobre a finalidade do tratamento, o armazenamento e eventual compartilhamento de dados, práticas de segurança adotadas, dentre outras. As informações fornecidas ao titular nestes documentos são essenciais para garantir a idoneidade do tratamento e colocar a campanha em um caminho seguro de comunicação política. Posteriormente, o diálogo da LGPD com a legislação eleitoral pode desengatilhar, ainda, uma transparência mais ampla, que permita a fiscalização sobre a integridade do processo eleitoral, através de novos tipos de documentação, como, por exemplo: um programa de governança que seja parte integrante do plano de campanha eleitoral; e/ou o registro das atividades de tratamento de dados, especialmente para que futuras diligências e avaliação de prestação de contas da campanha se dê também sobre eventual abuso de poder no uso de dados.

Ainda, é importante destacar que ***medidas de transparência ativa devem ser consideradas independentemente da base legal eleita para a atividade de tratamento de dados***. Muito vezes se tem a percepção equivocada de que tal dever é ativado apenas quando se faz necessário buscar o consentimento do titular. Na verdade, é uma medida que se faz ainda mais necessária no curso de outras hipóteses permissivas. Isto porque, o titular - e entidades representativas dos seus direitos - exerce controle sobre os dados pessoais quando se opõe a um tratamento de dados que considera ilegítimo. É o que sucede, por exemplo, do chamado opt-out.

Segurança e Prevenção

Estabelecer salvaguardas e medidas de segurança é essencial para garantir não só a proteção dos dados do titular mas, também, para evitar danos que possam advir de vazamentos ou do tratamento desses dados. Nesse sentido, é importante estar atento ao princípio da segurança e ao princípio da prevenção.

O princípio da segurança busca garantir que sejam adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. De modo geral, ele indica a necessidade de que sejam adotadas medidas e ferramentas de segurança da informação que evitem incidentes e riscos à proteção da privacidade e de direitos fundamentais do titular, como no caso de acessos não-autorizados ou vazamento de bancos de dados, por exemplo. Em contextos eleitorais, o cuidado com a segurança da informação traz uma garantia dupla. Por um lado, protege o eleitor de riscos à privacidade e direitos fundamentais, sobretudo diante de um contexto no qual obter informação sobre o eleitor pode significar mais poder de persuasão e manipulação. Por outro, protege a própria campanha, sua rede de apoiadores e suas estratégias de comunicação, além cultivar a confiança do eleitorado para com o candidato ou partido.

Em paralelo, o princípio da precaução prevê a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. De modo geral, ele indica a importância de que antes do tratamento de dados as campanhas realizem um exercício de avaliar os possíveis riscos e danos que aquele tratamento pode trazer para que, diante de riscos significativos, salvaguardas sejam adotadas ou o tratamento interrompido. Novamente, a preocupação protege tanto o eleitor quanto a campanha.

Não-discriminação

Dados pessoais não podem ser tratados de forma abusiva para discriminar indivíduos. É isso que o princípio da não-discriminação busca garantir ao vedar a realização do tratamento para fins discriminatórios ilícitos ou abusivos. Dados pessoais revelam informações sobre indivíduos que, muitas vezes, podem ser usadas para segregar ou discriminar de forma abusiva. Em contextos eleitorais, essa discriminação pode vir por meio do envio de mensagens contraditórias a diferentes segmentos de eleitores, ou pela dissuasão de determinados grupos de eleitores que possuem menos afinidade

com determinado projeto político. Um exemplo clássico de uso discriminatório de dados em processos eleitorais é a dissuasão de determinados grupos de eleitores que apoiam candidatos da oposição, buscando evitar que eles votem ou, no caso de países em que o voto é obrigatório, como no Brasil, informando números errados de candidatos que levem o eleitor a votar em candidato distinto daquele que ele escolheu.

BASES LEGAIS PARA TRATAMENTO DE DADOS PESSOAIS

Enquanto os princípios oferecem um caminho seguro para o tratamento de dados pessoais por campanhas políticas, as bases legais fornecem a fundamentação que possibilita esse tratamento. Elas definem as hipóteses nas quais esse dado pode ser tratado; isto é, os requisitos e condições necessários para que um dado possa ser coletado, processado, utilizado, armazenado etc. Em todo tratamento de dados pessoais é essencial se certificar qual é a base legal que subsidia e autoriza aquele tratamento.

A LGPD traz no art. 7º as hipóteses nas quais pode ocorrer tratamento de dados pessoais, ou seja, as bases legais. Dentre as 10 bases legais - algumas específicas para saúde, proteção ao crédito ou atividades da administração pública, por exemplo - quatro são especialmente importantes em contextos eleitorais: o consentimento, legítimo interesse, execução de contrato e para a execução de política pública. É importante destacar que tais hipóteses autorizativas de tratamento de dados estão em pé de igualdade, não havendo hierarquia entre elas. O que é importante é encontrar a base legal que melhor se adequa à situação.

