

Hackeando o Eleitorado

Sobre o uso de dados pessoais
em campanhas eleitorais



Detalhes da publicação

Editora:

Konrad-Adenauer-Stiftung e. V., 2020, Berlin

Foto da capa: © iStock/Orbon Alija

Divisor de capítulos: P. 10 © Adobe Stock/Gorodenkoff;

P. 28 © Adobe Stock/Alexander; P. 38 © Shutterstock/mrmohock

Design e composição tipográfica: yellow too, Pasiek Horntrich GbR

A versão impressa desta publicação foi impressa por:

copy print Kopie & Druck GmbH, Berlin.

Impresso na Alemanha.

Produzido com o apoio financeiro da República Federal da Alemanha.



O texto desta publicação está licenciado sob os termos da
“Creative Commons Attribution-Share Alike 4.0 international”, CC BY-SA 4.0
(disponível em: <https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>).

ISBN 978-3-95721-770-7

Hackeando o Eleitorado

Sobre o uso de dados pessoais
em campanhas eleitorais

Destaques

- › Embora a campanha eleitoral baseada em dados não seja um fenômeno novo, as ferramentas usadas, a quantidade de dados disponíveis e a capacidade potencial de influenciar os eleitores representam um cenário novo e desafiador para o Estado de Direito.
- › Com o advento da web colaborativa, o internauta passa a poder gerar dados em uma rede complexa e sem a obrigação de buscar a objetividade ou os padrões jornalísticos como pilares para a criação de conteúdo.
- › Pessoas em diferentes países procuram cada vez mais se informar e aprender sobre candidatos políticos e outras questões políticas por meio das redes sociais.
- › Nos últimos anos, partidos políticos e ativistas em todo o mundo têm feito um grande investimento em publicidade online, demonstrando todo o potencial para alcançar mais pessoas de forma eficiente, direcionada e acessível.
- › Empresas como a Cambridge Analytica reúnem grandes quantidades de dados individuais, tratam esses dados para identificar e prever detalhes individuais ainda mais íntimos e usam esses perfis e previsões para personalizar mensagens políticas, como publicidade em mídia social, para orientar decisões táticas de campanha.
- › Se os eleitores não compreenderem como seus dados estão sendo usados para influenciá-los, não poderão exercer seus direitos legais em relação a essas informações e às estratégias aplicadas.
- › As práticas atuais de tratamento de dados pessoais não autorizado estão aumentando a desinformação, assim como as “estratégias de astroturfing digital”, capazes de influenciar os cidadãos com ainda mais precisão.
- › A possibilidade de estabelecer uma ponte entre a regulamentação eleitoral e os quadros jurídicos para as atividades de campanha envolvendo dados pessoais depende de muitos fatores.
- › Esta falta de uniformidade ou má interpretação das orientações do Regulamento Geral de Proteção de Dados (RGPD) no contexto das eleições pode levar a diferenças no nível de proteção de dados pessoais nos Estados-Membros e, potencialmente, influenciar negativamente outras regiões.

- › A eficácia da regulação da proteção de dados depende da capacidade e da articulação institucional dos diferentes atores envolvidos.
- › Os regulamentos de proteção de dados são totalmente aplicáveis a campanhas eleitorais e têm a capacidade de auxiliar na redução do uso instrumental de dados pessoais, evitando também o impacto da desinformação e propaganda computacional usada para fins de manipulação política.
- › Uma abordagem de proteção de dados pode resumir estrategicamente outras iniciativas, ajudando a reduzir a desinformação nas campanhas eleitorais ao sancionar o tratamento ilegal de dados personalizados, servindo como um instrumento jurídico eficaz e útil no contexto atual.
- › Por um lado, as instituições públicas, através das suas resoluções e sanções, têm o papel de reforçar o cumprimento e a eficácia das diretrizes do RGPD. Por outro lado, é dever dos partidos políticos e ativistas cumprir os requisitos legais, tendo total responsabilidade, transparência e boa-fé no tratamento dos dados pessoais dos eleitores.
- › O tratamento não autorizado de dados pessoais, juntamente com técnicas de desinformação e uso injusto de bots, perfis, falsificações profundas e outros, mina a confiança dos eleitores e a integridade dos processos políticos e deve ser visto pelas instituições como ameaças à democracia.



Eduardo Magrani

Ph. D. em Direito e Fellow da Konrad-Adenauer-Stiftung e. V. na Alemanha, no Programa de Cooperação Europeia e Internacional para Políticas Globais de Inovação, Digitalização e Inteligência Artificial. Affiliate no Berkman Klein Center na Universidade de Harvard. Professor de Direito e Tecnologia e Propriedade Intelectual da Escola de Direito da FGV (Fundação Getúlio Vargas), IBMEC e Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) no Brasil.

Presidente do Instituto Nacional de Proteção de Dados no Brasil. Autor da Trilogia Cultura Digital no Brasil “Democracia, Hiperconectividade e Ética: uma trilogia sobre cultura digital”, sobre filosofia da tecnologia, democracia digital, proteção de dados, inovação, segurança cibernética e inteligência artificial.

Índice

Resumo	6
Introdução	7
1. Hackeando o Eleitorado	10
O efeito de câmara de eco/bolha de filtro	13
A experiência brasileira: campanha eleitoral em 2018	15
2. Conformidade dos regulamentos de proteção de dados nas eleições	28
3. Aumentar a eficácia e preencher as lacunas	38
Considerações finais	51

Resumo

A interação contínua entre dispositivos inteligentes, plataformas on-line, sensores e pessoas aponta para o crescente volume de dados sendo produzidos, armazenados e tratados, mudando cada vez mais nossa vida cotidiana em vários aspectos. O contexto da hiperconectividade pode trazer benefícios econômicos para Estado e empresas, além de conveniência para os consumidores. Por outro lado, essa nova realidade traz desafios significativos nas esferas dos processos democráticos, especialmente no contexto das campanhas eleitorais. O dano potencial que pode ser causado por estratégias de manipulação política através do uso não autorizado de dados é exponencial quando consideramos como as novas tecnologias estão sendo usadas de modo geral. Para uma ordem social cuja coesão se baseia no Estado de Direito, na soberania e no consentimento de seus cidadãos, isso representa um desafio sem precedentes e a maneira como as democracias abordarão esse desafio é um fator-chave para os sistemas políticos. As experiências dos últimos anos indicam como a tecnologia digital pode prejudicar e desestabilizar a democracia. Desinformação, manipulação algorítmica, microsegmentação comportamental e bots sociais são algumas das técnicas usadas atualmente e, na maioria das vezes, elas são baseadas em tratamento não autorizado de dados pessoais. Mais importante, esses elementos podem ser usados de maneira diferente em cada região, baseados em hábitos culturais, tecnológicos e pessoais. Considerando esse contexto, é extremamente importante que os regulamentos de privacidade e proteção de dados sejam efetivos e fortalecidos. Na União Europeia, o Regulamento Geral de Proteção de Dados (RGPD) traz uma sólida estrutura legal, que inspirou os regulamentos de muitos outros países nesse assunto. Apesar disso, há algumas diferenças entre os regulamentos de proteção de dados que devem ser destacadas com o propósito de identificar como eles podem ser reforçados e corretamente interpretados para o contexto das campanhas eleitorais. A intenção deste trabalho de pesquisa é comparar o RGPD com a Lei Geral de Proteção de Dados (LGPD) brasileira, investigando como ambos os regulamentos são aplicáveis no contexto do uso de dados pessoais em campanhas eleitorais. A justificativa para trazer o cenário brasileiro para essa análise é dupla: (i) o RGPD foi o principal pilar para a elaboração da LGPD, embora esta última tenha algumas diferenças em relação à conformidade que devem ser consideradas; e (ii) a política brasileira está passando por alguns episódios importantes de desinformação e estratégias de astroturfing digital para manipulação política que são relevantes para serem abordadas e melhor compreendidas. Por fim, este documento também oferecerá uma análise crítica da eficácia de ambos os regulamentos e sugerirá possíveis soluções.

