

UNIVERSIDADE PRESBITERIANA MACKENZIE

GUSTAVO HERMES HENNEMANN

IMPACTOS DA LEI GERAL DE PROTEÇÃO
DE DADOS NAS ELEIÇÕES DE 2020

São Paulo

2019

GUSTAVO HERMES HENNEMANN

IMPACTOS DA LEI GERAL DE PROTEÇÃO
DE DADOS NAS ELEIÇÕES DE 2020

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie como requisito parcial à obtenção do grau de Bacharel em Direito.

ORIENTADOR: PROF. DR. DIOGO RAIS

São Paulo
2019

GUSTAVO HERMES HENNEMANN

IMPACTOS DA LEI GERAL DE PROTEÇÃO
DE DADOS NAS ELEIÇÕES DE 2020

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie como requisito parcial à obtenção do grau de Bacharel em Direito.

Aprovado em:

BANCA EXAMINADORA

Prof. Dr. Diogo Rais

Examinador(a)

Examinador(a)

À pequena Isabel, pedaço de mim.
À gigante Martha, que tantas coisas fez e
outras tantas deixou de fazer para que este
momento chegasse.

AGRADECIMENTOS

Ao mestre e amigo Diogo Rais, pela impressionante capacidade de inspirar, pela paciência e clareza ao ensinar e por ter me aceito como orientando.

Às colegas e amigas Clara Brino Cacioli, Renata Nogueira Nascimento e Julia Narumi Nishio, pela parceria, lealdade e companheirismo nestes cinco anos de graduação.

Ao Henrique Andrea de Lima, pela gentileza ao aprimorar o *abstract* deste trabalho.

À Maria Luiza Correia Fernandes, pela rigorosa revisão de formatação.

*Ya estoy en la mitad de esta carretera
Tantas encrucijadas quedan detrás
Ya está en el aire girando mi moneda
Y que sea lo que
Sea*

(Jorge Drexler)

Impactos da Lei Geral de Proteção de Dados nas eleições de 2020

Gustavo Hermes Hennemann

Resumo

O artigo busca projetar o impacto que os principais institutos e regras da Lei Geral de Proteção de Dados – atualmente em período de vacância– podem trazer ao processo eleitoral de 2020, fazendo um exercício de cotejamento entre os dispositivos da norma e práticas comuns em campanhas políticas no Brasil. O texto também descreve casos paradigmáticos de uso indiscriminado de dados pessoais nas eleições presidenciais dos EUA, em 2016, e do Brasil, em 2018, apontando como tais situações seriam enfrentadas pela LGPD. O trabalho propõe ainda que a Autoridade Nacional de Proteção de Dados, órgão em fase de instalação, crie uma unidade especializada no intuito de aplicar a legislação de forma adequada e proporcional ao cenário eleitoral. Constata-se, ao fim, que há obstáculos para a implementação integral do sistema de proteção de dados até as próximas eleições e que a tutela da privacidade do indivíduo precisa ser equilibrada com o direito do eleitor de ter acesso à informação plural.

Palavras-chave: Eleições. Dados Pessoais. LGPD. ANPD. Direito Eleitoral Digital.

Abstract

This paper aims to outline the impact of the main elements of the Brazilian General Data Protection Law – still in *vacatio legis* – on the 2020 electoral process, by projecting how the new rules can be applied to standard political campaign practices. The text also describes paradigmatic cases of indiscriminate use of personal data in the most recent presidential elections in the US as well as in Brazil, pointing out how the new law would face such situations. The paper also proposes the establishment of a specialized unit by the National Data Protection Authority – to be set up – to apply the legislation appropriately and proportionally to the electoral environment. At last, the text concludes a) there are obstacles to the full implementation of the data protection system until the next elections; and b) individual privacy protection needs to be balanced with the voter's right to access plural information.

Keywords: Elections. Personal Data. LGPD. ANPD. Digital Electoral Law.

Sumário: 1. Introdução. 2. As regras eleitorais de proteção de dados e as evidências de vulnerabilidade 3. O sistema da LGPD e as normas com maior potencial de impacto nas eleições 4. A proteção prevista pela LGPD e os potenciais reflexos na campanha de 2020 5. O papel da ANPD e as possíveis adaptações da legislação ao contexto eleitoral 6. Considerações Finais 7. Referências.

1 Introdução

No segundo semestre de 2020, o Brasil realizará eleições municipais. Estima-se que aproximadamente 500.000 candidatos disputarão os cargos de prefeito, vice-prefeito e vereador justamente no período em que deve estrear a LGPD (Lei Geral de Proteção de

Dados). O impacto dessa nova norma no cotidiano nacional gera expectativas, em razão de seu amplo alcance e da relevância que os dados pessoais assumiram na dinâmica econômica e política, inclusive nas campanhas eleitorais.

Tecnicamente definido pela LGPD como “informação relacionada à pessoa natural identificada ou identificável”, dado pessoal, na prática, é um número de um documento, endereço completo, telefone ou mesmo um conjunto de informações sobre hábitos de alguém que podem levar à sua identificação. Cada vez mais, a presença física de um indivíduo está sendo substituída por esses dados, que representam a pessoa em suas relações com fornecedores, instituições públicas e demais interlocutores, constituindo uma espécie de corpo eletrônico (DONEDA, 2016). Ou seja, os dados pessoais são, em última instância, a própria pessoa.

No processo eleitoral, que envolve, fundamentalmente, um trabalho de persuasão e dissuasão por parte dos candidatos, as redes sociais digitais e os aplicativos de mensagem ganharam protagonismo em razão da escala, precisão e efetividade na entrega de propaganda. Esse conteúdo utiliza como insumo primário e como canal de acesso justamente dados pessoais. Em 2018, a regulamentação se mostrou limitada e insuficiente para tutelar os direitos dos eleitores nesse âmbito, o que justifica que se busque projetar e analisar o alcance das regras da LGPD sobre o contexto fático das próximas eleições. Esse é o principal propósito deste trabalho.

A primeira seção do artigo descreve os dispositivos já existentes na legislação eleitoral no intuito de proteger dados do eleitor e apresenta uma síntese dos episódios que expuseram a forma abusiva como as informações pessoais foram utilizadas para propaganda em campanhas nos EUA, em 2016, e no Brasil, em 2018.

Na segunda parte, são apresentadas as principais inovações trazidas pela LGPD, com ênfase nos institutos que compõem o núcleo da norma e que devem trazer maior impacto às atividades eleitorais.

Em seguida, a partir do cotejamento entre os dispositivos legais e práticas habituais de campanha, o trabalho faz um esforço de projeção do impacto da lei e aponta eventuais dificuldades que os candidatos poderão enfrentar para se adaptar às novas regras.

Por fim, a quarta seção dedica-se a explicar por que a estruturação da ANPD (Autoridade Nacional de Proteção de Dados) é essencial para que a LGPD seja implementada com efetividade. O trabalho também menciona alguns obstáculos à vigência integral da norma

já nas próximas eleições e propõe a criação de uma unidade administrativa especializada para cuidar dos dados pessoais dos eleitores.

2 As regras eleitorais de proteção de dados e as evidências de vulnerabilidade

A minirreforma realizada em 2009 na Lei nº. 9.504, conhecida como Lei das Eleições, trouxe novidades para a tutela de dados pessoais dos indivíduos especificamente no âmbito eleitoral, com a introdução de dois artigos que passaram a abordar o tema.