A primeira autoriza o tratamento de dados pessoais quando houver consentimento do titular. De forma geral, esta é a base legal que melhor se encaixa em diversas hipóteses de coletas de dados para finalidade político-eleitorais. Nestes casos, o consentimento deverá ser informado, livre e inequívoco - isto é, o titular deve ser informado sobre o tratamento e sua finalidade, ter a opção de consentir ou não com esse tratamento, e este consentimento deve ser fornecido de modo a não deixar dúvidas quanto à manifestação do titular. Isso significa que aquelas caixas pré-selecionadas indicando que o titular consente com o uso de dados ou com a política de privacidade não são válidas, pois elas induzem o titular a uma determinada decisão, além de não permitirem a comunicação adequada sobre o tratamento e sua finalidade. Da mesma forma que não é válido o consentimento fornecido

para finalidades amplas e genéricas. O importante é oferecer informações claras e acessíveis e opções para o eleitor consentir ou não com aquele tratamento.

A segunda base legal autoriza o tratamento de dados pessoais para atender interesses legítimos do controlador[6] de dados - como para a proteção do exercício regular de seus direitos ou prestação de serviços que o beneficiem - ***desde que respeitada a legítima expectativa do titular dos dados e seus direitos e liberdades fundamentais***. A aplicação desta base é mais complexa e envolve mais requisitos a serem cumpridos. Nestes casos, a análise deve ser realizada caso a caso, levando-se em consideração a legitimidade do interesse de quem está tratando os dados, a necessidade e adequação do tratamento (o que remete aos ***princípios*** do regime de proteção de dados pessoais), a legítima expectativa do titular quanto ao tratamento de seus dados, e as salvaguardas adotadas para garantir transparência e segurança. Para que o interesse seja legítimo, é preciso avaliar se este interesse encontra óbice em legislação e se é um interesse específico e bem delineado. É essencial garantir um balanceamento adequado entre o legítimo interesse e legítima expectativa; não é possível realizar um tratamento fundamentado pelo legítimo interesse se a realização daquele tratamento não estiver dentro de uma expectativa razoável do titular quanto ao uso de seus dados. A avaliação deve ser feita em cada caso, considerando as condições de cada contexto em específico, não sendo possível determinar a priori a validade da base legal. Em todo caso, vale ressaltar que ainda que possivelmente aplicável em contextos político-eleitorais, as possibilidades de adoção dessa base legal por campanhas parecem ser mais restritas do que o consentimento. Ainda, a adoção dessa base legal requer a operacionalização de outros requerimentos, como as medidas de transparência aos titulares de dados pessoais e o próprio direito do cidadão se opor ao tratamento dos seus dados pessoais - o direito de ***opt-out***.

A terceira autoriza o tratamento de dados quando for necessário para a execução de contrato. Caso a relação entre filiados(a)s e partidos seja considerada uma relação contratual, pode-se considerar que o uso de seus dados pessoais para comunicá-los de uma convenção ou mesmo da eleição das chapas é algo essencial para a performance do objeto principal de tal relação contratual. Ressalta-se que é uma base legal que deve ser mobilizada quando o que está em jogo é uma obrigação principal e não acessória do vínculo firmado entre o titular do dado e o agente de tratamento de dados.

A quarta é a hipótese desenhada para relação estado-cidadão.

6 O *controlador* dos dados pessoais é definido no artigo 5º, inciso VI da LGPD como "a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

O próprio Tribunal Superior Eleitoral trata dados pessoais do(a)s candidato(a)s para a organização do pleito eleitoral. Nesses casos, o uso de dados se dá para a "persecução de um interesse público" que está dentre as "competências legais"do TSE (artigo 7, III, combinado com o artigo 23) e, também deve estar em plena conformidade à LGPD.

Dados pessoais sensíveis

No caso de dados pessoais sensíveis, o regime de bases legais é mais rígido. A LGPD traz no artigo 11 uma lista de 8 hipóteses nas quais pode ocorrer tratamento de dados pessoais sensíveis. No entanto, estas bases não têm a mesma hierarquia normativa. Em regra, só é possível tratar dados sensíveis mediante o consentimento, de modo que tal base legal passa a prevalecer sobre as demais. O consentimento, nestes casos, deve ser, além de informado, livre e inequívoco, também específico. Essa qualificação, entretanto, deve ser relativizada, uma vez que, em razão do princípio da finalidade, ***todo*** consentimento deveria ser específico. Nesse sentido, uma possível interpretação para a diferença entre os consentimentos dos dados pessoais triviais e dados pessoais sensíveis é que, no segundo caso, a aplicação da base legal deve ser expressa, além de informada, livre e inequívoca.

No caso de não haver consentimento, a lei traz 7 outras hipóteses autorizativas, mas, dentre elas, não há o legítimo interesse. Assim, o enquadramento jurídico para o tratamento de dados sensíveis reduz significativamente a discricionariedade dos controladores, especialmente por terem que buscar, em regra, oconsentimento do titular e, ainda, por não poderem se valer da base legal do legítimo interesse. Em contextos eleitorais, é importante estar especialmente atento a este regime, posto que informações sobre opinião e filiação política são dados sensíveis, da mesma forma que dados sobre origem racial ou étnica e sobre convicção religiosa, muitas vezes utilizados para segmentar eleitores e enviar propaganda política. Além disso, é importante ressaltar que esse regime mais restrito de bases legais se aplica não apenas ao tratamento de dados sensíveis em si, mas a qualquer tratamento que revele dados sensíveis. Isto significa, por exemplo, que a segmentação de eleitores em grupos a partir de dados sobre origem geográfica na cidade que levem a inferências sobre convicção religiosa ou origem racial ou étnica destas pessoas com o propósito de direcionar mensagens e propaganda política deve se adequar às bases legais de dados sensíveis, só podendo, ***a priori***, ser realizada mediante consentimento específico do eleitor.