Introdução

Partidos políticos e ativistas têm usado diferentes práticas e tecnologias de comunicação ao longo do tempo. Agora, com o rápido desenvolvimento de novas tecnologias digitais e ferramentas de comunicação, as campanhas eleitorais se tornam cada vez mais sofisticadas. Embora a campanha política baseada em dados não seja um fenômeno novo, as ferramentas utilizadas, a quantidade de dados acessíveis e a potencial capacidade de influenciar os eleitores representam um cenário novo e desafiador para o Estado de Direito.¹

A possibilidade de reunir grandes bancos de dados de cidadãos, contendo milhares de informações que fornecem a imagem completa de quem eles são, onde vivem, o que fazem e o que está acontecendo ao seu redor, pode trazer vários benefícios para partidos e ativistas políticos. Milhões de endereços de e-mail, números de telefone e outros dados pessoais, como os coletados através de doações, comícios e merchandising, permitem que os ativistas políticos obtenham informações muito confidenciais sobre grupos-alvo e eleitores específicos. Nos últimos anos, partidos políticos e ativistas de todo o mundo fizeram pesados investimentos em publicidade on-line, demonstrando todo o potencial para alcançar mais pessoas de maneira eficiente, segmentada e acessível, às vezes por uma fração do custo dos métodos mais tradicionais.²

As estratégias de publicidade e manipulação política não são novas, mas a possibilidade de atingir pessoas em detalhes tão íntimos e na escala de populações inteiras não tem precedentes.³ Isso representa um ganho em escala e eficácia.. Isso deve ser tratado com cuidado e sempre com uma base jurídica, com transparência, justiça e responsabilização. Uma possível violação do direito de proteção de dados pessoais em processos democráticos, como campanhas eleitorais, pode afetar outros direitos fundamentais consideravelmente. Isso representa uma ameaça real à capacidade dos cidadãos de tomar suas próprias decisões independentes ou até mesmo seu direito de opinião, enfraquecendo o valor fundamental da dignidade, que sustenta todos os direitos humanos. O público tem o direito de esperar que a publicidade política seja feita de acordo com a lei. Além disso, todos os partidos políticos e ativistas precisam cumprir as mesmas regras eleitorais e de proteção de dados, independentemente do método ou de novos desenvolvimentos tecnológicos.⁴

O tratamento não autorizado de dados pessoais, junto com técnicas de desinformação e astroturfing digital, prejudica a confiança dos eleitores e a integridade dos processos políticos e será considerada uma ameaça à democracia.⁵ Os cidadãos só podem fazer escolhas genuinamente informadas sobre em quem votar se estiverem seguros de que suas decisões não foram influenciadas injustamente. É por isso que a confiança na integridade dos processos democráticos não deve ser enfraquecida.^{6,7}

Levando em consideração a importância do tratamento de dados pessoais nesse contexto, parte dos potenciais abusos e riscos decorrentes do uso indevido pode ser mitigada pela aplicação de estruturas legais robustas, como os regulamentos gerais europeu e brasileiro de proteção de dados (o “RGPD” e a “LGPD”, respectivamente).

Ambos os regulamentos são aplicáveis a campanhas eleitorais e podem reduzir o uso instrumental de dados pessoais para manipulação política injusta. Combinar os regulamentos gerais de privacidade e proteção de dados com as leis eleitorais pode garantir mecanismos eficazes para assegurar direitos e deveres relacionados a dados pessoais sensíveis, ajudando a promover um ambiente saudável, legal e ético nos períodos eleitorais.⁸

Contudo, a conexão entre a regulamentação eleitoral e as estruturas legais para atividades de campanha que envolvam dados pessoais ainda está em desenvolvimento. Por mais que existam bases sólidas de ambos os lados, os regulamentos gerais de proteção de dados, como o RGPD e a LGPD, ainda não acumularam aplicação e jurisprudência significativas para garantir uma diretriz perfeitamente clara para conformidade e responsabilização. Ainda está sendo debatido como exatamente esses regulamentos devem ser aplicáveis na prática a uma série de atividades. A extensão dessa proteção às campanhas ainda é uma meta a ser atingida e está sendo substancialmente debatida por especialistas da área, tribunais e entidades de proteção de dados.⁹

A eficácia da regulamentação da proteção de dados depende da capacidade e articulação institucional das diferentes partes interessadas. As atividades relacionadas ao uso de dados pessoais em campanhas eleitorais exigirão um olhar atento não apenas das entidades públicas, como tribunais judiciais e autoridades de proteção de dados, que terão que harmonizar a interpretação e definir orientações adequadas, mas também do setor privado, para ajudar a prevenir práticas de manipulação e desinformação.¹⁰

Considerando as idiossincrasias culturais e normativas, por meio da análise dos regulamentos de proteção de dados europeu e brasileiro e seus possíveis efeitos nas campanhas eleitorais, fica evidente que é necessário que partidos, ativistas, tribunais, autoridades de proteção de dados e empresas privadas comprometam-se com a privacidade dos usuários, reagindo aos efeitos colaterais e às ameaças da tecnologia às instituições democráticas e aos direitos de seus cidadãos, nos dois contextos.

- 1 Information Commissioner's Office (ICO) (2018), "Investigation into the use of data analytics in political campaigns: a report to Parliament", <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>, acessado em setembro de 2019.
- 2 Information Commissioner's Office (ICO) (2018), "Investigation into the use of data analytics in political campaigns: a report to Parliament", <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>, acessado em setembro de 2019.
- 3 Autoridade Europeia para a Proteção de Dados (2018), "Opinion 3/2018 EDPS Opinion on online manipulation and personal data", https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf, acessado em outubro de 2019.
- 4 Leia <https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets>, acessado em outubro de 2019.
- 5 Como mostram evidências recentes, os eleitores não entendem a existência oculta do uso de dados pessoais, prejudicando o sistema da democracia através de propaganda computacional. Leia Samuel C. Woolley e Philip N. Howard (2017), "Computational Propaganda Worldwide", Universidade de Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, acessado em outubro de 2019.
- 6 ICO (2019), "Guidance on political campaigning: Draft framework code for consultation", <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>, acessado em dezembro de 2019.
- 7 Kaltheuner, Frederike (2018), "It's about human dignity and autonomy", Digital Society Blog.
- 8 A conformidade com estruturas legais relevantes, como regulamentos gerais de proteção de dados, tem efeitos sobre partidos, candidatos e consultores de marketing político, bem como sobre seus fornecedores que, juntamente com as plataformas da Internet, devem estar sujeitos a responsabilização, supervisão e sanções no caso de descumprimento legal. O veredito tradicional e específico para campanhas políticas é, na maioria dos casos, desatualizado ou ineficaz, por não refletir as práticas de campanha modernas. A importância de tratar dados pessoais em conformidade com as leis de proteção de dados durante as campanhas políticas é crucial para manter a integridade das eleições, a autonomia dos eleitores e a confiança no uso de suas informações. Leia ICO (2019), "Guidance on political campaigning: Draft framework code for consultation", <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>, acessado em dezembro de 2019.
- 9 Britto, Cruz et al. (2019), "Internet e eleições no Brasil: Diagnósticos e recomendações", InternetLab.
- 10 Britto, Cruz et al. (2019), "Internet e eleições no Brasil: Diagnósticos e recomendações", InternetLab.

The background image shows a person wearing a dark hoodie, seen from the side, working at a desk. Their hands are on a keyboard. The scene is dimly lit, with light coming from a computer screen and possibly a window in the background. Overlaid on the image is a white network diagram consisting of several nodes connected by lines. There are also four white L-shaped corner brackets in the upper left and lower left areas of the image. A large, dark teal diagonal shape with fine horizontal lines cuts across the right side of the image.

1. Hackeando o Eleitorado

**Microsegmentação, bots e desinformação
como os novos desafios à democracia**

A Federal Trade Commission (FTC) nos EUA, agência americana de proteção ao consumidor, concordou em impor uma multa recorde ao Facebook: US\$ 5 bilhões, a maior multa por privacidade na história da FTC. O acordo decorre da investigação das práticas de privacidade da empresa relacionadas ao escândalo da Cambridge Analytica (CA). O caso da CA expôs como os dados pessoais foram usados de maneira inadequada para microsegmentação (*micro-targeting*) e potencialmente manipulação de eleitores indecisos nas eleições dos EUA em 2016.¹¹

A Cambridge Analytica afirmou que tinha até 5.000 pontos de dados relacionados a cada eleitor dos EUA coletados por meio de perfis individuais, sites, mensagens no Twitter, perfis do Facebook e fotos do Instagram. Ao aplicar a 'análise psicográfica' ao seu conjunto de dados, ela alegou ser capaz de atestar o tipo de pessoa que era cada eleitor, incluindo uma avaliação relativamente precisa das necessidades e medos individuais e como eles provavelmente se comportariam.¹²

A psicometria (ou análise psicográfica) concentra-se na medição de traços psicológicos, com a intenção de avaliar os seres humanos com base em cinco características da personalidade: abertura, consciência, extroversão, amabilidade e neuroticismo. Com base nessas cinco características, é possível avaliar informações importantes e confidenciais sobre um indivíduo, que podem ser usadas para diferentes propósitos. Antes da Internet e da disseminação das redes sociais, um dos principais desafios para uma psicometria eficaz era exatamente a dificuldade de reunir todos os dados necessários, que dependiam de questionários abrangentes e altamente pessoais. Esse desafio foi superado devido às plataformas on-line e ao engajamento dos usuários nas redes sociais.¹³ Atualmente, a psicometria é amplamente utilizada para diferentes propósitos, incluindo campanhas eleitorais.

Embora existam algumas divergências sobre a eficácia das práticas da psicometria, pesquisas recentes no campo da propaganda e sociologia computacional afirmam que os perfis mentais dos indivíduos podem ser precisamente antecipados a partir das trilhas que eles deixam na web. Estudos sobre o impacto da microsegmentação na publicidade sugerem que a microsegmentação psicológica pode ser usada secretamente para atrair até 40 % mais cliques e até 50 % mais compras. As descobertas também afirmam que os profissionais de marketing podem atrair até 63 % mais cliques e até 1.400 mais conversões em campanhas publicitárias no Facebook quando combinam produtos e mensagens de marketing com as características de personalidade dos consumidores.¹⁴

Esse tipo de avaliação derivada das interações digitais reforça a importância de entender até que ponto o uso de big data e psicometria pode influenciar as atividades de grandes grupos de indivíduos.¹⁵ Esse pode não ser o único motivo para o resultado específico das eleições de 2016 nos EUA, mas existem indicações de que essa foi uma contribuição útil¹⁶, e não só nos EUA.. Mais recentemente, o Facebook concordou em pagar £ 500.000 por não impedir que organizações como a Cambridge Analytica tivessem acesso às informações pessoais dos usuários do Reino Unido (CA). O Information Commissioner's Office (ICO) declarou que o Facebook permitiu que ocorresse uma violação e não tomou medidas suficientes para impedir que aplicativos coletassem dados em violação à lei de proteção de dados.^{17 18}

De acordo com o ICO:¹⁹

Nossa investigação descobriu que, entre 2007 e 2014, o Facebook processou de forma desleal as informações pessoais dos usuários, permitindo que desenvolvedores de aplicativos acessassem suas informações, sem o consentimento suficientemente claro e informado, e possibilitando o acesso mesmo que os usuários não tivessem baixado o aplicativo, mas fossem simplesmente “amigos” de pessoas que o baixaram. O Facebook também falhou em manter as informações pessoais seguras, porque não verificou adequadamente os aplicativos e desenvolvedores que usam sua plataforma.