O art. 57-E proíbe determinadas pessoas jurídicas¹ de utilizar, doar ou ceder o “cadastro eletrônico de seus clientes, em favor de candidatos, partidos ou coligações”, além de vedar em seu § 1º a “venda de cadastro de endereços eletrônicos”. O dispositivo denota cuidado com as formas de acesso a dados pessoais pelas campanhas e tenta impedir que os cadastros e endereços eletrônicos sejam utilizados para finalidade diferente daquela imaginada pelo indivíduo cadastrado, sem que ele seja informado (CRUZ, 2018, p. 167).

Já o art. 57-G estabelece que as mensagens eletrônicas enviadas pelas campanhas eleitorais, independentemente do meio utilizado, precisam “dispor de mecanismo que permita seu descadastramento pelo destinatário”, o que deve ser feito em 48 horas pelo remetente sob pena de multa de R\$ 100,00 por mensagem após o prazo. Aqui se busca dar ao eleitor o poder de decidir quem pode ou não continuar lhe enviando conteúdo.

Esses dois dispositivos, que se restringem a algumas formas de tratamento de dados entre as muitas possíveis, foram os únicos vigentes durante a eleição de 2018, quando as práticas de propaganda eleitoral deixaram evidente para as autoridades e para toda a sociedade que os dados pessoais dos eleitores estavam desprotegidos também do ponto de vista jurídico (CRUZ, 2019).

Antes de expor o que se sabe até o momento sobre o uso indiscriminado de dados pessoais de eleitores brasileiros no último pleito, é necessário recordar o caso paradigmático da campanha digital de Donald Trump, ao concorrer à Presidência dos EUA em 2016. A imprensa internacional revelou em março do ano passado (CADWALLADR, 2018; ROSENBERG, 2018) como a empresa britânica Cambridge Analytica, contratada pela campanha do atual presidente americano, utilizou dados pessoais de 87 milhões de usuários do Facebook obtidos ilegalmente para entregar propaganda personalizada via correios, TV e redes sociais aos eleitores americanos.

¹ O art. 57-E faz referência às pessoas relacionadas no art. 24 da Lei das Eleições, que elenca entidades que integram ou que se relacionam com a administração pública em geral, além daquelas com caráter filantrópico, sindical, religioso e esportivo.

O marketing praticado pela empresa, como explicou o próprio executivo-chefe, Alexander Nix, baseia-se em três pilares, que, para a lógica eleitoral, podem ser assim resumidos: a) teorias de ciências comportamentais são utilizadas para se estabelecer elementos genéricos de personalidades humanas que sejam do interesse do estrategista de campanha para a categorização de eleitores; b) uma infinidade de dados pessoais é analisada pela metodologia de *big data*² dentro de um modelo informático capaz de fazer um enquadramento de pessoas reais em diferentes categorias de personalidade, deduzindo assim as inclinações políticas dos indivíduos; c) as mensagens de propaganda são desenvolvidas de forma segmentada e entregues com um alto grau de aderência a cada eleitor.

Em síntese, a Cambridge Analytica “elabora materiais específicos para pessoas mais ‘amáveis’, ‘neuróticas’ ou menos ‘extrovertidas’, por exemplo. Ao explorar a dimensão da personalidade que mais afeta cada pessoa, a empresa aumenta a chance de que o eleitor vote em determinado candidato” e facilita a convergência de votos de pessoas com visões de mundo completamente diferentes (FLORES, 2017).

A ferramenta de informática utilizada pela campanha de Trump havia sido desenvolvida por um professor associado da Universidade de Cambridge, Aleksadr Kogan, que participou de uma pesquisa acadêmica que coletou o consentimento de 270 mil pessoas para o uso de seus perfis do Facebook com finalidade científica. Os dados pessoais desses usuários e de todos os seus amigos na rede social acabaram transferidos posteriormente, sem qualquer consulta ou autorização, para a empresa que prestou serviços ao então candidato a presidente dos EUA.

O episódio teve desdobramentos judiciais e econômicos, abalando a imagem do Facebook, que fechou acordo de US\$ 5 bilhões com as autoridades regulatórias norte-americanas para encerrar investigações em razão da fragilidade em sua política de privacidade (STACEY, 2019) e aceitou pagar outros £ 500 mil de multa à agência britânica de proteção de dados ICO (HERN, 2019). O escândalo político também fez com que se recalculasse a dimensão do impacto que o uso indevido de dados pessoais pode trazer aos sistemas de governo e, especialmente, aos processos de escrutínio em regimes democráticos. Isso porque Trump, surpreendentemente, venceu uma disputa acirrada com a ajuda de uma estratégia até então inédita, ao menos em grande escala.

² Trata-se de uma metodologia que permite aos computadores processar e organizar dados para inferir a ocorrência de acontecimentos, sem que esses dados estejam necessariamente estruturados. Por dispensar a estruturação, que toma tempo dos analistas à medida em que a quantidade de dados aumenta, o big data é revolucionário, por viabilizar análises em volume, velocidade e variedade antes impossíveis. BIONI, Bruno R. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 39-41.

No Brasil, a campanha de 2018 ocorreu sob a sombra do que havia sido então descoberto em relação à eleição americana. A Lei das Eleições sofreu novamente uma minirreforma no ano que antecedeu o pleito e algumas das modificações ampliaram as possibilidades de propaganda na internet, permitindo o impulsionamento pago de conteúdo nas redes sociais e outras plataformas, desde que seguidas as regras estipuladas pelos artigos 57-B e 57-C, que exigem, por exemplo, que o material seja identificado como propaganda eleitoral (RAIS, 2018). Apenas candidatos, partidos e coligações foram autorizados a impulsionar conteúdo, sendo vedadas, portanto, eventuais “doações” nessa modalidade por pessoas naturais que queiram pagar para aumentar a visibilidade de seu candidato nas plataformas digitais.

As alterações da legislação em 2017 abriram a possibilidade de que as campanhas passassem a utilizar ferramentas de microdirecionamento oferecidas em aplicações de internet, sobretudo no Facebook, em que é possível escolher um público-alvo específico, dentro de determinada região geográfica, por faixa etária ou por gênero, por exemplo, dependendo do tipo de eleitor que a propaganda busca alcançar (CRUZ, 2018, p. 172). Apesar disso, nenhuma nova regra foi introduzida naquele ano com o objetivo de proteger os dados pessoais dos eleitores, que acabariam sendo bastante alcançados em outro canal digital, o aplicativo de mensagens WhatsApp, protagonista da principal polêmica envolvendo as estratégias de marketing no pleito de 2018.

O uso irregular de dados pessoais de eleitores brasileiros para propaganda eleitoral desse ano foi revelado pela imprensa, assim como no caso norte-americano. Aqui, porém, as reportagens foram publicadas em plena campanha do segundo turno, disputado entre Jair Bolsonaro (PSL) e Fernando Haddad (PT). O jornal Folha de S.Paulo (MELLO, 2018) e o site de notícias UOL (REBELLO, 2018) revelaram como agências de marketing digital viabilizaram o disparo em massa de mensagens com propaganda eleitoral via WhatsApp para números de telefone que constavam de bancos de dados comprados de terceiros, cuja origem exata até hoje não foi esclarecida.

As reportagens afirmaram que empresários apoiadores de Bolsonaro contrataram diretamente os serviços das agências de marketing digital Yacows, Quick Mobile e CrocServices, e também adquiriram 40 licenças de um software de disparos em massa da empresa espanhola EnviaWhatsApp, o que possibilitou o encaminhamento de até 20 mil mensagens por hora (MELLO, 2019). Esses programas oferecidos pelas agências são

necessários para esse tipo de ação no caso do WhatsApp porque a plataforma do aplicativo em si não permite e até coíbe a prática do *spam*, como são chamados os disparos em massa.