3.3. PROTEÇÃO DE DADOS NO MARCO CIVIL DA INTERNET

Em paralelo ao regime geral de proteção de dados da LGPD, outras legislações setoriais trazem regras específicas sobre proteção de dados que se aplicam a campanhas eleitorais. Na hipótese de tratamento de dados na internet, o Marco Civil define um conjunto de regras que garantem a proteção da privacidade e dos dados pessoais.

Ao definir princípios, garantias, direitos e deveres, a lei estabeleceu uma estrutura regulatória geral para o uso da internet no Brasil. Dentre os valores e princípios que informam essa constituição, estão a proteção da privacidade (art. 3º, II) e a proteção de dados pessoais (art. 3º, III).

Além dos princípios, a lei garante uma série de direitos ao usuário de internet, que se aplicam a qualquer tratamento de dados pessoais na internet (art. 7º), com regras gerais sobre consentimento, finalidade, transparência e compartilhamento de dados pessoais:

> **O inciso VII garante ao usuário que seus dados não sejam compartilhados com terceiros, a não ser que o mesmo ofereça seu consentimento de forma livre, expressa e informada.**

> **O inciso VIII garante ao usuário o direito de receber informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais. Aqui também a transparência é realizada, em regra, através de uma política de privacidade que traga informações sobre os dados coletados, para que eles serão utilizados, por quanto tempo serão armazenados, com quem eles podem ser compartilhados, dentre outras informações. O inciso garante ao usuário, ainda, que o tratamento desses dados respeite o princípio da finalidade - isto é, os dados só podem ser utilizados para finalidades que não sejam vedadas pela legislação, que justifiquem sua coleta, e que tenham sido devidamente informadas ao usuário.**

> **O inciso IX garante ao usuário que seu consentimento para coleta, uso, armazenamento e tratamento de dados pessoais seja expresso e destacado**

Em processos eleitorais, esses direitos devem ser observados pelas campanhas em qualquer tratamento de dados que ocorra na internet ou a partir dela. Isto vale para situações como as de coleta de dados através de formulários divulgados em redes sociais ou no site de candidatos ou partidos; coleta de dados realizadas por páginas ou perfis de candidatos ou partidos nas redes sociais; uso de dados para envio de propaganda eleitoral

em redes sociais ou aplicativos de mensagens; raspagem de dados em redes sociais; coleta de dados através de aplicativos próprios ou pelo site de candidatos ou partidos são todos exemplos de atividades que, ao serem operacionalizadas, devem estar atentas aos direitos dos usuários garantidos pelo Marco Civil da Internet.

Quando candidatos, partidos ou coligações desenvolvem aplicações ou serviços próprios na internet que coletem dados pessoas e metadados sobre acesso a aplicações, é importante estar atento aos artigos 10 a 12 da lei. Nestes casos, a lei reforça ainda o princípio da finalidade e da necessidade, vedando expressamente que sejam guardados dados pessoais excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular (art. 16, I).

3.4. A PROTEÇÃO DE DADOS NA LEGISLAÇÃO ELEITORAL

A legislação eleitoral, através de regras específicas de proteção de dados em contextos eleitorais, vai costurar, junto com o MCI e a LGPD, um arcabouço de regras e princípios que balizam a proteção de dados em processos eleitorais. Um dos fundamentos do regime brasileiro de proteção de dados, *a garantia da autodeterminação informativa, também assegura a proteção de dados dos eleitores na legislação eleitoral, garantindo a autonomia de decisão do eleitor*. Em um contexto de campanhas políticas transformadas, a proteção de dados passa a ser, também, uma ferramenta necessária para a proteção da integridade do processo eleitoral, a garantia da igualdade de chances entre os candidatos, e o combate a abusos.

Nesse sentido, tanto a Lei das Eleições quanto a Resolução TSE 23.610/19 trazem regras que regulamentam usos específicos de dados pessoais. Além disso, como regra geral, a Resolução n. 23.610/19, que dispõe sobre propaganda eleitoral, prevê que se aplicam, no âmbito da resolução, as disposições da Lei Geral de Proteção de Dados (art. 41). Ao mesmo tempo, a resolução traz uma regra geral no §4º do art. 31, dispondo que o tratamento de dados pessoais, inclusive sua doação, uso ou cessão, por pessoa jurídica ou pessoa natural, deverá respeitar as disposições da Lei Geral de Proteção de Dados Pessoais. O que o conjunto de ambos os dispositivos sugere é que as atividades de tratamento de dados pessoais realizadas por, ou em favor de, candidatos, partidos políticos, ou coligações devem estar de acordo com as regras da LGPD, sobretudo no âmbito de práticas relacionadas à propaganda eleitoral.