Além da notoriedade do escândalo da CA e seus desdobramentos nos EUA e no Reino Unido, ao analisar a economia de big data baseada na Internet e os usos políticos, a conclusão é que esse fenômeno não se trata de apenas uma empresa nem se restringe a episódios excepcionais em regiões específicas. Estudos recentes mostraram evidências de que isso está acontecendo em todo o mundo, onde dados pessoais não autorizados são massivamente tratados por empresas, partidos e ativistas que buscam manipulação comportamental, com capacidade de influenciar injustamente os resultados das eleições usando mensagens individualizadas de alto impacto. Além disso, essa prática está se tornando ainda mais eficaz e manipuladora com o uso de técnicas de desinformação e astroturfing digital.

De acordo com o Comitê Europeu de Proteção de Dados:²⁰

*Partidos políticos, coalizões e candidatos dependem cada vez mais de dados pessoais e técnicas sofisticadas de definição de perfis para monitorar e segmentar eleitores e formadores de opinião. Na prática, os indivíduos recebem mensagens e informações altamente personalizadas, especialmente nas plataformas de mídia social, com base em interesses pessoais, hábitos de vida e valores. São usadas ferramentas preditivas para classificação ou definição de perfis de traços de personalidade, características, humor e outros pontos de influência em ampla escala, permitindo que sejam feitas suposições sobre traços de personalidade profundos, incluindo visões políticas e outras categorias especiais de dados. A extensão dessas técnicas de tratamento de dados para propósitos políticos apresenta sérios riscos, não apenas aos direitos à privacidade e à proteção de dados, mas também à confiança na integridade do processo democrático.*²¹

Apesar do aumento dos esforços das plataformas web²² para combater esses efeitos²³, de acordo com o novo relatório de Oxford, o uso dessas técnicas por governos de todo o mundo está crescendo e as estratégias não estão mais limitadas aos grandes países. Estados menores também podem facilmente configurar operações na Internet, usando não apenas informações pessoais, mas combinando isso com o potencial de bots²⁴, desinformação segmentada, perfis falsos e “trolls” contratados.

Pesquisadores do Oxford Internet Institute construíram uma análise de propaganda computacional baseada em casos²⁵ para melhor entender seu alcance global. Foi descoberto que nos últimos dois anos, o número de países com campanhas de desinformação política mais do que dobrou, chegando a 70, com evidências de pelo menos um partido político ou entidade governamental envolvido na manipulação de mídias sociais em cada um desses países. O Fórum Econômico Mundial listou recentemente

a disseminação de desinformação on-line entre os 10 principais perigos para a sociedade. A pesquisa descobriu que as mídias sociais favorecem o conteúdo sensacionalista, independentemente de ter sido verificado se o conteúdo é factual ou proveniente de uma fonte confiável.²⁶

Pesquisadores de Oxford disseram que os governos estão cada vez mais optando pelas mídias sociais para restringir os direitos humanos, prejudicar oponentes políticos e reprimir a dissidência, inclusive em países como Azerbaijão, Zimbábue e Bahrein. O relatório também afirma que no Tajiquistão, estudantes universitários foram recrutados para criar contas falsas e compartilhar pontos de vista pró-governo.^{27 28 29 30} Através da combinação de notícias reais com desinformação e conteúdo de Internet sem restrições, os eleitores-alvo encontram mensagens em muitas páginas que reforçam suas perspectivas sem saberem que são algumas das poucas pessoas no mundo que recebem essas mensagens e sem terem noção de que são alvo de campanhas eleitorais.^{31 32 33}

Os pesquisadores concluíram que a maioria dos esforços de desinformação vinculados ao governo estavam focados no mercado interno, mas pelo menos sete países estão tentando influenciar opiniões fora de suas fronteiras: China, Índia, Irã, Paquistão, Rússia, Arábia Saudita e Venezuela. Os anúncios políticos visavam criar imagens, vídeos ou outras peças de conteúdo desenvolvidos para tirar proveito dos algoritmos das redes sociais e de seu poder amplificador, aproveitando o potencial viral de cada plataforma.^{34 35}

Os recortes informativos e algorítmicos das plataformas da Internet frequentemente carecem de suficiente transparência, o que dá aos consumidores uma falsa ideia de que as informações têm um fluxo neutro e livre. Mas, em alguns casos, os usuários estão interagindo em bolhas de filtro, olhando para uma realidade digital fornecida por filtragem algorítmica adaptada especificamente a eles, considerando suas necessidades, desejos, medos e fraquezas com base em seus dados pessoais. A filtragem de algoritmos em ambientes on-line permite um grau de personalização e segmentação em uma escala muito maior. Isso tende a acelerar com o aumento do cenário da Internet das Coisas, uma vez que, com mais e mais dispositivos inteligentes conectados ao nosso redor, teremos dados ainda mais pessoais sendo coletados, armazenados, tratados e transferidos.^{36 37}

O efeito de câmara de eco/bolha de filtro

O chamado efeito de câmara de eco/bolha de filtro³⁸ está relacionado a um conjunto definido de dados produzidos por todos os mecanismos algorítmicos usados para criar uma edição invisível voltada para a personalização da navegação on-line.³⁹ É a personalização de conteúdo feita por plataformas/aplicativos da Internet para aprimorar a experiência dos usuários e a receita de anúncios de suas empresas.⁴⁰

A filtragem surgiu como uma necessidade e frequentemente é considerada bem-vinda, gerando um grande conforto para o usuário, que, na maioria dos casos, encontra de maneira rápida e eficiente as informações ou qualquer outro conteúdo que deseja acessar. Esse é o modelo de negócios da Netflix, por exemplo, que per-

mite ao usuário ter uma coleção de filmes com base apenas em seu perfil por meio da sugestão de títulos e filtros personalizados, a fim de melhorar sua experiência. O mesmo argumento de conveniência e aprimoramento de experiência pode ser aplicado ao mecanismo de busca do Google, à linha do tempo do Facebook, ao Instagram, ao LinkedIn, à Amazon e a muitas outras plataformas e aplicativos em que o modelo de negócios se baseia em anúncios, microssegmentação e definição de perfis de usuários.⁴¹

Para além da conveniência e da experiência do usuário, o problema está na forma e no excesso de filtragem, tanto por empresas quanto pelos próprios indivíduos, que, inconscientemente, se restringem e se afastam de perspectivas contraditórias, empobrecendo o valor do debate na esfera pública virtual⁴². Consequentemente, as bolhas de filtro podem limitar os usuários a uma previsão algorítmica que fornece apenas conteúdo específico segmentado com base no tratamento de dados pessoais.⁴³ Isso cria um problema de acesso às informações que deveriam ser vistas para enriquecer o debate democrático.⁴⁴ De outra perspectiva, atualmente, o usuário da Internet, quando navega pelos sites mais conhecidos, é alvo de uma enxurrada de publicidade segmentada que dá significado ao interesse comercial por trás desse mecanismo de filtragem e personalização.⁴⁵

Transformar as plataformas digitais em espaços de realidade personalizada pode criar câmaras de eco e bolhas de filtro, isolando as pessoas daquilo que elas eventualmente precisam ver. Esse efeito pode ser percebido como prejudicial ao debate e à formação de consenso na esfera pública conectada, pois pode restringir o acesso à informação e também a autonomia dos indivíduos, potencialmente aumentando a polarização e a radicalização dos discursos.^{46 47 48}

Há, contudo, divergências quanto ao efeito real que as bolhas de filtro e as câmaras de eco⁴⁹ representam hoje nas plataformas sociais e também no contexto político. É preciso evitar uma generalização imprecisa para permitir uma análise mais complexa.⁵⁰ Como afirma Simon Hegelich, os usuários não estão de fato em uma “bolha”:⁵¹ “Eles estão, na verdade, comunicando tópicos diferentes em várias redes e decidindo quando discutir ideias que vão além de seus próprios limites ideológicos.” No entanto, como Hegelich colocou, “embora todo usuário, em princípio, tenha a opção de procurar a fonte original da informação e consumir informações imparciais, isso, mais uma vez, exige uma mudança para a lógica racional. A arquitetura das redes sociais não impede que isso aconteça, mas o Facebook, o Twitter, etc. são projetados para trocas privadas entre amigos, onde, por princípio, a homofilia é bem-vinda (...)”.⁵²

Portanto, apesar de ainda haver divergências⁵³ quanto ao impacto das câmaras de eco e bolhas de filtro, bem como suas variações em diferentes países e contextos sociotécnicos, sua existência e importância são bem destacadas por muitos estudiosos e pesquisadores. Embora as evidências empíricas ainda estejam sendo consolidadas para dar suporte a preocupações mais fortes sobre bolhas de filtro, à medida que a tecnologia de personalização melhora⁵⁴ e o conteúdo de notícias personalizadas se torna a principal fonte de informações das pessoas, podem surgir problemas para nossa democracia.⁵⁵

De acordo com Michela Del Vicario et. Al.:⁵⁶

Os usuários tendem a se agregar em comunidades de interesses comuns, o que causa reforço e promove viés de confirmação, segregação e polarização. Isso ocorre às custas da qualidade das informações e leva à proliferação de narrativas tendenciosas fomentadas por boatos, desconfiança e paranoia sem fundamento. De acordo com essas configurações, as soluções algorítmicas não parecem ser as melhores opções para quebrar essa simetria.