Os relatos indicam que o processamento ilegal de dados pessoais na campanha brasileira não se resumiu ao uso de cadastros comprados de terceiros, cuja finalidade original nada tinha a ver com atividade política. Segundo as reportagens, a agência QuickMobile minerava números de celulares disponíveis nos perfis de redes sociais e a agência Yacows usava nomes, datas de nascimento e documentos de idosos sem qualquer consentimento para a compra de chips de operadoras de telefonia (RODRIGUES; MELLO, 2018). Isso seria necessário, segundo pessoas ouvidas pela imprensa, para a manutenção do esquema de disparo em massa, que demandava muitos números diferentes, já que o WhatsApp bloqueia perfis após o envio de quantidades excessivas de mensagens.

Os representantes das campanhas de Bolsonaro e Haddad chegaram a admitir aos jornalistas que utilizaram o sistema BulkServices, da agência Yacows, para disparos em massa pontuais via WhatsApp, mas disseram que, para isso, usaram cadastros próprios, com dados de apoiadores e filiados, que cederam as informações voluntariamente.

Os episódios relatados indicam a violação de inúmeros dispositivos da legislação eleitoral, como o provável financiamento ilegal por parte das pessoas jurídicas, que acabaram doando ao candidato o serviço contratado com as agências de marketing digital. Há provável violação também do art. 57-B, III, que autoriza o envio de mensagens eletrônicas apenas para “endereços cadastrados gratuitamente pelo candidato, partido ou coligação” (CRUZ; MASSARO; BORGES, 2018, pg. 26). Em decorrência do que foi divulgado pela imprensa, a Polícia Federal abriu inquérito e, por iniciativa das coligações lideradas pelo PT e pelo PDT, foram instauradas duas Ações de Investigação Judicial Eleitoral no TSE³. Até a conclusão deste trabalho⁴, nenhuma delas havia sido julgada.

No âmbito da ação ajuizada pela coligação liderada pelo PDT⁵, o Corregedor-Geral da Justiça Eleitoral, Ministro Jorge Mussi, determinou, em 10 de outubro de 2019, que as operadoras de telefonia celular informassem os números utilizados pelas agências de marketing digital investigadas e por seus respectivos sócios (TUROLLO JR., 2019). A decisão veio dois dias depois de o Gerente de Políticas Públicas e Eleições Globais do WhatsApp, Ben Supple, admitir publicamente que constatou, na eleição brasileira de 2018, a

³ Tribunal Superior Eleitoral.

⁴ Última consulta à tramitação processual realizada em 05 de novembro de 2019, data de entrega do presente trabalho na Faculdade de Direito da Universidade Presbiteriana Mackenzie.

⁵ AIJE nº 0601782-57.2018.6.00.0000.

“atuação de empresas fornecedoras de envios maciços de mensagens” que violaram os termos de uso do aplicativo “para atingir um grande número de pessoas” (MELLO, 2019b). Esse desdobramento também levou à reabertura da fase de instrução da ação ajuizada pela coligação liderada pelo PT⁶, para que as informações e as provas eventualmente produzidas no outro processo possam ser aproveitadas por este, já que ambos têm o mesmo objeto de apuração (MARTINES, 2019).

Apesar de a estratégia dos disparos em massa via WhatsApp ter um caráter descentralizado e de difícil mensuração, pela natureza privada das mensagens, alguns indícios apontam que ela impactou a campanha de forma substancial. Segundo pesquisa realizada pela Opinion Box e publicada pelo site especializado em telecomunicações MobileTime, 26% dos brasileiros com mais de 16 anos que possuem smartphones receberam mensagens de números desconhecidos sobre política no WhatsApp ao longo do período eleitoral (PAIVA, 2018).

O processamento de dados pessoais sem a devida transparência e controle, portanto, parece ter influenciado a última eleição no Brasil, embaralhando as regras da comunicação, com propaganda massiva sem origem clara e praticamente irrastrável. Mesmo que não se tenha domínio total sobre a extensão e a gravidade do problema, é razoável pensar que a Lei Geral de Proteção de Dados pode contribuir para melhorar o arcabouço normativo que regulará o processo de escolha de prefeitos e vereadores em 2020.

3 O sistema da LGPD e as normas com maior potencial de impacto nas eleições

Uma análise estrutural dos dez capítulos que integram a Lei Geral de Proteção de Dados evidencia que não se trata apenas de novas regras para tutelar direitos da personalidade decorrentes da era digital. É a introdução de um verdadeiro sistema de proteção de dados pessoais no ordenamento jurídico brasileiro.

A aprovação da norma pelo Congresso Nacional, depois de oito anos de debates, está vinculada a um movimento global, capitaneado pela União Europeia, no intuito de trazer mais proteção à privacidade dos cidadãos ao mesmo tempo em que se dá mais segurança jurídica ao setor privado. Essa tentativa de conciliar o desenvolvimento tecnológico e econômico com a defesa de garantias individuais constitucionais decorre do fato de o processamento de dados pessoais servir hoje de insumo ou mesmo de núcleo tanto para atividades comerciais quanto para a formulação de políticas públicas, como observa o parecer da Comissão de Assuntos

⁶ AIJE nº 0601771-28.2018.6.00.0000

Econômicos do Senado ao final da tramitação do então projeto de lei (FERRAÇO, 2018, p. 3).

A nova norma brasileira tem uma grande amplitude de incidência. Abarca atos praticados por pessoas naturais e jurídicas, de direito público e privado, em todas as formas de operação realizadas com dados pessoais, unificadas pelo termo genérico “tratamento”⁷, seja em plataformas analógicas ou digitais. Foram excluídas do escopo da lei apenas atividades de investigação penal e segurança pública, além de trabalhos jornalísticos, artísticos e acadêmicos. Essa abrangência é uma característica central e inovadora, já que, até então, o tema era abordado somente de forma setORIZADA e parcial, em diplomas esparsos como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e o Marco Civil da Internet.

Além disso, a técnica legislativa adotada dedica os primeiros artigos para estabelecer os pilares do sistema, em disposições preliminares, que elencam os fundamentos e os princípios a serem considerados na redação, interpretação e aplicação dos dispositivos, além de trazer 19 conceitos técnicos, que constituem um glossário para dar mais precisão e clareza ao texto legal.

Por fim, a LGPD estabelece a arquitetura de uma Autoridade Nacional de Proteção de Dados, com competências detalhadas em 24 incisos, que incluem a fiscalização e aplicação das sanções administrativas previstas, a edição de normas infralegais, orientações aos destinatários da norma, e a promoção de atividades e políticas públicas para o setor – o órgão é descrito com mais detalhes na seção 5 deste artigo.

Como este trabalho busca vislumbrar os tipos de proteção que a lei pode trazer aos dados pessoais do eleitor na prática e os possíveis efeitos para os métodos de propaganda eleitoral, serão enfatizados os elementos mais relevantes, com potencial de impacto nesse âmbito.

Entre os fundamentos⁸ elencados pela lei em seu Art. 2º, destacam-se os dois primeiros, “o respeito à privacidade” e “a autodeterminação informativa”, que estão entrelaçados.