TRATAMENTO DE DADOS PARA ENVIO DE PROPAGANDA ELEITORAL

No caso da realização de tratamento de dados pessoais com a finalidade de enviar propaganda eleitoral, a legislação eleitoral indica alguns caminhos com relação às hipóteses nas quais dados pessoais podem ser tratados para essas finalidades e sob quais condições esse tratamento deve ocorrer.

Ao prever a possibilidade de realização de propaganda eleitoral na internet no art. 57-B, a Lei das Eleições autoriza que candidatos, partidos ou coligações enviem propaganda eleitoral por meio de mensagens eletrônicas, desde que os endereços eletrônicos para envio destas mensagens tenham sido cadastrados de forma gratuita pelo candidato, partido ou coligação. A lei veda, assim, o uso de dados pessoais que tenham sido coletados de forma onerosa ou por qualquer outra pessoa física ou jurídica, que não seja o candidato, o partido ou coligação. Nesse caso, o uso de bancos de dados pessoais de uma pessoa física para envio de propaganda eleitoral por meio de mensagem eletrônica pode configurar propaganda irregular na internet, sujeita à multa.

Ao regulamentar este artigo, levando em consideração o cenário e as ferramentas tecnológicas atuais (art. 57-J da Lei das Eleições), a Resolução 23.610/2019 especificou as hipóteses e condições para esta coleta consensual de endereços. Com uma indicação mais específica, o art. 28, III da Resolução dispõe que a propaganda eleitoral poderá ser realizada por meio de mensagem eletrônica para endereços cadastrados gratuitamente pelo candidato, partido ou coligação, observadas as disposições da LGPD quanto ao consentimento do titular. Nestes casos, não só os dados pessoais têm que ser coletados de forma gratuita, como também deve ser obtido o consentimento do titular nos termos da LGPD, ou seja, o consentimento informado, livre e inequívoco. O que o artigo sugere, ainda, é que, no caso de marketing direto, ou seja, no caso de envio de mensagem com propaganda eleitoral para o eleitor, a base legal aplicável para o tratamento desses dados seria o consentimento do titular.

Em complemento a essas regras, tanto a Lei das Eleições (art. 57-G) quanto a Resolução 23.610/2019 (art. 33) preveem um dever de descadastramento para candidatos, partidos e coligações. No caso de envio de mensagens eletrônicas ou mensagens instantâneas, deve ser oferecido ao eleitor um mecanismo que permita seu descadastramento. Na prática, a previsão assegura ao eleitor a possibilidade de retirar o

consentimento concedido para o recebimento de mensagens eletrônicas, garantindo um mecanismo de proteção à autodeterminação informativa.

Vale ressaltar que nenhuma dessas regras se aplica à comunicação consensual entre eleitores. A Resolução prevê que nem o dever de descadastramento nem as regras sobre propaganda eleitoral se aplicam às mensagens enviadas consensualmente por pessoa natural, de forma privada ou em grupos restritos de participantes (art. 33 §2º).

DOAÇÃO, VENDA OU CESSÃO DE BANCOS DE DADOS

No caso da construção e formação de bancos de dados por candidatos, partidos e coligações, a legislação eleitoral traz vedações expressas no art. 57-E da Lei das Eleições e no art. 31 da Resolução 23.610/2019 que devem ser observadas.

A regra veda que pessoas jurídicas de direito privado doem, usem, ou cedam dados pessoais de seus clientes em favor de candidatos, partidos e coligações. Assim, fica expressamente proibido que empresas usem ou doem seus bancos de dados para fins de campanhas político-eleitorais, podendo a violação desse dispositivo ensejar sanções. Além disso, o dispositivo veda, de forma ampla, a venda de cadastros de endereços eletrônicos para candidatos, partidos ou coligações, seja por pessoas jurídicas ou pessoas naturais. Isso implica que qualquer tipo de atividade que envolva a compra de bancos de dados com endereços eletrônicos viola a legislação eleitoral, estando sujeita a sanções.

As regras formuladas nesses dispositivos trazem uma proteção significativa aos dados de eleitores, além de estabelecerem um diálogo direto com as vedações às doações pecuniárias para campanhas eleitorais, indicando que dados pessoais também podem ser vistos como ativos.

SANÇÕES: INSTRUMENTOS DA JUSTIÇA ELEITORAL PARA COIBIÇÃO DE ILÍCITOS E ABUSOS

Apesar de vigente desde 18 de setembro de 2020, as sanções previstas na LGPD não poderão ser aplicadas pela Justiça Eleitoral nas eleições de 2020. Em primeiro lugar porque a vigência dos artigos 52, 53 e 54, que preveem as sanções na LGPD, entrarão em vigor apenas em 1º de setembro de 2021 (art. 65, I-A). Em segundo lugar porque, ainda que estivessem vigentes, as sanções previstas na LGPD, que possuem natureza administrativa, somente podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (art. 52).

Isso não significa que não existam mecanismos de coerção do uso abusivo e ilícito de dados dos eleitores já aplicáveis para as eleições de 2020. Caso sejam violadas qualquer uma das normas eleitorais acima indicadas, a Justiça Eleitoral poderá ser acionada por candidatos, partidos, coligações e o Ministério Público para que determine que a prática ilícita seja cessada imediatamente e posteriormente sancionar o candidato responsável ou beneficiário do ilícito. Nestes casos, violações a princípios de proteção de dados pessoais podem até servir como parâmetros para mensuração da gravidade da conduta.