De acordo com Dr. Judith Moeller, Prof. Dr. Natali Helberger⁵⁷

Não se pode negar que, como resultado da proliferação de práticas de definição de perfis e segmentação, a forma como as notícias são distribuídas e consumidas mudou profundamente. Um número crescente de usuários (também) consome conteúdo de notícias por meio de grandes plataformas ou intermediários de informação altamente personalizados, plataformas que não compartilham o espírito editorial e o compromisso com a diversidade aos quais os meios de comunicação tradicionais e de qualidade aderem. Particularmente, as partes da população para as quais essas plataformas são os principais portais de informações correm o risco de, se não acabarem em bolhas de filtro, terem somente acesso limitado, fortemente filtrado e com potencial tendência para fontes de notícias populares (principalmente EUA e Reino Unido). Além disso, a multiplicação de conteúdo informativo e fontes on-line cria a necessidade de novas maneiras de selecionar e filtrar o conteúdo de notícias.

À luz do exposto, a ideia de que a infraestrutura da Internet, como esfera pública, tem o potencial de permitir que as discussões sejam fortes o suficiente para atingir diferentes segmentos e grupos de interesse, replicando através das várias redes de pessoas que compõem a sociedade, pode ser uma realidade cada vez mais distante.⁵⁸ Isso se deve ao fato de que as expressões podem ser frequentemente restritas a redes de pessoas com interesses comuns e canais de comunicação projetados pelos titulares da plataforma para reforçar esse efeito.⁵⁹ A consequência disso tem o potencial de levar a uma fragmentação e polarização do debate público⁶⁰, criando um terreno mais fértil para a manipulação política.⁶¹

A experiência brasileira: campanha eleitoral em 2018

Semelhante à campanha de Donald Trump em 2016, a campanha eleitoral brasileira de 2018 no Brasil também revelou que foram enviadas mensagens em massa através de plataformas de mídia social para influenciar o eleitorado.⁶² A manipulação política através de desinformação, manipulação algorítmica, microsegmentação comportamental e bots sociais⁶³ tem sido amplamente usada e baseada principalmente no tratamento não autorizado de dados pessoais, aproveitando também as idiossincrasias nacionais e aspectos culturais.

O Brasil é o maior país da América Latina, com uma população de aproximadamente 208 milhões de pessoas. Embora 66 % dos brasileiros tenham acesso à Internet, 49 % acessam a Internet apenas por telefones móveis.⁶⁴ De acordo com uma pesquisa rea-

lizada pela Consumer Watch, o principal motivo para os brasileiros acessarem a Internet é o uso de redes sociais.. O Brasil é um dos países que mais utiliza plataformas sociais. 39 % dos internautas nacionais acessam suas redes sociais mais de 10 vezes por dia, estando on-line em média cinco horas por dia, navegando principalmente nas redes sociais.⁶⁵

Enquanto o Facebook e o Twitter foram massivamente usados na campanha eleitoral dos EUA, no Brasil, foi o WhatsApp que teve um papel importante.⁶⁶ O WhatsApp se tornou uma das armas mais importantes para propaganda e desinformação computacional no cenário político brasileiro. A facilitação do acesso à plataforma por meio de práticas de zero-rating impulsionou a taxa de penetração de usuários do WhatsApp no país. O Facebook foi o primeiro aplicativo a driblar as regras de neutralidade⁶⁷ da rede no Brasil e hoje o WhatsApp é o aplicativo de bate-papo mais usado no Brasil (120 milhões de usuários).⁶⁸

Apesar de pertencer ao mesmo grupo econômico do Facebook, o WhatsApp traz uma nova camada de desafios. Ele tem um papel diferente como plataforma de mensagens instantâneas e suas mensagens apresentam criptografia de ponta a ponta. Portanto, embora garanta melhor proteção à privacidade e aos dados pessoais do usuário, ao mesmo tempo também é mais difícil investigar e moderar o conteúdo, pois nem mesmo a própria empresa tem acesso direto ao conteúdo das mensagens (*a priori*).⁶⁹ A complexidade da plataforma tornou ainda mais difícil a sinalização de conteúdo eleitoral em massa ou até mesmo a garantia aos candidatos de que a plataforma não fosse usada para fins ilícitos, como publicidade política injusta, propagação de discurso de ódio ou fatos falsos disseminados por processos automatizados.⁷⁰

Embora o WhatsApp não permita publicidade, as empresas de marketing oferecem serviços de campanha política exclusivamente para o aplicativo de mensagens. Investigações em andamento no Brasil mostram que empresas terceirizadas, dedicadas a campanhas de marketing político, agiram na última campanha eleitoral no Brasil, segmentando grupos com o propósito de manipulação política, não apenas desrespeitando os termos de uso da plataforma, através de suas técnicas de mensagens em massa para espalhar desinformação (o que é proibido pela plataforma), mas também usando bancos de dados não autorizados, desrespeitando as práticas recomendadas de proteção de dados.⁷¹ Como prática comum, elas coletam dados dos eleitores, como números de telefone em eventos e a partir daí constroem listas de transmissão que podem chegar a 20.000 usuários para enviar uma média de 10 mensagens por dia para cada usuário no aplicativo de mensagens.⁷²

Com base nos padrões do RGPD, as possibilidades de qualquer tratamento de dados pessoais, mesmo quando baseadas em “dados pessoais disponíveis ao público” e usadas no contexto eleitoral, devem ser cuidadosamente abordadas, levando em consideração o que ocorreu em situações específicas, como o caso da CA mencionado acima. Embora possa haver isenções de consentimento, em muitos casos, o tratamento pode ser considerado ilegal por não serem adotadas etapas fundamentais de conformidade, como informar o titular dos dados sobre o tratamento e garantir princípios e direitos básicos de proteção de dados.^{73 74 75 76}

Em outubro de 2019, pela primeira vez, o WhatsApp admitiu o envio de mensagens em massa em sua plataforma, com sistemas automatizados (bots)⁷⁷ contratados por empresas, durante a última campanha eleitoral no Brasil. O reconhecimento foi feito pelo oficial de Políticas Públicas da plataforma de mensagens, Ben Supple, que explicou que houve uma “violação dos termos de uso”, que proíbem a automação e o envio massivo de conteúdo.⁷⁸ No entanto, um ano antes, em outubro de 2018, um jornal brasileiro⁷⁹ já havia revelado que empresas de marketing foram contratadas para enviar mensagens políticas em massa contendo, também, conteúdo de⁸⁰ desinformação.⁸¹ A estratégia tornou-se pública quando a imprensa divulgou que havia contratos de cerca de R\$ 12 milhões para envio de mensagens em massa e também compra de bancos de dados de terceiros. Nomes, datas de nascimento e números de identificação de idosos nacionais e estrangeiros também foram usados para registrar chips de celular sem o consentimento deles, com o propósito de gerar mensagens em massa no WhatsApp a partir desses números e segmentar destinatários com base em sua renda e região geográfica.⁸²

O crescimento das ações conduzidas por robôs é um perigo real para o debate público, representando riscos para a própria democracia, interferindo no processo de construção de consenso na esfera pública e na escolha de representantes e agendas do governo.⁸³ Confirmando a tese de risco para a democracia, a Diretoria de Análise de Políticas Públicas (DAPP) da FGV (Fundação Getúlio Vargas) divulgou interferência ilegítima no debate on-line durante⁸⁴ as eleições⁸⁵ de 2018 e nos debates públicos em geral.⁸⁶ As contas programadas para publicações em massa tornaram-se uma ferramenta para manipular os debates nas mídias sociais. No decorrer da corrida eleitoral de 2018, as contas automatizadas foram responsáveis por 12,9 % das interações no Twitter.^{87 88 89 90}

Um ex-funcionário de uma das empresas (Yacows) que coordenou o processo de mensagens afirmou ter usado uma lista com informações de dez mil pessoas para acessar ilegalmente seus dados pessoais para enviar as mensagens, com a intenção de burlar a filtragem de números em vigor no WhatsApp. O uso de robôs também foi declarado, com a confissão de que, para cada 50 mensagens, houve uma pausa de 10 segundos para também tentar burlar o bloqueio do WhatsApp.^{91 92} Até 300.000 contas do WhatsApp podem ter sido usadas para automatizar transmissões de desinformação e coordenar publicidade política não relatada para milhares de grupos do WhatsApp.^{93 94 95 96}

Devido às divulgações da imprensa, as investigações estão examinando o envolvimento de políticos, partidos e apoiadores no que diz respeito à desinformação e manipulação política. As investigações estão expondo fatos e depoimentos importantes. Ao mesmo tempo, elas revelam as circunstâncias complexas que o sistema judicial, em especial, enfrenta na luta contra a má conduta nas campanhas digitais.^{97 98 99 100}