⁷ Art. 5º Para os fins desta Lei considera-se: (...) X - tratamento: toda operação realizada com dados pessoais, como as que se referem 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;

⁸ Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

Privacidade, em essência, é a “capacidade de o indivíduo controlar a circulação de informações a seu respeito” (LEONARDI, 2011, p. 67). O conceito atual do termo entende que o controle do sujeito sobre seus dados vai além de decidir sobre o que pode ou não ser comunicado para além de sua intimidade, estendendo-se para sempre, mesmo depois de os dados estarem sob a posse de terceiros, pois será sempre ele o titular. Essa concepção de que o sujeito deve poder controlar o trânsito de seus dados pessoais permanentemente, de forma dinâmica, é a base do princípio da autodeterminação informativa. Isso traz como reflexo a obrigação de transparência por parte do controlador dos dados, que precisa dar ao titular informações suficientes para que ele requisite, por exemplo, a correção ou a eliminação de dados seus que estejam sob tratamento (MALDONADO; BLUM, 2019, p. 26-28).

Em relação aos princípios⁹ estabelecidos no Art. 6º, cabe apontar o primeiro deles, o da “finalidade”, como um dos principais vetores de todo o sistema da LGPD, por vincular o uso dos dados pessoais ao objetivo comunicado ao titular antes de eles serem coletados. A descrição que consta do inciso I indica que os propósitos para o tratamento de dados têm de ser **legítimos, específicos e informados. (grifo nosso)**

Danilo Doneda (2011, p. 100), a partir da obra de Stéfano Rodotà, aponta que esse princípio tem muita relevância prática, pois “nele fundamenta-se a restrição da transferência de dados pessoais a terceiros” e, a partir dele, pode-se estruturar “um critério para valorar a

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

⁹ Art. 6º *As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*

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;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

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;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade)”.¹⁰

Diretamente vinculados a essa ideia estão os princípios da “adequação” (Art. 6º, II) e da “necessidade” (Art. 6º, III), que limitam o tratamento de dados pessoais a situações compatíveis com o objetivo informado ao titular e impedem uso excessivo e desproporcional, para além do mínimo necessário ao cumprimento da finalidade.

Tais fundamentos e princípios são balizas para o tratamento de dados pessoais, que somente podem ser processados por terceiros mediante o cumprimento de uma das dez hipóteses legais¹⁰ do Art. 7º, sendo que para este trabalho é suficiente detalhar a primeira delas, o “consentimento pelo titular”. As outras nove, para as quais não se exige o consentimento, tratam de situações específicas, como proteção da vida do próprio titular ou proteção ao crédito, sem relação direta com o contexto eleitoral.

Principal base legal para o tratamento de dados pessoais, o consentimento também é a que traz maior segurança jurídica ao responsável pela operação. No entanto, para que seja reconhecido juridicamente, tem de cumprir alguns requisitos constantes do Art. 5º, XII, que descreve consentimento como a “manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

(grifo nosso)

Para que a manifestação de vontade seja livre, é preciso facultar ao titular a possibilidade de recusar o consentimento ou de revogá-lo futuramente. Sua decisão somente será informada se puder saber previamente as finalidades e se puder prever as consequências do tratamento de seus dados, por meio de explicações em linguagem simples e clara. E, para ser inequívoca, dependerá de um “ato positivo do titular”, que pode ser “mediante declaração

¹⁰ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (...).

escrita, inclusive em formato eletrônico ou oral” a ser “armazenado pelo controlador, para fins de prova” da obtenção do consentimento (MALDONADO; BLUM, 2019, p. 118-119). A definição legal tampouco considera válida autorização genérica quando o tratamento de dados tiver diversas finalidades, sendo necessário que se obtenha o consentimento de forma granular, oferecendo a possibilidade de o titular concordar ou não com cada finalidade.

Antes de passar à análise de como essas normas se assentam sobre o cenário eleitoral, vale destacar os quatro sujeitos abstratos das relações jurídicas previstas pela LGPD, para que os conceitos sejam mais bem articulados na seção seguinte. Além do titular dos dados pessoais, que é exclusivamente uma pessoa natural, foram criados os institutos do controlador, do operador e do encarregado¹¹.

Para distinguir um do outro, é importante ter claro que o controlador é quem supostamente tem o direito de utilizar os dados pessoais. Cabe a ele a tomada de decisões como o propósito do tratamento e o tempo de armazenagem, por exemplo, sendo dele a maior responsabilidade imposta pela lei. Já o operador age de acordo com as determinações e instruções passadas pelo controlador, em tarefas que podem ser simples ou complexas, a depender do caso. O encarregado, que será uma espécie de ouvidor especializado, servirá de elo entre o titular dos dados, o controlador, o operador e a Autoridade Nacional de Proteção de Dados. (MALDONADO; BLUM, 2019, p. 104-108)

4 A proteção prevista pela LGPD e os potenciais reflexos na campanha de 2020

De início, é importante identificar os atores reais do processo eleitoral com os institutos previstos na LGPD. O eleitor, claramente, corresponde à figura do titular dos dados pessoais, para os fins deste trabalho. Já o candidato ou a coligação, na maioria das vezes, será o controlador, que terá de comprovar que detém o direito de uso sobre os dados através do consentimento, além de disponibilizar um encarregado para receber reclamações de titulares e instruções da ANPD, em linha com o art. 41 da nova lei. Quando o candidato recorrer a prestadores de serviços para executar tarefas técnicas de tratamento de dados na campanha, como agências de marketing digital, estas exercerão o papel de operador, se o trabalho ficar restrito ao cumprimento das ordens do contratante.

¹¹ Art. 5º Para os fins desta Lei considera-se: (...)

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

A distinção de papéis, contudo, pode ficar menos nítida, a depender do caso concreto. Por exemplo, se uma agência tiver armazenado milhares de números de telefones celulares ao executar um trabalho lícito contratado por um cliente do ramo de varejo e decidir oferecer, posteriormente, um pacote de serviços de propaganda eleitoral a um candidato, incluindo o uso desses dados pessoais, estaria automaticamente assumindo o posto de controlador, por desvirtuar a finalidade pela qual os dados lhe foram confiados. A agência poderia, conseqüentemente, ser cobrada e responsabilizada como um controlador de dados, por equiparação, conforme previsão do art. 42, § 1º, I, da LGPD.

Seria esse um dispositivo capaz de, em 2020, dar resposta a episódios como os ocorridos na campanha de 2018, quando a imprensa relatou que agências de marketing digital ofereceram bancos de dados adquiridos de terceiros para disparos em massa de mensagens via WhatsApp. Além de estar sujeita a sanções administrativas¹² que nasceram com a LGPD, como advertências, multas e eliminação dos dados pessoais armazenados, a empresa poderia ser responsabilizada no âmbito civil¹³, cumulativamente. A conduta das prestadoras de serviços, segundo as reportagens, teria violado claramente o princípio da finalidade e afrontado os fundamentos da privacidade e da autodeterminação informativa, por inexistir consentimento ou qualquer outra base legal para o tratamento de dados realizado.

A nova lei também permitiria o enquadramento, como ato ilícito, da mineração de dados pessoais dispersos em perfis das redes sociais, como supostamente teria feito a agência QuickMobile em 2018, segundo os relatos jornalísticos. Isso porque o Art. 7º, § 4º, apesar de dispensar o consentimento quando o próprio titular torna manifestamente públicos os seus dados pessoais, mantém resguardados direitos e os princípios da LGPD. Não é legal nem legítima, portanto, a mineração de números de celulares e endereços de e-mails em redes sociais para envio posterior de propaganda política, ainda que o perfil do titular seja aberto a qualquer pessoa, por se tratar de um uso desconexo com o intuito ou expectativa do eleitor e

¹² Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração.

¹³ Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

por violar o art. 9º, que garante ao titular o direito de saber a finalidade específica do tratamento de um dado pessoal seu e de saber a identidade do controlador.