No caso de descumprimento dos dispositivos que exigem o consentimento prévio (art. 57-B, III, da Lei das Eleições e art. 28, III, da Res. TSE 23.610/2019) e proíbem a venda de banco de dados e utilização, cessão ou doação de dados pessoais de clientes de pessoa jurídica em favor de candidato, partido ou coligação (art. 57-E da Lei das Eleições e art. 31 da Res. TSE 23.610/2019), os responsáveis pela divulgação da propaganda e seus beneficiários estarão sujeitos a multas que variam entre R$5.000 a R$30.000. No caso de descadastramento de usuário (art. 57-G da Lei das Eleições e art. 33 da Res. TSE 23.610/2019), uma vez solicitado o descadastramento, ele deve ser efetivado em até 48 horas, sob pena de multa de R$100,00 por mensagem enviada após o prazo. Todos esses fatos poderão ser apurados pela Justiça Eleitoral em representações eleitorais ajuizadas com base no artigo 96 da Lei das Eleições.

Além das sanções pecuniárias, a utilização ilícita de dados de eleitores que afetar a normalidade e a legitimidade das eleições pode também configurar atos de abuso de poder. Caso exista utilização excessiva de recursos materiais ou humanos que representem valor econômico relacionados à utilização indevida de dados pessoais, como, por exemplo, a compra de um banco de dados significativo de eleitores, os atos podem representar abuso de poder econômico. Na hipótese de o detentor do poder valer-se de sua posição para utilizar dados pessoais de eleitores, como por exemplo a utilização do cadastro de contribuintes de IPTU em um município para envio de propaganda eleitoral, é possível que o ato seja entendido como abuso de poder político. Todos esses fatos poderão ser apurados pela Justiça Eleitoral em uma Ação de Investigação Judicial Eleitoral, proposta com fundamento no artigo 22 da Lei Complementar n° 64/90, podendo levar à cassação e inelegibilidade do candidato e responsáveis pelo ilícito.

4 PROPAGANDA ELEITORAL E PROTEÇÃO DE DADOS

CONSTRUÇÃO DE BANCOS DE DADOS PESSOAIS E O CONSENTIMENTO

Construir e alimentar bancos de dados é uma prática recorrente em campanhas. Em alguns casos, esses dados são coletados durante as atividades de campanhas de rua. Na internet, a construção destes bancos de dados muitas vezes é feita em sites de candidatos, a partir de formulários online, ou pela interação com eleitores nas redes sociais. Em qualquer que seja o caso, é essencial que a construção destes bancos se fundamente em uma das bases legais da LGPD - ou seja, é essencial que esteja presente alguma das hipóteses que autorizam o tratamento de dados pessoais. Muitas vezes, essa hipótese será o consentimento do eleitor, fornecido no momento da coleta de dados. Para que este consentimento seja válido, no entanto, ele tem que ser ***informado***, ***livre*** e ***inequívoco***.

Mas como garantir que o consentimento tenha esses atributos?

Primeiro, para que o consentimento seja informado, é essencial que antes de consentir com a coleta e tratamento dos dados, o titular receba informações claras e acessíveis sobre o tratamento de dados e a finalidade deste tratamento, que deverá ser determinada. Por um lado, isso significa que consentimento para finalidades amplas e genéricas, como "atividades político-eleitorais" não é válido. Por outro lado, isso não significa que seja necessário fornecer descrições minuciosas sobre o tratamento e a finalidade, até para evitar a ''fadiga do consentimento'', isto é, que o excesso e complexidade das informações produza o resultado contrário ao almejado.

Em relação ao período, o consentimento fornecido para que a campanha se comunique com o eleitor, por exemplo, vale tanto para comunicações realizadas no período pré-eleitoral quanto para comunicações durante o período eleitoral. De forma geral, o escopo do consentimento e as atividades de tratamento de dados que ele autorizará vão depender das informações fornecidas e das finalidades comunicadas ao titular nesse momento.

Segundo, para que o consentimento seja livre, o titular deve ter a opção de consentir ou não com aquele tratamento. A manifestação da vontade do titular, neste caso, não pode ser fruto de uma coação ou de uma relação de subordinação, por exemplo, nem pode ser uma condição para que o titular acesse

informações, serviços ou canais de comunicação e participação que não dependam do tratamento dos dados pessoais em questão. Da mesma forma, opções pré-selecionadas indicando que o titular consente com o tratamento de dados também impedem que o consentimento seja livre.

Terceiro, para que o consentimento seja inequívoco é importante que não haja dúvidas quanto à manifestação de vontade do titular. Para isso, o consentimento poderá ser fornecido por escrito, mas não é necessário que assim o seja. Aqui, novamente, é essencial uma análise contextual. A depender das circunstâncias e do contexto, o consentimento poderá ser tácito, desde que seja possível verificar a manifestação de vontade do titular. No caso de um formulário na internet, por exemplo, o próprio preenchimento do formulário pode indicar um consentimento inequívoco, a depender do contexto.