101 102

O novo modelo de campanha orientada a dados apresenta um desafio sistêmico e institucional que não pode ser resolvido rapidamente e precisa de uma combinação de abordagens políticas e regulamentares. Uma proteção mais forte dos dados é certamente parte da resposta¹⁰³: fazer cumprir adequadamente o Regulamento

Geral de Proteção de Dados da Europa, que tem alcance internacional, e usá-lo como modelo em outros países pode ajudar a reduzir a extensão da mineração de dados e definição de perfis usada para manipulação política.¹⁰⁴ Nas palavras de Iva Nenadić, “a eficiência da segmentação on-line depende muito de dados e definição de perfis. Portanto, se efetivamente implementado, o RGPD deve ser útil aqui, impedindo o tratamento ilegal de dados pessoais”.¹⁰⁵

De acordo com a Organização Internacional de Privacidade:¹⁰⁶

Onde os dados são gerados, os indivíduos deveriam poder saber quais empresas possuem quais tipos de dados a seu respeito. A definição de perfis gera inferências e previsões altamente confidenciais sobre a personalidade, comportamento ou crenças das pessoas. (...) As empresas que acumularam anos de dados sensíveis de bilhões de pessoas em todo o mundo podem mudar o comportamento real das pessoas em ampla escala. (...) Os indivíduos devem poder acessar essas inferências e previsões a seu respeito para desafiá-los efetivamente ou solicitar que os perfis sejam excluídos.

Os dados pessoais são essenciais para este debate. Repetindo as palavras de Linda Risso:¹⁰⁷ “Está claro que os legisladores estão atrasados e que há uma lacuna cada vez maior entre o status atual da tecnologia e o foco da lei.”¹⁰⁸ Portanto, é crucial que os governos nacionais se familiarizem rapidamente com os desafios éticos e legais impostos pelas mídias sociais, propaganda computacional e proteção de dados.¹⁰⁹ Desde 2017, as regras de proteção de dados da UE significam que os dados pessoais só podem ser tratados em determinadas situações e sob certas condições. No entanto, a questão de como isso funcionará na prática permanece em aberto.”^{110 111 112 113}

11 “A mais importante fonte de dados foi o Facebook. Por meio de um aplicativo de terceiros, a Cambridge Analytica obteve indevidamente dados de até 87 milhões de perfis do Facebook – incluindo atualizações de status, curtidas e até mensagens privadas, e microsegmentou mensagens individualmente para influenciar o seu comportamento”. Westby, Joe (2019), “The Great Hack: Cambridge Analytica is just the tip of the iceberg”, Amnesty Tech, <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>, acessado em janeiro de 2020.

12 De acordo com Christopher Wylie, um dos cofundadores e denunciantes da Cambridge Analytica: “Exploramos o Facebook para coletar perfis de milhões de pessoas e construímos modelos para explorar o que sabíamos sobre elas e segmentar seus demônios internos.” Leia <https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting>, acessado em janeiro de 2020.

13 “O fato de não possuir uma conta no Facebook não forneceu proteção – a diversidade de fontes de dados disponíveis não se limita ao Facebook e a análise pode ser aplicada facilmente a outros pontos de preferência pessoal. Além disso, todos os sites com o logotipo do Facebook estão vinculados ao Facebook, permitindo o rastreamento de membros e não membros que podem não ter optado pelo serviço. Há muitas fontes semelhantes de rastreamento on-line (*web beacons*, por exemplo), a maioria ligada a “cookies” que podem ser usados em sites e o acesso pode ser vendido a compradores interessados.” Isaak; Mina J. Hanna (2018), “User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection”, IEEE Computer Volume: 51 Edição: 8, <https://ieeexplore.ieee.org/abstract/document/8436400>, acessado em agosto de 2018.

14 Grassegger, Hannes e Krogerus, Mikael (2017), “The Data That Turned the World Upside Down”, Motherboard, https://www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win, acessado em outubro de 2019.

15 S. C. Matz, M. Kosinski, G. Nave, D. J. Stillwell (2017), “Psychological targeting in digital mass persuasion”, National Academy of Sciences, Leia também Moon, Y. (2016), “Personalization and personality: Some effects of customizing message style based on consumer personality”, Journal of Consumer Psychology, Elsevier.

- 16 Devido aos muitos fatores envolvidos no processo de manipulação política, de fatores culturais a tecnológicos e psicológicos/idiossincráticos, ainda é difícil atestar com absoluta certeza exatamente como isso aconteceu e quantas pessoas foram manipuladas por essas técnicas. A pesquisa empírica que examina processos e resultados especificamente de comunicação on-line ainda é escassa.
- 17 Youyou, Wu et al. (2015), "Computer-based personality judgments are more accurate than those made by humans", PNAS. <https://www.bbc.com/news/technology-45976300>, acessado em outubro de 2019.
- 18 Information Commissioner's Office (ICO) (2018), "Investigation into the use of data analytics in political campaigns: a report to Parliament", <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>, acessado em setembro de 2019.
- 19 Information Commissioner's Office (ICO) (2018), "Investigation into the use of data analytics in political campaigns: a report to Parliament", <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>, acessado em setembro de 2019.
- 20 Comitê Europeu de Proteção de Dados (2019), "Declaração 2/2019 relativa à utilização de dados pessoais no decurso das campanhas políticas", https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_pt.pdf, acessado em janeiro de 2020.
- 21 O Conselho Europeu adotou um conjunto de políticas exigindo que os partidos políticos cumpram as regras de proteção de dados da UE. Conselho Europeu (2019), "Eleições para o PE: UE adota novas regras para impedir a utilização abusiva de dados pessoais pelos partidos políticos europeus", <https://www.consilium.europa.eu/pt/press/press-releases/2019/03/19/ep-elections-eu-adopts-new-rules-to-prevent-misuse-of-personal-data-by-european-political-parties/>, Em: Chester, J. e Montgomery, K. C. (2019), "The digital commercialization of US politics – 2020 and beyond", Internet Policy Review, 8(4).
- 22 O WhatsApp, por exemplo, limitou o número de membros de cada grupo a 256 e o número de encaminhamento de mensagens a cinco por vez. O WhatsApp também implementou a necessidade de autorização para inclusão em um grupo específico do WhatsApp e excluiu quase 1,5 milhão de contas nas últimas eleições brasileiras que, de certa forma, estavam envolvidas na automatização de conteúdo ou em qualquer outra prática imprópria. O Google deixará de dar aos anunciantes a capacidade de segmentar anúncios eleitorais usando dados como registros de eleitores públicos e afiliações políticas em geral. O Facebook, por sua vez, afirmou que removerá os *deepfakes*. O Twitter decidiu em outubro que simplesmente não aceitaria mais propaganda política. Em novembro, o Google determinou que quem quisesse contratar publicidade política nos Estados Unidos (inclusive no YouTube) não seria mais capaz de segmentar a publicação para usuários filtrados por preferência ideológica. Leia <https://piaui.folha.uol.com.br/materia/o-algoritmo-da-agera/>. Leia <https://www.zdnet.com/article/whatsapp-banned-nearly-half-a-million-accounts-during-brazilian-elections/>. Leia <https://faq.whatsapp.com/en/30046788/?lang=en>. Leia <https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKBN1XU2WT>. Leia https://link.estadao.com.br/noticias/empresas,facebook-passara-a-remover-videos-falsos-e-deep-fakes-da-rede-social,70003146938?utm_source=facebook:newsfeed&utm_medium=social-organic&utm_campaign=redes-sociais:012020:e&utm_content=:&utm_term=, acessado em fevereiro de 2020.
- 23 Nesse contexto, uma questão que não deve ser negligenciada é a importância do trabalho educacional e de treinamento sobre o fenômeno da desinformação on-line. De acordo com uma pesquisa realizada pela empresa Kaspersky, que se aprofundou na compreensão de como a América Latina lida com *fake news* (notícias falsas): Em média, 70 % dos latino-americanos não sabem identificar ou não têm certeza se são capazes de diferenciar se as notícias na internet são falsas ou verdadeiras. Por nacionalidade, os cidadãos menos capazes de reconhecer notícias falsas são peruanos (79 %), seguidos por colombianos (73 %) e chilenos (70 %). Mais atrás, estão argentinos e mexicanos, com 66 %, e depois brasileiros (62 %). Leia <https://veja.abril.com.br/tecnologia/62-dos-brasileiros-nao-sabem-reconhecer-uma-noticia-falsa/>. Leia https://amp/?_twitter_impression=true&fbclid=IwAR0hLFm_NOTv61xTWYDazqY4OI_Uf_HFUCnlkqyDjF6A1zJwNd-fGIUGM8gE, acessado em fevereiro de 2020.
- 24 "Bots, os programas automatizados essenciais à propagação de propaganda computacional, são softwares destinados a executar tarefas simples, repetitivas e robóticas. Eles são usados para melhorar computacionalmente a capacidade dos seres humanos de realizar trabalhos on-line. Os bots de mídia social são identidades automatizadas que podem executar tarefas mundanas, como coletar informações, mas também podem se comunicar com pessoas e sistemas. Eles são implantados para executar tarefas legítimas, como fornecer notícias e informações. Eles também são usados para atividades mais maliciosas associadas a spam e assédio. Sejam quais forem seus usos, eles são capazes de implantar mensagens, interagir com o conteúdo de outros usuários e afetar algoritmos de tendências rapidamente enquanto se passam por usuários humanos. Bots políticos, bots de mídia social usados para manipulação política, também são ferramentas eficazes para fortalecer a propaganda on-line e campanhas de ódio. Uma pessoa, ou um pequeno grupo de pessoas, pode usar um exército de bots políticos no Twitter para dar a ilusão de um consenso em larga escala." Woolley, Samuel e Howard, Philip (2017), "Computational Propaganda Worldwide", Universidade de Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, acessado em fevereiro de 2020.