Apesar de o episódio da Cambridge Analytica ter ocorrido na eleição americana, é pertinente analisarmos também a adequação das ferramentas jurídicas da LGPD para enfrentar eventual situação similar no Brasil. Sobretudo se consideramos que o modelo utilizado pela empresa britânica, atualmente inativa em razão do escândalo, vem sendo divulgado como método de trabalho pela IDEA Big Data, empresa global que estabeleceu sua base de dados no Brasil e que afirma ter partidos políticos nacionais e estrangeiros entre seus clientes (GOLDHILL, 2019).

Conforme detalhado anteriormente, a lei veda o uso de dados coletados via redes sociais para fins eleitorais sem o consentimento explícito e específico. O grande desafio será trazer a público esse tipo de conduta, já que ocorre de forma imperceptível ao eleitor, sendo verificável, talvez, nas plataformas que permitem microdirecionamento de mensagens de propaganda impulsionadas. Uma vez revelada a ilegalidade, a ANPD poderá exigir que a empresa preste informações, detalhe seus serviços de tratamento de dados e, no caso de ilícitos comprovados, poderá impor sanções como multa e determinação para que os dados sejam eliminados.

Deixando para trás o que ocorreu nos pleitos passados e tentando olhar para as mudanças que a LGPD pode exigir nas rotinas de trabalho das equipes de campanha eleitoral, é possível vislumbrar dificuldades no gerenciamento dos bancos de dados que reúnem cadastros de eleitores. Diante do cerco da legislação eleitoral e da LGPD ao uso de cadastros montados por terceiros, os contatos pessoais armazenados pelos próprios candidatos ganham ainda mais importância para articulação das ações de propaganda.

A primeira preocupação do candidato deverá ser com a forma de coleta desses dados pessoais. Isso porque o eleitor precisa assinalar ou declarar expressamente que consente com o tratamento de seus dados, para que se configure a hipótese legal do art. 7º, I, e para que ela esteja consoante o art. 8º, que exige o consentimento “por escrito ou por outro meio que demonstre a manifestação de vontade do titular”.

Opções pré-selecionadas ou o mero silêncio passivo não serão considerados manifestação do consentimento inequívoco, não havendo espaço para dúvidas acerca da efetiva intenção do titular. Na ausência de certeza, certamente se estará em momento de insegurança para o controlador, o que pode ensejar o entendimento da ilicitude do tratamento dos dados pessoais, com as consequências negativas daí decorrentes. (MALDONADO; BLUM, 2019, p. 182).

Não seria recomendável para esse fim, portanto, a utilização da tradicional lista de presença que costuma circular em eventos, na qual as pessoas inserem seus dados de contato, ainda que constasse no final ou no começo do documento uma observação por escrito dizendo que a assinatura autoriza o uso dos dados para envio de conteúdo eleitoral por determinado candidato. Isso porque o eleitor, ao inserir seus dados em determinada altura da lista de papel, poderia deixar de ler o alerta genérico, configurando um consentimento passivo ou pré-selecionado, que pode ser considerado nulo. Tal formato seria, por isso, ineficaz para comprovar inequivocamente o consentimento dos eleitores e legitimar o envio posterior de propaganda. O recomendável, em casos como esse, é um modelo de documento que abra espaço para algum ato positivo do eleitor, que demonstre claramente a manifestação de vontade, como um alerta contíguo a cada assinatura da lista em que se possa coletar a anuência por meio de um X, por exemplo. Essa mesma preocupação deve permear a coleta do consentimento via plataformas digitais, onde o ato positivo poderia ser um clique do eleitor em uma caixinha posicionada ao lado de uma breve e simples explicação sobre o intuito da coleta dos dados.

Outra questão a ser equacionada é a utilização de cadastros de eleitores em diferentes eleições, em razão de um aparente conflito com a regra da finalidade específica.

A incerteza deve recair já sobre 2020. Os candidatos que concorrerão à reeleição e pretendem usar dados pessoais captados em campanhas anteriores terão de buscar o consentimento dos titulares nos termos da LGPD? Em princípio, entende-se que sim, pois apesar de as informações já terem sido coletadas, ocorrerão novos tipos de tratamento nas espécies armazenamento, acesso, utilização, etc., já em plena vigência da lei, aplicando-se as novas regras (MALDONADO; BLUM, 2019, p. 116). Seria preciso, então, ir atrás dos eleitores para obter-lhes o consentimento expresso para que qualquer tipo de tratamento com os dados armazenados em campanha anteriores seja lícito. Caso contrário, os candidatos estão suscetíveis às sanções, como o bloqueio ou eliminação dos dados.

E poderia um candidato utilizar os dados pessoais coletados em 2020 também nos pleitos seguintes? Como as campanhas futuras são mera hipótese e podem não se concretizar por uma infinidade de motivos, a coleta de consentimento do eleitor para enviar-lhe propaganda eleitoral também em 2022 ou 2024 dá a impressão de não estar sintonizada com a ideia de finalidade específica, por serem eventos aleatórios. Sendo assim, parece prevalecer o disposto no art. 15, I, da LGPD, que determina o término do tratamento de dados, ou seja, a

eliminação deles, assim que a finalidade for alcançada, o que se daria no último dia de campanha oficial.

Essa obrigação teria forte impacto sobre políticos mais longevos, que têm como vantagem competitiva justamente os canais já estabelecidos e a base de eleitores construída ao longo de diversas eleições.

Outra conduta que vai de encontro à regra da finalidade específica é o uso de um mesmo banco de dados por diferentes candidatos.

Seria permitido a um candidato a prefeito, por exemplo, utilizar cadastros montados por candidatos a vereador de seu partido no intuito de amplificar o alcance de sua propaganda? Como já exposto anteriormente, o princípio da finalidade exige que, para ser lícito o tratamento de dados neste caso, o consentimento do eleitor teria de ter dado, especificamente, para o envio de mensagens de propaganda pelo candidato ao Legislativo e também para o compartilhamento com a campanha do candidato ao Executivo, conforme disposição expressa do art. 7º, § 5º¹⁴. O dispositivo encerra qualquer dúvida e evidencia a impossibilidade de um candidato, uma coligação ou um partido simplesmente ceder seu banco de dados a um aliado sem o devido acionamento e consentimento do eleitor.

Ademais, se for coletado o consentimento do eleitor em uma mesma oportunidade para envio de mensagens de propaganda por diversos candidatos¹⁵, essa decisão precisaria ser livre e, para isso, como destacado na seção anterior, é necessário que se obtenha o consentimento de forma granular, sendo exigível que o eleitor possa escolher, de um em um, quais candidatos ele autorizaria como remetentes, pois são finalidades distintas.

Por fim, as mensagens de propaganda, independentemente do canal que utilizem para chegar ao eleitor, precisarão dispor de informações ou botão direto que permitam a revogação do consentimento, para que se cumpra o disposto no Art. 8, § 5º¹⁶, da nova lei.

Cabe registrar que todas as inferências feitas nesta seção decorrem de um exercício de cotejamento entre os dispositivos da LGPD e práticas corriqueiras em campanhas eleitorais no Brasil. Por isso, estão sujeitas a revisão, já que a aplicação prática da norma ainda depende

¹⁴ §5º *O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.*

¹⁵ Aqui se vislumbra uma situação comum em eleições para os cargos de deputado federal e deputado estadual -o que ocorreria em 2022-, quando formam-se as “dobradinhas”, em que candidatos a cargos distintos fazem propaganda um do outro, no intuito de potencializar o alcance da campanha de cada um.