No caso de bancos de dados que contenham dados sensíveis, o consentimento não deverá ser apenas informado, livre e inequívoco, mas, também, *específico*. Em ambos os casos, vale ainda reforçar que a construção e alimentação de um banco de dados deve levar em consideração as vedações à venda, cessão e doação de dados pessoais do art. 57-E da Lei das Eleições, assim como as regras do Marco Civil da Internet, na hipótese do banco de dados ser construído a partir de dados coletados pela internet.

O CONSENTIMENTO PARA ENVIO DE PROPAGANDA ELEITORAL ATRAVÉS DE MENSAGENS PRIVADAS

O envio de propaganda eleitoral é uma prática que muitas vezes envolve tratamento de dados pessoais. Quando campanhas coletam informações sobre email, telefone ou endereço residencial de eleitores e os utilizam para enviar propaganda eleitoral, configuram-se atividades de tratamento de dados pessoais, que devem ser autorizadas por alguma das bases legais da LGPD. No caso do envio de propaganda eleitoral por mensagem eletrônica, a Resolução 23.610/19 determina não só que os endereços devem ter sido cadastrados gratuitamente pelo candidato, partido ou coligação, mas indica também que a base legal aplicável nesses casos é o consentimento. Assim como no caso de construção de bancos de dados, o consentimento deve ser informado, livre e inequívoco - e específico, caso o tratamento envolva dados sensíveis.

DESCADASTRAMENTO

A legislação eleitoral exige que no caso de envio de mensagens eletrônicas ou instantâneas por candidatos, partidos e coligações seja disponibilizado um mecanismo de descadastramento, que permita ao eleitor se opor ao recebimento destas mensagens. A previsão dialoga com tanto com o direito do titular revogar seu consentimento para tratamento de dados e quanto com o direito do titular de se opor ao tratamento de seus dados pessoais, ambos garantidos pela LGPD. Na prática, esse arcabouço normativo exige que as campanhas ofereçam informações claras aos titulares sobre a possibilidade deles se oporem ao tratamento de seus dados e ao recebimento de mensagens e a forma como esse descadastramento pode ser feito.

POLÍTICA DE PRIVACIDADE

A transparência é tanto um princípio da LGPD quanto um direito garantido aos usuários pelo Marco Civil da Internet. Oferecer informações claras, precisas e acessíveis sobre tratamento de dados pessoais é essencial para que o titular exerça autonomia sobre suas informações. Por um lado, é através de informações sobre a realização de tratamento de dados e os agentes responsáveis por esse tratamento, que o titular pode exercer seus direitos, oferecer seu consentimento, ou se opor à realização de determinado tratamento. Por outro, a promoção de transparência garante segurança às campanhas, na medida em que assegura que o titular foi informado sobre as operações de tratamento.

Um primeiro passo para a promoção de transparência para com o eleitor titular de dados é a formulação de políticas de privacidade, que tragam informações sobre os dados coletados, as atividades de tratamento, a finalidade do tratamento, período de guarda e armazenamento, eventual compartilhamento de dados, práticas de segurança adotadas, direitos do titular, dentre outras. Esse tipo de documento deve ter uma linguagem clara, trazendo informações precisas e facilmente acessíveis ao titular. Políticas de privacidade escondidas em sites, aplicativos ou formulário, por exemplo, que dificilmente serão vistas ou acessadas pelo titular não cumprem a função de promover transparência. Da mesma forma que políticas de difícil compreensão, com linguajar excessivamente técnico, são um obstáculo à transparência. É importante que em cada contexto de coleta e tratamento de dados se avalie a melhor forma de garantir esse tipo de transparência. Vale ressaltar que medidas de transparência

como essa devem ser adotadas não apenas para a obtenção do consentimento do titular, mas em qualquer hipótese de tratamento de dados pessoais.

ENVIO DE MENSAGENS POR PESSOA NATURAL CONSENSUALMENTE E/OU EM "GRUPOS RESTRITOS"

Todo o arcabouço de regras discutido até aqui não se aplica, em regra, à comunicação consensual e espontânea entre eleitores. Por um lado, a LGPD não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos. Quando um eleitor envia mensagem para algum familiar ou conhecido, por exemplo, o tratamento referente ao uso deste número de telefone não está sujeito às regras e deveres da LGPD. Por outro, a legislação eleitoral protege a livre manifestação do eleitor e considera que essa manifestação espontânea na internet não é considerada como propaganda eleitoral. No caso de envio de mensagens privadas, a Resolução 23.610/19 prevê ainda que nem o dever de descadastramento nem as regras sobre propaganda eleitoral se aplicam às mensagens enviadas consensualmente por pessoa natural, de forma privada ou em grupos restritos de participantes (art. 33 §2º).