- 25 Woolley, Samuel e Howard, Philip (2017), "Computational Propaganda Worldwide", Universidade de Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-Executive-Summary.pdf>, acessado em fevereiro de 2020.
- 26 Woolley, Samuel e Howard, Philip (2017), "Computational Propaganda Worldwide", Universidade de Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-Executive-Summary.pdf>, acessado em fevereiro de 2020.
- 27 "Governos e partidos estão usando 'tropas cibernéticas' para moldar a opinião pública, incluindo redes de bots para ampliar mensagens, grupos de 'trolls' para assediar dissidentes políticos, como jornalistas e ativistas, e contas falsas nas redes sociais para deturpar o número de pessoas envolvidas em uma questão. Os governos estão espalhando desinformação a fim de desacreditar os oponentes políticos, ocultar pontos de vista opostos e até intervir em assuntos externos". Alba, D. e Satariano, A. (2019), "At Least 70 Countries Have Had Disinformation Campaigns", NY Times.
- 28 "Por fim, se esses recursos são tão poderosos quanto as empresas e seus clientes afirmam, eles representam uma ameaça real à nossa capacidade de tomar nossas próprias decisões autônomas ou mesmo ao nosso direito à opinião, prejudicando o valor fundamental da dignidade que sustenta todos os direitos humanos. Publicidade e propaganda não são novidade, mas a segmentação de indivíduos em um nível tão íntimo e na escala de populações inteiras é sem precedentes." Westby, Joe (2019), "The Great Hack: Cambridge Analytica is just the tip of the iceberg, Amnesty Tech, <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>, acessado em janeiro de 2020.
- 29 Isaak; Mina J. Hanna (2018), "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection", IEEE Computer Volume: 51 Edição: 8, <https://ieeexplore.ieee.org/abstract/document/8436400>, acessado em agosto de 2018.
- 30 Woolley, Samuel e Howard, Philip (2017), "Computational Propaganda Worldwide", Universidade de Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-Executive-Summary.pdf>, acessado em fevereiro de 2020.
- 31 Risso, Linda (2017), "Harvesting Your Soul? Cambridge Analytica and Brexit", Akademie der Wissenschaften und der Literatur, http://www.adwmainz.de/fileadmin/user_upload/Brexit-Symposium_Online-Version.pdf#page=75, acessado em dezembro de 2019. Leia também Samuel C. Woolley e Philip N. Howard (2017), "Computational Propaganda Worldwide", Universidade de Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>, acessado em outubro de 2019. Leia também Funke D. e Flamini, D. (2019), "A guide to anti-misinformation actions around the world", <https://www.poynter.org/ifcn/anti-misinformation-actions/>, acessado em dezembro de 2019.
- 32 Bradshaw, S. Howard, P. (2019), "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation", Universidade de Oxford, <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf>, acessado em dezembro de 2019.
- 33 Funke D. e Flamini, D. (2019), "A guide to anti-misinformation actions around the world", <https://www.poynter.org/ifcn/anti-misinformation-actions/>, acessado em dezembro de 2019.
- 34 Alba, D. e Satariano, A. (2019), "At Least 70 Countries Have Had Disinformation Campaigns", NY Times.
- 35 Samuel C. Woolley e Philip N. Howard (2017), "Computational Propaganda Worldwide", Universidade de Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-Executive-Summary.pdf>, acessado em outubro de 2019.
- 36 Bayer, J. et al. (2019), "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States". Parlamento Europeu, [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf), acessado em fevereiro de 2020.
- 37 Anderson, J. e Rainie, L. (2017), "The Future of Truth and Misinformation Online", Pew Research Center, [web/imagining/surveys/2017_survey/Future_of_Info_Environment_Elon_University_Pew_10-18-17.pdf](http://www.pewresearch.org/fact-tank/2017/07/10/the-future-of-truth-and-misinformation-online/), acessado em fevereiro de 2020.
- 38 Pariser, E. (2011), "The Filter Bubble: What the Internet is Hiding from You", Penguin Press.
- 39 Magrani, Eduardo (2014), "Democracia Conectada", Jurua, <https://bibliotecadigital.fgv.br/dspace/bits-tream/handle/10438/14106/Democracia%20conectada.pdf?sequence=1&isAllowed=y>, acessado em setembro de 2019.
- 40 "Em poucas palavras, cookies são dados de acesso que consistem nas 'pegadas digitais' deixadas ao passar e se manifestar em ambientes on-line". Wu, Tim (2011), "The Master Switch: The Rise and Fall of Information Empire", Vintage.
- 41 Magrani, Eduardo e Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018", Cyber law.
- 42 Magrani, Eduardo (2014), "Democracia Conectada", Jurua, <https://bibliotecadigital.fgv.br/dspace/bits-tream/handle/10438/14106/Democracia%20conectada.pdf?sequence=1&isAllowed=y>, acessado em setembro de 2019.
- 43 Morozov, E. (2013), "To Save Everything, Click Here: The Folly of Technological Solutionism", Public Affairs.
- 44 Borgesius, Z. et al. (2016), "Should we worry about filter bubbles?", Internet Policy Review, 5(1).

- 45 Magrani, Eduardo e Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018", *Cyber law*.
- 46 Uma declaração decisiva nesse sentido exigiria um estudo mais aprofundado, de modo que a abordagem específica desse ponto iria além dos limites deste estudo.
- 47 "Muitas pessoas sequer sabem que bolhas de filtro existem. Mais de 60 % dos usuários do Facebook desconhecem totalmente qualquer curadoria no Facebook, acreditando, em vez disso, que todas as histórias de seus amigos e páginas seguidas apareceram no feed de notícias." Hern, A. (2017), "How social media filter bubbles and algorithms influence the election." *The Guardian*. <https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles>, acessado em outubro de 2019.
- 48 Allred, K. (2018), "The Causes and Effects of 'Filter Bubbles' and how to Break Free", *Medium*, <https://medium.com/@10797952/the-causes-and-effects-of-filter-bubbles-and-how-to-break-free-df6c-5cbf919f>, acessado em outubro de 2019.
- 49 Os conceitos divergentes em torno de ambos os termos também dificultam esse debate. Leia Bruns, A. (2019), "Filter Bubbles and Echo Chambers: Debunking the Myths", *Medium*, <https://medium.com/dmrc-at-large/are-filter-bubbles-real-3be22bd9230e>, acessado em outubro de 2019. Leia também Moeller, J. e Helberger, N. (2018), "Beyond the filter bubble: Concepts, myths, evidence, and issues for future debates", Universidade de Amsterdã, https://www.ivir.nl/publicaties/download/Beyond_the_filter_bubble_concepts_myths_evidence_and_issues_for_future_debates.pdf, acessado em outubro de 2019.
- 50 Bruns, A. (2019), "Are Filter Bubbles Real?", *Digital future series*.
- 51 Hegelich, S. e Shahrezaye, M. (2017), "Disruptions to political opinion: Political debate in the age of echo chambers and filter bubbles", *KAS Facts and Findings* n 253, https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_49188_2.pdf/d3741812-3abb-c52a-fe75-658665e274d7?version=1.0&t=1539649011639, acessado em outubro de 2019.
- 52 Hegelich, S. e Shahrezaye, M. (2017), "Disruptions to political opinion: Political debate in the age of echo chambers and filter bubbles", *KAS Facts and Findings* n 253, https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_49188_2.pdf/d3741812-3abb-c52a-fe75-658665e274d7?version=1.0&t=1539649011639, acessado em outubro de 2019.
- 53 "Tal pânico moral nos distrai de questões mais importantes, como Sebastian Meineck colocou, é apenas quando o conto da bolha de filtro explode que o debate sobre a transformação da esfera pública pode começar. Esse debate deverá examinar se as sociedades em todo o mundo, da Austrália ao Brasil, da Alemanha aos Estados Unidos, estão cada vez mais polarizadas ou se é essa polarização que simplesmente está mais visível; (...) essas transformações atrapalham muito e às vezes paralisam os sistemas políticos existentes e enfraquecem o consenso social fundamental. Mas também será necessário reconhecer que essas transformações não são alimentadas simplesmente por fatores superficiais, como as tecnologias e plataformas de comunicação preferidas por esses novos atores políticos e seus adversários estabelecidos, respectivamente – pelo contrário, são uma expressão de desafios sociais, econômicos, sociais e políticos muito mais fundamentais. Isso não significa que as plataformas de pesquisa e mídia social estejam livres de falhas, é claro – de fato, atualmente, há uma necessidade urgente de obrigá-las (através de regulamentações ou outros meios) a fazer mais para remover contas extremistas, impedir a circulação de desinformação e se abrirem ao escrutínio acadêmico independente. Na questão específica das bolhas de filtro, no entanto, elas parecem bastante livres de culpa." Bruns, A. (2019), "Filter bubble", *Internet Policy Review*.
- 54 Devido aos muitos fatores envolvidos no processo de manipulação política, de fatores culturais a tecnológicos e psicológicos/idiossincráticos, ainda é difícil atestar com clara certeza exatamente como e quantas pessoas foram influenciadas. A pesquisa empírica que examina processos e resultados especificamente de comunicação on-line ainda é escassa. Ecoando as palavras de Zuiderveen et al.: "A pesquisa empírica sobre a extensão da comunicação personalizada e seus efeitos no acesso a diversas informações pode servir como uma verificação da realidade. A pesquisa empírica pode ajudar a ajustar as prioridades nas políticas públicas e a identificar áreas nas quais simplesmente não temos conhecimento suficiente para fazer declarações políticas conclusivas. (...) se a tecnologia de personalização for aprimorada e o conteúdo de notícias personalizadas se tornar a principal fonte de informações das pessoas, problemas para a nossa democracia poderão, de fato, surgir, como demonstrou nossa análise dos estudos empíricos dos efeitos da mídia." Zuiderveen Borgesius, F. J. e Trilling, D. e Möller, J. e Bodó, B. e de Vreese, C. H. e Helberger, N. (2016), "Should we worry about filter bubbles?", *Internet Policy Review*, 5(1).
- 55 Zuiderveen Borgesius, F. J. e Trilling, D. e Möller, J. e Bodó, B. e de Vreese, C. H. e Helberger, N. (2016), "Should we worry about filter bubbles?", *Internet Policy Review*, 5(1).
- 56 Del Vicario, Michela et al. (2016), "The spreading of misinformation online", *Proceedings of the National Academy of Sciences dos Estados Unidos da América*, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4725489/>, acessado em outubro de 2019.
- 57 Moeller, J. e Helberger, N. (2018), "Beyond the filter bubble: Concepts, myths, evidence, and issues for future debates", Universidade de Amsterdã, https://www.ivir.nl/publicaties/download/Beyond_the_filter_bubble_concepts_myths_evidence_and_issues_for_future_debates.pdf, acessado em outubro de 2019.