¹⁶ § 5º *O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.*

do fim de sua vacância e pode ser direcionada via regulamentos infralegais a serem editados pela Autoridade Nacional de Proteção de Dados, ainda em fase de implantação, como veremos na seção seguinte.

5 O papel da ANPD e as possíveis adaptações da legislação ao contexto eleitoral

Entidade garantidora do sistema criado pela LGPD, a Autoridade Nacional de Proteção de Dados nasceu como órgão da administração pública federal ligada à Presidência da República. Dotada de autonomia técnica e decisória, teve sua composição e competências definidas pelos artigos 55-A a 55-L, introduzidos pela Medida Provisória 869, em dezembro de 2018, quase cinco meses após a aprovação dos demais dispositivos. Sua estrutura regimental será definida por ato do Presidente da República, como previsto pelo Art. 55-G, mas até a conclusão deste trabalho¹⁷ o texto do futuro decreto ainda não havia sido apresentado.

A criação da ANPD, com caráter centralizado, pretende trazer mais efetividade e um padrão consistente à aplicação das regras de proteção de dados, o que teoricamente oferecerá mais segurança jurídica em comparação com um cenário hipotético em que caberia apenas ao Poder Judiciário interpretar e aplicar a LGPD. A norma estabelece medidas regulatórias e competências que dão certa flexibilidade à ANPD para adaptação da lei às novas circunstâncias que podem surgir em razão do desenvolvimento tecnológico, o que é relevante nesta esfera para que a legislação não se torne logo obsoleta. O órgão pode ainda “estabelecer parâmetros para a aplicação da lei conforme as características de cada setor ou mercado, objetivando ações que sejam mais eficazes para a proteção de direitos do cidadão e garantindo a proporcionalidade na sua aplicação” (DONEDA, 2018).

Nesse sentido, é possível que se vislumbre a forma como a ANPD poderia atuar em um contexto eleitoral. Devido à relevância das eleições para o sistema institucional brasileiro e a dimensão dos pleitos que ocorrem de dois em dois anos, é razoável que se considere a alternativa de criação de uma unidade especializada, lastreada no Art. 55-C¹⁸, VI, da LGPD, com a atribuição de zelar pela aplicação da legislação de proteção de dados nesse campo.

¹⁷ Última atualização realizada em 05 de novembro de 2019, data de entrega do presente trabalho na Faculdade de Direito da Universidade Presbiteriana Mackenzie.

¹⁸ Art. 55-C. A ANPD é composta de:

I - Conselho Diretor, órgão máximo de direção;

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;

III - Corregedoria;

IV - Ouvidoria;

V - órgão de assessoramento jurídico próprio; e

A unidade especializada poderia operacionalizar o exercício das competências da ANPD na relação com o cidadão, aqui na condição de eleitor, e com os candidatos, via encarregado a ser indicado pela campanha. Isso, na prática, seria concretizado, por exemplo, com: a) realização de consultas públicas para a coleta de sugestões de partidos políticos, Justiça Eleitoral e entidades do terceiro setor; b) edição de normas infralegais específicas para aplicar a LGPD com proporcionalidade e para dar mais segurança aos atores envolvidos nas eleições; c) estruturação de sistemas eletrônicos para o recebimento de reclamações de eleitores sobre o tratamento de dados em desconformidade com a legislação; d) fiscalização e sanção de atividades de campanha que se utilizem de dados pessoais de forma irregular.

A atuação desse braço eleitoral de proteção de dados, obviamente, teria de se restringir às suas competências legais, sem invadir a esfera da Justiça Eleitoral. Isso não impede, porém, que se estabeleça um convênio entre a ANPD e o TSE, a quem cabe a administração de todo o processo eleitoral, para que exista intercâmbio de informações e acompanhamento conjunto de procedimentos investigatórios, que poderiam ter efeitos ampliados. Um candidato cuja campanha utilize dados pessoais em desconformidade com a LGPD, hipoteticamente, pode estar obtendo vantagem comparativa em relação a seus concorrentes, o que traria desdobramentos para o âmbito eleitoral, ensejando, por exemplo, providências do Ministério Público Eleitoral.

Um ajuste formal entre os órgãos públicos poderia trazer sinergia e, conseqüentemente, mais eficiência às atividades de ambos. Essa ideia também parece encontrar guarida nos dispositivos da lei, que atribui à ANPD, no Art. 55-J, XXIII, a competência de se articular com “autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação”. O possível trabalho conjunto entre ANPD e Justiça Eleitoral estaria em consonância ainda com o prescrito no Art. 55-J, § 3^o¹⁹ e § 4^o²⁰, que estimulam a coordenação de atividades entre órgãos reguladores nas respectivas esferas de atuação e a cooperação técnica a fim de aprimorar a aplicação da LGPD.

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

¹⁹ Art. 55-J. *Compete à ANPD: (...) § 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei.*

²⁰ § 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.

Outro aspecto que pode ser analisado é a forma de responsabilização do candidato, da coligação ou do partido que utilizar dados pessoais de forma irregular ao longo da campanha. Além de estar sujeito a sanções administrativas do Art. 52 da LGPD, o infrator poderia também ser alcançado pelo Sistema Judiciário Eleitoral, caso o TSE admita a incidência das normas de proteção de dados em processos de sua competência. Tal desdobramento, porém, dependeria de estudos de compatibilização entre sistemas normativos e demandaria eventuais resoluções editadas pela Justiça Eleitoral ou adaptações de dispositivos legais, no intuito de prever sanções neste âmbito²¹.

As proposições aventadas nesta seção não ignoram o fato de que a nova legislação deve entrar em vigor integralmente em 16 de agosto de 2020, exatamente o mesmo dia em que fica permitida a campanha eleitoral, nos termos do Art. 36 da Lei das Eleições. A possível coincidência enfatiza o caráter de novidade da norma e parece alertar para a necessidade de a ANPD e o TSE estabelecerem prévio diálogo e, conseqüentemente, regulamentação específica sobre o tema.

A data exata do início da vigência da LGPD em sua integralidade, porém, não é consensual. Uma divergência interpretativa levanta dúvidas sobre o termo inicial a ser considerado para contagem do prazo de 24 meses de vacância estabelecido pelo art. 65, II.

A polêmica resulta do fato de a norma ter surgido em duas etapas. A primeira delas foi a aprovação da Lei 13.709 pelo Congresso Nacional, cuja publicação no Diário Oficial da União ocorreu em 15 de agosto de 2018. Foi quando se instituiu a maior parte dos dispositivos, inclusive a previsão de um período de vacância único de 18 meses. A segunda etapa veio com a Medida Provisória 869, publicada no dia 28 de dezembro de 2018 e convertida na Lei 13.853 em 8 de julho de 2019. O texto da MP trouxe novos artigos, que criaram a Autoridade Nacional de Proteção de Dados, e alterou outros aprovados anteriormente, inclusive o art. 65, eliminando a vacância única de 18 meses e estabelecendo dois prazos:

Art. 65. Esta Lei entra em vigor:

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

²¹ Questionado formalmente para os fins deste artigo, via Ouvidoria, em 15 de outubro de 2019, o TSE não respondeu até 5 de novembro de 2019, data de entrega deste texto, se foi instalado Grupo de Trabalho dedicado a estudar eventual introdução da LGPD ao sistema da Justiça Eleitoral.