No entanto, a definição prática de quando uma comunicação não será considerada propaganda eleitoral nem envolverá tratamento de dados sujeitos à LGPD envolve algumas dificuldades, sobretudo na delimitação do que seria "pessoas naturais", "consensualmente" e "fins exclusivamente particulares e não econômicos". De um lado, parece inviável que cada indivíduo obtenha consentimento para o envio de cada mensagem com conteúdo político-eleitoral. A previsão parece se referir muito mais a um contexto implícito de troca de mensagens entre eleitores que se conhecem ou que compartilharam seus contatos voluntariamente entre si. Por outro lado, a definição do que se enquadraria como pessoas naturais parece não abranger representantes de campanhas, indivíduos que trabalham para campanhas ou que operacionalizam estratégias de comunicação desenvolvidas para campanhas. Da mesma forma que "finalidades exclusivamente particulares e não econômicas" envolve considerações sobre o grau de controle e organização exercido pelas campanhas e a relação dessa prática com as próprias estratégias da campanha. Um caminho interpretativo pode vir da garantia à manifestação livre e espontânea do eleitor na internet, que não é considerada propaganda eleitoral. Assim, na ausência do elemento espontaneidade, essa manifestação

pode vir a ser considerada propaganda eleitoral, sujeitando-se, portanto, às regras da legislação eleitoral e às regras e princípios da LGPD quando houver tratamento de dados.

DISPARO EM MASSA

Uma das novidades da Resolução 23.610/19 é a vedação ao disparo em massa de conteúdo. A regra dialoga com a proteção de dados pessoais na medida em que a realização de disparos em massa depende, na maioria das vezes, de bancos de dados com números de telefone ou endereços eletrônicos. O art. 34 da resolução veda realização de propaganda por meio de disparo em massa de mensagens instantâneas sem anuência do destinatário, exigindo, portanto, que o eleitor esteja de acordo com o recebimento de propaganda nestes termos. No entanto, a anuência do destinatário não parece autorizar qualquer prática de disparo em massa, já que no art. 28, IV a resolução veda de forma ampla o contratamento de disparo em massa para a realização de propaganda por meio de aplicações de mensagens instantâneas.

DOAÇÃO DE BANCOS DE DADOS POR PESSOA NATURAL

A legislação eleitoral veda que pessoas jurídicas de direito privado doem, usem ou cedam dados pessoais em favor de candidatos, partidos ou coligações. No entanto, ela não aborda as hipóteses de uso, doação ou cessão de dados pessoais por pessoas naturais em favor de candidatos, partidos ou coligações. No entanto, a ausência de uma regulação eleitoral específica não significa automaticamente que a prática é permitida e legítima. O ideal é que campanhas construam suas próprias bases de dados, atentas às regras da LGPD, do MCI e da legislação eleitoral. Como o próprio recebimento destes dados por candidatos, partidos ou coligações configura tratamento de dados pessoais, o caminho para avaliar a legitimidade da atividade passa pelos princípios da LGPD - notadamente, o princípio da finalidade e o princípio da transparência - pela existência de uma base legal que fundamente este tratamento, e pelas informações oferecidas ao titular no momento do consentimento, quando este for o caso. No caso de uma pessoa física que queira compartilhar sua lista de contatos para que uma campanha encaminhe propaganda eleitoral, por exemplo, o recebimento e uso destes dados pela campanha esbarra na ausência de uma base legal que autorize o tratamento destes dados, além de estar em desacordo com o princípio da finalidade e da transparência. Em paralelo, é

importante considerar também que, no âmbito da legislação eleitoral, bancos de dados podem ser considerados como ativos econômicos, estando, assim, sujeitos às regras sobre doação.

FINALIDADE E REAPROVEITAMENTO DE BANCOS DE DADOS

É bastante comum que campanhas mantenham bases de dados antigas, coletadas ao longo dos anos e de diferentes períodos eleitorais. Diante disso, existe um questionamento bastante relevante sobre o que se pode fazer com essas bases. Elas podem ser utilizadas livremente? Há necessidade de algum procedimento, como uma nova coleta de consentimento?

São perguntas complexas e para as quais não há resposta certa, ao menos até que haja interpretações consolidadas acerca delas pelos órgãos competentes. A despeito disso, é possível levantar alguns possíveis caminhos a partir do que já foi exposto nesse documento. Dessa forma, é importante atentar para a definição de tratamento de dados pessoais, bem como para os princípios e bases legais que legitimam esse tratamento.

O tratamento de dados ocorre a todo momento em que uma das ações descritas no art. 5º, X da LGPD - como coleta, classificação, utilização, reprodução, armazenamento, etc - é realizada. Assim, a manutenção de uma base de dados, mesmo sem uma utilização efetiva é, em si, um tratamento de dados e, por isso, requer uma base legal adequada que a justifique. Por esse motivo, não é recomendável que partidos, candidatos e campanhas, armazenem dados sem dar a eles utilização por longos períodos de tempo, na medida em que isso também desrespeita a ideia de um ciclo de vida dos dados, com o seu descarte uma vez atingida a finalidade. Guardar uma base de dados para o caso hipotético de ela vir a se tornar necessária ou útil não é uma boa prática do ponto de vista da proteção de dados pessoais.