- 58 "O Facebook conduziu um experimento psicológico maciço com 689.003 usuários, manipulando seus feeds de notícias para avaliar os efeitos em suas emoções. O Facebook tem a capacidade de fazer você se sentir bem ou mal, apenas ajustando o que aparece no seu feed de notícias. Eles contavam com um sistema automatizado que identificava palavras positivas ou negativas com base em um dicionário eletrônico. Eles reduziram o conteúdo positivo nos feeds de notícias de alguns usuários, descobrindo que, quando o conteúdo positivo era reduzido, uma porcentagem maior de palavras nas atualizações de status das pessoas era negativa e uma porcentagem menor era positiva. Quando a negatividade foi reduzida, ocorreu o padrão oposto. Os autores descobriram que esses resultados sugerem que as emoções expressas pelos amigos, através das redes sociais on-line, influenciam nosso próprio humor, constituindo, para nosso conhecimento, a primeira evidência experimental de contágio emocional em grande escala via redes sociais e dando suporte às afirmações, anteriormente contestadas, de que as emoções se espalham via contágio através por rede." McNeal, G. (2014), "Facebook Manipulated User News Feeds to Create Emotional Responses", <https://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/#10567b1039dc>, acessado em outubro de 2019. Leia também Ryan, C. (2013), "Digital Market Manipulation", Trabalho de pesquisa nº 2013-27 da Faculdade de Direito da Universidade de Washington.
- 59 Como afirma Cass Sunstein, os filtros de bolhas seriam um sério risco ao potencial da esfera pública conectada devido à falta de contato com opiniões divergentes e à polarização dos discursos, o que leva ao radicalismo. Isso seria um problema com as tendências de sofisticação dos algoritmos de personalização de conteúdo, não para sua resolução, mas para seu agravamento. Sunstein, C. (2011), "Republic.com 2.0", Princeton University Press. Leia também Sunstein, C. (2001), "Republic.com", Princeton University Press.
- 60 Os indivíduos têm uma responsabilidade importante nesse contexto, pois reduzem suas próprias bolhas de filtro pessoais. Ao entender e gerenciar recursos de personalização, coleta de cookies e anúncios segmentados em sites, podemos limitar o efeito que os algoritmos têm sobre nosso conteúdo.
- 61 Magrani, Eduardo e Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018", Cyber law. Uma declaração decisiva nesse sentido exigiria um estudo mais aprofundado, de modo que a abordagem específica desse ponto iria além dos limites deste estudo.
- 62 Leia <https://www1.folha.uol.com.br/poder/2019/10/whatsapp-admite-envio-massivo-ilegal-de-mensagens-nas-eleicoes-de-2018.shtml>, acessado em outubro de 2019.
- 63 De acordo com os resultados apresentados no estudo "Poder Computacional: Automação no uso do WhatsApp nas Eleições", sobre o uso de bots e do WhatsApp nas eleições brasileiras de 2018, ele afirma: "Identificamos especificamente que existem fortes elementos de uso da automação para impulsionar a distribuição de informações entre diferentes grupos no WhatsApp. Também identificamos que há uma ação coordenada entre diferentes membros em suas atividades nas redes de grupos de discussão no WhatsApp. (...) cerca de 56 % dos eleitores brasileiros disseram que suas escolhas de candidatos à presidência foram influenciadas pelas redes sociais. Deste modo, há hipóteses que apontam para a efetividade dessa estratégia, principalmente no primeiro turno, mesmo que, em diferentes extensões e com diferentes estratégias, todos os candidatos tenham feito uso de campanhas digitais. Ainda há pouco entendimento do uso da automação e do poder computacional para influenciar as decisões eleitorais", Machado, Caio e Konopacki, Marco (2018), "Poder Computacional: Automação no uso do WhatsApp nas Eleições; Estudo sobre o uso de ferramentas de automação para o impulsionamento digital de campanhas políticas nas eleições brasileiras de 2018", ITS Rio.
- 64 Casaes, D. e Córdova, Y. (2019), "Weaponized Information in Brazil: Digitizing Hate", Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, acessado em janeiro de 2019.
- 65 Casaes, D. e Córdova, Y. (2019), "Weaponized Information in Brazil: Digitizing Hate", Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, acessado em janeiro de 2019.
- 66 "O WhatsApp se tornou um instrumento de campanha particularmente poderoso. Fácil de usar, criptografado de ponta a ponta e facilitador do compartilhamento de mensagens para grandes grupos, o WhatsApp tem sido extremamente popular em países como Índia (Hickok, 2018), Brasil e outros países do Sul Global. No entanto, o WhatsApp não apenas permite que os partidos personalizem as mensagens para grupos precisos, mas também oferece anonimato, facilitando a deturpação da identidade de um remetente com as previsíveis e muito difundidas preocupações sobre o envio de "fake news" e mensagens de incitação ao ódio. Rafael Evangelista e Fernanda Bruno (2019) demonstram o uso pernicioso do WhatsApp para a disseminação de mensagens racistas, misóginas e homofóbicas no Brasil (...). A análise deles sugere que o WhatsApp conta com um relacionamento mais confiável entre os membros de um grupo do que é aparente em outras mídias sociais. Portanto, produz um meio mais suscetível à disseminação de desinformação." Leia Bennett, C. J. e Lyon, D. (2019), "Data-driven elections: implications and challenges for democratic societies", Internet Policy Review, 8(4). Leia também: Evangelista, R. e Bruno, F. (2019), "WhatsApp and political instability in Brazil: targeted messages and political radicalization", Internet Policy Review, 8(4).