A maioria dos juristas, parlamentares, especialistas em tecnologia da informação e representantes do governo responsáveis pela estruturação da ANPD consultados ao longo desta pesquisa tratam do tema como se a LGPD encerrasse sua vacância em 15 de agosto de 2020, ou seja, 24 meses após a publicação da Lei 13.709. No entanto, há posições contrárias defendendo que a contagem do prazo foi zerada com a publicação da Medida Provisória 869, encerrando-se a vacância, portanto, somente em 29 de dezembro de 2020 (BRUNA, 2019). O fundamento jurídico para tal conclusão seria o § 3º do art. 1º da Lei de Introdução às Normas do Direito Brasileiro²², que prevê a contagem do prazo a partir da publicação das correções feitas no texto legal.

Além da questão sobre o início e o fim do período de vacância, outros fatores podem resultar em eventual postergação da aplicação integral da LGPD. Como o decreto presidencial que cuidará da estrutura regimental da ANPD ainda não foi apresentado e tampouco foram nomeados os cinco membros de seu Conselho Diretor nem designados os 23 membros do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade²³, deve ganhar força a tese daqueles que defendem uma estruturação gradativa do órgão. O trabalho inicial da ANPD teria, assim, foco na regulamentação da Lei e em iniciativas educacionais, para só depois começar o trabalho de recepção de denúncias, fiscalização e aplicação de punições (MALDONADO; BLUM, 2019, p. 398).

Ainda que se valorize a dimensão pedagógica do órgão, que terá papel relevante no desenvolvimento de uma cultura de proteção de dados pessoais no país, não há qualquer disposição legal prevendo eventual cronograma de implementação da agência, sendo mera hipótese a sua estruturação gradual. Além disso, como afirmou o próprio diretor responsável pelo tema no Ministério da Economia, José Ziebarth, a ANPD é citada 53 vezes na LGPD e a ausência dessa autoridade central ao fim da vacância traria “caos ao sistema”, aumentando a insegurança jurídica, indo de encontro ao objetivo da nova lei (RUSSO, 2019).

Essa demora do Executivo na edição do referido decreto e na instalação da ANPD é também uma das justificativas do Projeto de Lei 5762/2019, que busca estender a vacância da lei por mais dois anos (BRASIL, 2019). O texto, protocolado na Câmara dos Deputados no dia 30 de outubro de 2019, pretende alterar o inciso II do art. 65 da LGPD, estabelecendo 15

²² Art. 1º Salvo disposição contrária, a lei começa a vigorar em todo o país quarenta e cinco dias depois de oficialmente publicada. (...) § 3º Se, antes de entrar a lei em vigor, ocorrer nova publicação de seu texto, destinada a correção, o prazo deste artigo e dos parágrafos anteriores começará a correr da nova publicação.

²³ Até o dia 5 de novembro de 2019, data de entrega deste trabalho à Faculdade de Direito da Universidade Presbiteriana Mackenzie, apenas o CNMP (CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO, 2019) e a Câmara dos Deputados (CÂMARA DOS DEPUTADOS, 2019) haviam indicado seus respectivos representantes titulares e suplentes, nos termos do Art. 58-A, § 2º, da LGPD, por meio de atos normativos.

de agosto de 2022 como data para a entrada em vigor de todos os artigos da lei, exceto os citados no inciso I, que se restringem à criação da ANPD e do Conselho Nacional de Proteção de Dados e Privacidade. O início da tramitação da proposta do Deputado Carlos Bezerra, do MDB do Mato Grosso, ainda dependia, até a entrega deste trabalho²⁴, de despacho do Presidente da Câmara.

6 Considerações Finais

O impacto que a LGPD terá no pleito do próximo ano ainda conta com razoável grau de incerteza. A polêmica sobre a data exata do término da vacância da lei e a dificuldade de se prever o grau de organização e maturidade da Autoridade Nacional de Proteção de Dados em agosto de 2020 são fatores relevantes que trazem certa insegurança jurídica para candidatos que pretendam planejar suas ações de campanha.

Independentemente disso, as próximas eleições deverão ser observadas sob o prisma do uso de dados pessoais, com atenção às novas estratégias utilizadas nesse âmbito. Caso se confirme a vigência plena da lei, sua eficácia para evitar ou resolver problemas como os relatados no início deste trabalho estará sob prova.

Uma análise preliminar da Lei Geral de Proteção de Dados do ponto de vista eleitoral também permite concluir que os candidatos, provavelmente, terão de fazer adaptações substanciais às suas práticas para buscar votos em conformidade com as novas regras. Alguns dispositivos devem repercutir nas atividades mais básicas de campanha e geram dúvidas, por exemplo, sobre a possibilidade de um político manter um banco de dados ao longo de toda sua carreira, o que parece pouco razoável e indica a necessidade de regulamentações infralegais específicas, no intuito de esclarecer e adaptar a norma, evitando-se um rigor desproporcional.

Outro aspecto a ser considerado é o impacto que a restrição ao uso de dados pessoais pode ter no acesso do eleitor à propaganda durante a campanha, já que a informação plural é o principal insumo para alimentar o debate e a tomada de decisão na escolha dos candidatos.

A LGPD é mais que pertinente para o momento, em que países democráticos se questionam sobre os efeitos que o uso indiscriminado de dados pessoais provocam em processos eleitorais, como a possível manipulação dos cidadãos de forma sub-reptícia e desleal. A preocupação legítima com o direito à privacidade do indivíduo, porém, não pode se exacerbar a ponto de tirar-lhe o acesso à pluralidade de informação, isolando-o dos candidatos

²⁴ Trabalho entregue em 5 de novembro de 2019 à Faculdade de Direito da Universidade Presbiteriana Mackenzie.

justamente nos canais digitais mais propícios ao embate de ideias. Afinal, privar o eleitor do contato com a diversidade de discursos e propostas, em vez de fortalecer sua autodeterminação, pode tornar sua escolha menos esclarecida e mais restrita.

7 Referências Bibliográficas

BIONI, Bruno R. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

BRASIL. Projeto de Lei 5.762/2019. Altera a Lei 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais – LGPD – para 15 de agosto de 2022. Brasília, DF, 30 out. 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=7109E002A211FC4F07A01DDFA796B398.proposicoesWebExterno1?codteor=1828120&filename=PL+5762/2019 Acesso em: 3 nov. 2019.

BRASIL. Congresso. Câmara dos Deputados. *Ato da Presidência de 15 de outubro de 2019*. Torna pública a indicação de representantes da Câmara dos Deputados no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Diário da Câmara dos Deputados. Brasília, DF, 16 out. 2019. Disponível em: https://www2.camara.leg.br/legin/int/atopre_sn/2019/atodapresidencia-58108-15-outubro-2019-789258-publicacaooriginal-159224-cd-presi.html Acesso em: 17 out. 2019.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a lei nº 12.965, de 23 de abril de 2014 (marco civil da internet). Brasília, DF, 15 ago. 2018. Disponível em: http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2013.709-2018?OpenDocument Acesso em: 28 out. 2019.

BRASIL. Lei nº 9.504, de 30 de setembro de 1997. Estabelece normas para as eleições. Brasília, DF, 01 out. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19504.htm Acesso em: 07 set. 2019.

BRUNA, Sérgio Varella. A LINDB e a entrada em vigor da Lei de Proteção de Dados. *Jota*, São Paulo, 10 jan. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-lindb-e-a-entrada-em-vigor-da-lei-de-protecao-de-dados-10012019> Acesso em: 13 out. 2019.

CADWALLADR, Carole; HARRISON, Emma G.. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, [s.l.], 17 mar. 2018. Disponível em <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> Acesso em 8 set. 2019.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. Presidência. Portaria nº 128, de 6 de agosto de 2019. Indica os representantes do CNMP no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Brasília, DF, 6 ago. 2019. Disponível em: http://www.cnmp.mp.br/portal/images/Portarias_Presidencia_nova_versao/2019/Portaria-CNMP-PRESI.128.pdf Acesso em: 17 out. 2019.