Por outro lado, é compreensível o interesse em reutilizar bases de dados, a fim de se otimizar as campanhas a partir do contato com pessoas que, em tese, já apresentaram algum nível de interesse naquele determinado candidato. Diante disso, as considerações sobre princípios, especialmente da finalidade, e bases legais, são relevantes. Em primeiro lugar, todo tratamento de dados deve ter uma finalidade específica e informada ao titular e não pode haver um tratamento posterior que seja incompatível com essa finalidade. Isso se conecta, diretamente, com o dispositivo da LGPD que afirma que, no caso de requisição do consentimento, o controlador deve informar o titular dos dados sobre mudanças para finalidades não compatíveis com a original.

Parece, portanto, que o cerne da questão é a compatibilidade da nova finalidade com a que deu origem ao primeiro tratamento dos dados pessoais em questão. As campanhas e candidatos devem se atentar, portanto, para a finalidade específica (lembrando que não basta uma finalidade como ‘’atividade político-partidária’’ ou mesmo ‘’campanha eleitoral’’) que deu origem àquela base de dados e avaliar, contextualmente, se a finalidade permanece ou se a nova finalidade é plenamente compatível com a anterior. Em todo caso, é importante que sejam adotadas medidas de transparência ativa, garantindo ao titular o direito de se opor ao tratamento, de for o caso.

RASPAGEM DE DADOS

Outra prática presente muitas vezes em campanhas é a coleta de dados em redes sociais, seja para identificar tendências no debate público, mapear perfil de eleitores ou identificar indivíduos alinhados com determinado partido ou candidato. Nestes casos, ainda que os dados sejam de acesso público, e tornados manifestamente públicos pelo titular, isso não significa que o tratamento desses dados pode ser realizado livremente.

Se a coleta ou raspagem de dados em redes sociais envolver dados pessoais é necessário que haja uma base legal que autorize esse tratamento. Além disso, o princípio da finalidade e da transparência também colocam restrições para essas práticas. Por um lado, quando uma campanha coleta dados pessoais em redes sociais, configura-se um tratamento para finalidades incompatíveis com aquelas para as quais o dado foi tornado público. Ao publicar conteúdos ou informações nas redes sociais, o usuário em regra não espera que esses dados sejam utilizados por campanhas. Por outro lado, esse tipo de tratamento normalmente ocorre sem que o titular receba qualquer tipo de informação quanto ao tratamento desses dados, colidindo com o princípio da transparência. Em paralelo, devem ser respeitados, ainda, os direitos dos usuários previstos no Marco Civil da Internet.

Essas restrições, todavia, não se aplicam a toda e qualquer coleta de dados em redes sociais. Quando a coleta ou a raspagem de dados envolver exclusivamente dados anonimizados, não se configura tratamento de dados pessoais, para fins da LGPD. Para que os dados sejam considerados anonimizados, o processo de anonimização não pode ser revertido a partir de esforços razoáveis. Nestes casos, a análise deverá levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

OS DADOS DOS CANDIDATOS DEVEM SER PROTEGIDOS?

A proteção de dados pessoais se estende a todos, abrangendo tanto eleitores quanto candidatos. Dados pessoais de candidatos e candidatas não deixam de ser dados pessoais pelo fato de tais indivíduos estarem disputando um processo eleitoral. Mas a garantia da proteção de dados pessoais não significa que estes dados não possam ser tratados, mas que este tratamento deve obedecer princípios e regras. No caso de candidatos, a Justiça Eleitoral estabeleceu como prática a divulgação de informações sobre candidaturas registradas em todo o Brasil, para cada pleito, bem como informações detalhadas sobre suas contas . Plataformas como a ***divulgacandcontas*** tem informado mais do que apenas filiação partidária, nome completo e limites de gastos das candidaturas, mas também dados como gênero, estado civil, data de nascimento, grau de instrução do candidato e declarações de bens. Essas atividades de tratamento se fundamentam na base legal desenhada para a relação estado-cidadão e são realizadas a partir de determinação legal e regulamentar, com o objetivo de oferecer informação aos eleitores e transparência a respeito da atividade partidária.

Nesses casos, o uso de dados se dá para a "persecução de um interesse público" que está dentre as "competências legais"do TSE (artigo 7, III, combinado com o artigo 23) e, também, deve estar em plena conformidade à LGPD. Para equilibrar a transparência e a informação ao eleitor e o regime de proteção de dados pessoais, vale ponderar que a divulgação de informações relativas aos candidatos deve atender aos princípios da finalidade, necessidade e adequação, bem como ao interesse público vislumbrado na divulgação de informações pessoais extremamente necessárias ante o contexto do pleito eleitoral. Essa parametrização é necessária, a fim de evitar exposições indevidas e que os próprios candidatos também sejam vítimas de ataques de divulgação de suas informações pessoais (conhecidos como ***doxxing***) durante o período de campanha, o que pode ensejar assédio direcionado, ameaças e outros ilícitos. Nesse sentido, o próprio TSE proferiu uma decisão recente restringindo a divulgação no ***divulgacandcontas*** de dados pessoais de candidatos que não foram eleitos. No caso, o tribunal se valeu da LGPD como norte interpretativo e pontuou que a finalidade que justificativa a publicidade dos dados se exauriu com o fim do processo eleitoral uma vez que o candidato não foi eleito.[7]

7 Tribunal Superior Eleitoral. Processo Administrativo nº 0600448-51.2019.6.00.0000. Relator Ministro Og Fernandes.