CRUZ, Francisco Brito; *et al.* *Direito Eleitoral na Era Digital*. Belo Horizonte: Letramento, 2018.

CRUZ, Francisco Brito; MASSARO, Heloisa; BORGES, Ester. *Santinhos', memes e correntes: um estudo exploratório sobre spams recebidos por WhatsApp durante as eleições*. São Paulo: Internet Lab, 2018. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2019/04/Relat%C3%B3rio-Spam-WhatsApp.pdf> Acesso em: 27 mai. 2019.

CRUZ, Francisco Brito; SILVEIRA, Hélio Freitas de Carvalho da; ANDRADE, Marcelo Santiago de Pádua. É urgente proteger a privacidade do eleitor. *O Estado de São Paulo*, São Paulo, 26 abr. 2019. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/e-urgente-protoger-a-privacidade-do-eleitor/> Acesso em: 27 mai. 2019.

DADOS anônimos exigem legislação transparente. Entrevista com Danilo Doneda. [s.l.]: CDTV, 2016. (7 min.), color. Disponível em: <https://www.youtube.com/watch?v=FF38EeUQ2og&feature=youtu.be> Acesso em: 22 set. 2019.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJLL]*, Joaçaba, v. 12, n. 2, p. 91-108, 11. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658> Acesso em: 19 set. 2019.

DONEDA, Danilo. O que está em jogo com a nova autoridade nacional de proteção de dados. *Jota*, [s.l.], 13. ago. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-que-esta-em-jogo-com-a-nova-autoridade-nacional-de-protecao-de-dados-13082018> Acesso em: 22 set. 2019.

FERRAÇO, Ricardo. *Parecer da Comissão de Assuntos Econômicos sobre o Projeto de Lei que daria origem à LGPD*. Senado Federal, Brasília, DF, jun. 2018. Disponível em: <https://legis.senado.leg.br/sdleggetter/documento?dm=7751566&ts=1567535187796&disposition=inline> Acesso em: 14 set. 2019.

FLORES, Paulo. O que a Cambridge Analytica, que ajudou a eleger Trump, quer fazer no Brasil. *Nexo Jornal*, São Paulo, 8 dez. 2018. Disponível em: <https://www.nexojornal.com.br/expresso/2017/12/08/O-que-a-Cambridge-Analytica-que-ajudou-a-eleger-Trump-quer-fazer-no-Brasil> Acesso em: 8 set. 2019.

GOLDHILL, Olivia. A 'big data' firm sells Cambridge Analytica's methods to global politicians, documents show. *Quartz*, [s.l.], 14 ago. 2019. Disponível em: <https://qz.com/1666776/data-firm-ideia-uses-cambridge-analytica-methods-to-target-voters/> Acesso em: 19 ago. 2019.

HERN, Alex. Facebook agrees to pay fine over Cambridge Analytica scandal. *The Guardian*, [s. l.], 30 out. 2019. Disponível em: <https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal> Acesso em 3 nov. 2019.

LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2011.

MARTINES, Fernando. TSE reabre investigação sobre uso de *fake news* em massa nas eleições. *Conjur* [s.l.], 17 out. 2019. Disponível em: <https://www.conjur.com.br/2019-out-17/tse-reabre-investigacao-uso-fake-news-massa> Acesso em: 4 de nov. 2019.

MALDONADO, Viviane N.; BLUM, Renato O. (Orgs.). *LGPD: Lei Geral de Proteção de Dados Comentada*. São Paulo: Revista dos Tribunais, 2019.

MELLO, Patrícia Campos. Empresários bancam campanha contra o PT pelo WhatsApp. *Folha de São Paulo*, São Paulo, 18 out. 2018. Disponível em: <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml> Acesso em: 9 de set. 2019.

MELLOa, Patrícia Campos. Empresas contrataram disparos pró-Bolsonaro no WhatsApp, diz espanhol. *Folha de São Paulo*, São Paulo, 18. jun. 2019. Disponível em: <https://www1.folha.uol.com.br/poder/2019/06/empresas-contrataram-disparos-pro-bolsonaro-no-whatsapp-diz-espanhol.shtml> Acesso em: 9 set. 2019.

MELLOb, Patrícia Campos. WhatsApp admite envio massivo ilegal de mensagens nas eleições de 2018. *Folha de São Paulo*, Medellín, 08. out. 2019. Disponível em: <https://www1.folha.uol.com.br/poder/2019/10/whatsapp-admite-envio-massivo-ilegal-de-mensagens-nas-eleicoes-de-2018.shtml> Acesso em: 13 out. 2019.

PAIVA, Fernando. 26% dos brasileiros afirmam ter recebido spam político por WhatsApp. *Mobile Time*, [s.l.], 10 dez. 2018. Disponível em: <https://www.mobiletime.com.br/noticias/10/12/2018/26-dos-brasileiros-afirmam-ter-recebido-spam-politico-por-whatsapp/> Acesso em: 9 set. 2019.

RAIS, Diogo [Coord.]. *Direito Eleitoral Digital*. São Paulo: Revista dos Tribunais, 2018.

REBELLO, Aiuri; COSTA, Flávio; PRAZERES, Leandro. PT usou sistema de WhatsApp; campanha de Bolsonaro apagou registro de envio. *UOL*, São Paulo, 20 out. 2018. Disponível em: <https://noticias.uol.com.br/politica/eleicoes/2018/noticias/2018/10/26/bolsonaro-apagou-registro-whatsapp-pt-haddad-usou-sistema-mensagens.htm> Acesso em: 9 set. 2019.

RODRIGUES, Arthur; MELLO, Patrícia Campos. Fraude com CPF viabilizou disparo de mensagens de WhatsApp na eleição. *Folha de São Paulo*, São Paulo, 2 dez. 2018. Disponível em: <https://www1.folha.uol.com.br/poder/2018/12/fraude-com-cpf-viabilizou-disparo-de-mensagens-de-whatsapp-na-eleicao.shtml> Acesso em: 10 set. 2019.

ROSENBERG, Matthew; CONFESSORE, Nicholas; CADWALLADR, Carole. How Trump Consultants Exploited The Facebook Data of Millions. *The New York Times*, Londres, 17 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> Acesso em: 8 set. 2019.

RUSSO, Rodrigo. Brazilian data protection authority should have directors with different profiles, senior official says. *mLex Market Insight*, [s.l], 23 abr. 2019. Disponível em: <https://mlexmarketinsight.com/insights-center/editors-picks/Data-Protection-Privacy-and-Security/latin-america/brazilian-data-protection-authority-should-have-directors-with-different-profiles,-senior-official-says> Acesso em: 22 set. 2019.

STACEY, Kiran. Facebook pagará multa de US\$ 5 bi e criará comitê independente de privacidade. *Folha de S.Paulo*, São Paulo, 24 jul. 2019. Disponível em: <https://www1.folha.uol.com.br/mercado/2019/07/facebook-pagara-multa-de-us-5-bi-e-criara-comite-independente-de-privacidade.shtml> Acesso em: 8 set. 2019.

TUROLLO JR., Reynaldo. Operadoras devem informar ao TSE linhas de agências suspeitas de disparos pelo WhatsApp. *Folha de São Paulo*, Brasília, 10 out. 2019. Disponível em: <https://www1.folha.uol.com.br/poder/2019/10/operadoras-devem-informar-ao-tse-linhas-de-agencias-suspeitas-de-disparos-pelo-whatsapp.shtml> Acesso em: 13 out. 2019.