- 67 A neutralidade da rede é o princípio da igualdade de tratamento de todos os pacotes de dados enviados pela Internet, independentemente de seu conteúdo, origem, destino e tipo de equipamento usado para acessá-lo. “Zero-rating” é quando um provedor de serviços de Internet aplica um preço zero ao tráfego de dados associado a um aplicativo ou a uma categoria de aplicativos específicos com base em um contrato comercial ou em uma decisão unilateral de um provedor de serviços de Internet que resulta na exclusão de algum conteúdo do limite mensal de dados dos usuários finais.
- 68 Casaes, D. e Córdova, Y. (2019), “Weaponized Information in Brazil: Digitizing Hate”, Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, acessado em janeiro de 2019.
- 69 Gollatz, K. e Jenner, L. (2018), “Hate Speech und Fake News – Zwei verwobene und politisierte Konzepte”, HIIG.
- 70 Martins, B e Varon, J. (2018), “Data and elections in Brazil”, Coding Rights.
- 71 Também existem investigações em andamento nos tribunais eleitorais sobre pagamentos e contratos não declarados relacionados a mensagens em massa e desinformação na campanha eleitoral de 2018.
- 72 Além disso, foram usados *bots* para aumentar a penetração em bolhas de filtro, aumentando a capacidade de enviar um grande número de mensagens on-line, atacando adversários e forjando discussões. Eles manipulam debates, produzem e divulgam notícias falsas e influenciam a opinião pública postando e replicando mensagens em grande escala. Muitos *bots* reproduziram hashtags no Twitter e no Facebook que ganham destaque ao enviar mensagens automatizadas para sufocar debates repentinos sobre um assunto específico. Martins, B e Varon, J. (2018), “Data and elections in Brazil”, Coding Rights.
- 73 Ruediger, M. (2019), “Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018”, FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, acessado em julho de 2019.
- 74 Ao interferir nas discussões, os robôs estão atingindo diretamente os processos políticos e democráticos por meio da influência da opinião pública. Cordova Y. e Doneda, D. (2017), “Um lugar para os robôs (nas eleições)”, JOTA, <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017>, acessado em março de 2018.
- 75 Magrani, Eduardo e Medeiros, R. (2019), “The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018”, Cyber law.
- 76 Leia <https://observa2018.com.br/posts/debate-influenciado-por-robos-volta-a-crescer-e-chega-a-104-das-discussoes-sobre-os-presidenciais-no-twitter/>, acessado em outubro de 2018.
- 77 É importante observar que as contas automatizadas também podem conferir aspectos positivos da vida nas redes sociais. Os chatbots, por exemplo, agilizam o atendimento ao cliente e, em alguns casos, até ajudam os consumidores a processar suas solicitações e obter mais informações. No entanto, um número crescente de robôs age com propósitos maliciosos na esfera pública. Os bots sociais (robôs sociais) são contas controladas por software, que geram conteúdo artificialmente e estabelecem interações com não robôs. Eles tentam imitar o comportamento humano e se passar por tal, para interferir em debates legítimos e voluntários e produzir discussões forjadas (não orgânicas). Instituto Tecnologia e Equidade (2017), “Especialistas explicam como o robô pode influenciar o debate nas redes”, Medium, <https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849>, acessado em outubro de 2017.
- 78 O estudo do uso de robôs já estabelece claramente o potencial prejudicial dessa prática para disputas políticas e debates públicos. Uma das conclusões mais aparentes nesse sentido é a concentração dessas ações em polos localizados no extremo do espectro político, promovendo artificialmente uma radicalização do debate nos filtros de bolhas e, portanto, prejudicando possíveis pontes de diálogo entre os diferentes campos políticos constituídos. Portanto, os robôs podem não só espalhar desinformação, o que pode ter efeitos prejudiciais à sociedade, mas também podem impedir ativamente que os usuários se informem adequadamente. Magrani, Eduardo e Medeiros, R. (2019), “The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018”, Cyber law.
- 79 Leia <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml>, acessado em janeiro de 2020.
- 80 Outro tipo de técnica de desinformação que está aumentando na prática e criando uma grande preocupação são os “*deepfakes*”. Eles são uma nova e muito mais sofisticada maneira de produzir desinformação. *Deepfakes* são vídeos falsos ou gravações de áudio que parecem e soam exatamente como uma pessoa real. As tecnologias já permitem a gravação de áudio com imitação quase semelhante à voz das pessoas e a edição de vídeos em que o rosto de um indivíduo que nunca esteve na situação aparece como participante. Se no cenário cotidiano de pessoas não públicas isso já é extremamente prejudicial à reputação e à imagem de uma pessoa, esse risco aumenta exponencialmente quando falamos de pessoas públicas. Vídeos e áudios editados podem ser usados, por exemplo, para difamar a imagem de um determinado candidato a um cargo eleitoral. Em 23 de outubro de 2018, no Brasil, foi divulgado um vídeo na internet

(principalmente no WhatsApp) no qual, supostamente, o candidato a governador do estado de São Paulo, João Doria (PSDB), aparecia em cenas íntimas com mulheres. Cinco dias após o segundo turno das eleições, a circulação de um vídeo nesse sentido prejudica imensamente a imagem do candidato, principalmente quando se considera que Doria é defensor dos valores da família tradicional. O então candidato entrou com uma investigação no Tribunal Eleitoral. Inicialmente, as investigações em relação ao vídeo constataram que ele foi montado ou simulado: um relatório de especialista afirmou que o rosto do candidato foi inserido desonestamente no vídeo, colocando-o em uma situação da qual ele não fez parte. Posteriormente, um novo relatório confirmou a veracidade do vídeo. Em resumo, dois relatórios técnicos com duas declarações contraditórias. Após o lançamento do vídeo, as pesquisas de preferências de votação mostraram alguma variação nos pontos percentuais de cada candidato. De acordo com a pesquisa do Datafolha de 25 de outubro de 2018, Doria tinha 52 % dos votos, já no dia 27 do mesmo mês havia caído para 49 %. Considerando a intensidade das campanhas nos dias imediatamente anteriores às eleições e a profusão de informações divulgadas, não podemos afirmar que o vídeo foi diretamente responsável por esta queda. O fato é que a divulgação desse *deepfake*, acompanhada de laudos de especialistas que não indicaram o mesmo resultado, não foi suficiente para impedir a vitória do candidato, que venceu com 51,77 % dos votos válidos. Observe, no entanto, que podemos afirmar que esse tipo de vídeo pode ser um fator importante a ser enfrentado nos momentos finais de uma campanha. Além disso, a própria realidade é posta à prova e o que é verdadeiro ou falso deixa de ser conhecido. Isso cria uma confusão mental no eleitorado, que acredita em um lado sem fundamento sólido, contando com narrativas. Sendo tudo questionável, o desejo humano por uma resposta se agarra a qualquer indício de veracidade, viés anterior ou mesmo autoengano. O uso conjunto de *deepfakes* com microsegmentação e inteligência artificial, sem uma regulamentação adequada e robusta para controlá-lo, já é uma das principais preocupações para as próximas eleições. Magrani, Eduardo e Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018", Cyber law.

- 81 Pablo Ortellado (2018), "Polarização na internet não parece ser causada pelas bolhas", Folha de São Paulo, <https://www1.folha.uol.com.br/colunas/pablo-ortellado/2018/02/polarizacao-na-internet-nao-parece-ser-causada-pelas-bolhas.shtml>, acessado em outubro de 2018. Leia também Mello, P. (2018), "Empresários bancam campanha contra o PT pelo WhatsApp", Folha de São Paulo, <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml>, acessado em outubro de 2018.
- 82 Magrani, Eduardo e Medeiros, R. (2019), "The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018", Cyber law.
- 83 Os bots representam mais de 50 % do tráfego da Internet em todo o mundo. Alguns bots têm o propósito de, por exemplo, exigir a responsabilização de políticos, erradicar a desigualdade de gênero ou ajudar a organizar as (muitas) tarefas diárias de seus usuários. Outros bots visam espalhar mentiras para influenciar discussões na esfera pública, um fenômeno que vem ganhando escala global desde 2014. Esses bots estão por aí e quase ninguém sabe como eles funcionam, quem os desenvolve e por quem são financiados. Leia <https://g1.globo.com/rs/rio-grande-do-sul/noticia/pesquisa-demonstra-que-repercussao-do-cancelamento-do-queermuseu-foi-insuflada-por-robos-na-internet.ghhtml>, acessado em março de 2017.
- 84 Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018", FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, acessado em julho de 2019.
- 85 Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018", FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, acessado em julho de 2019.
- 86 Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018", FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, acessado em julho de 2019.
- 87 Em 2014, a primeira eleição presidencial em que os robôs tiveram um papel mais importante, a interferência foi semelhante. Os bots foram responsáveis por mais de 10 % das interações no Twitter. Anteriormente, durante o processo de impeachment da ex-presidente Dilma Rousseff, os robôs foram responsáveis por 20 % do debate entre os apoiadores de Dilma. No segundo turno das eleições de 2014, 20 % das interações a favor de Aécio Neves foram realizadas por robôs. Leia Ruediger, M. (2019), "Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018", FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, acessado em julho de 2019.
- 88 "O Twitter afirma que, desde junho de 2017, detectou uma média diária de 130.000 contas que tentaram manipular assuntos populares através de bots sociais. A rede social afirma que existem cerca de 16 milhões de contas falsas ou de spam. Especialistas estimam um número maior. A dinâmica é conhe-

- cida como “botnet”, ou rede de robôs, quando os perfis agem de maneira sincronizada, com o mesmo desempenho – um publica e outros retuitam, respondem ou publicam algo semelhante. As regras gerais da plataforma declaram que não é permitido o uso dos serviços do Twitter para amplificar ou suprimir artificialmente as informações ou se envolver em comportamentos que manipulem ou prejudiquem a experiência das pessoas no Twitter. De acordo com a rede social, contas que violam essas regras podem ser punidas com visualização reduzida, removidas do mecanismo de busca do Twitter e até banidas.” Leia <https://apublica.org/2019/12/como-funciona-um-perfil-robo-no-twitter/>, acessado em janeiro de 2020.
- 89 “A detecção através do aprendizado de máquina acontece codificando os padrões de comportamento a partir da coleta de metadados. Dessa forma, o sistema é capaz de identificar automaticamente seres humanos e robôs com base no padrão comportamental do perfil. Os metadados do usuário são considerados um dos aspectos mais previsíveis da diferenciação entre humanos e robôs e podem contribuir para entender melhor como os robôs sofisticados funcionam. No entanto, identificar esses robôs ou contas invadidas é difícil para esses sistemas. Além disso, a constante evolução dos robôs faz com que o sistema, construído a partir de um banco de dados estático, se torne menos preciso ao longo do tempo. Contudo, ele permite processar um grande número de correlações e padrões complexos, além de analisar um grande número de contas. Os mecanismos de identificação mais eficientes combinam diferentes aspectos dessas abordagens, explorando várias dimensões do comportamento do perfil, como padrões de atividade e tempo. Esses sistemas levam em conta, por exemplo, que usuários reais passam mais tempo na rede trocando mensagens e visitando o conteúdo de outros usuários, como fotos e vídeos, enquanto as contas de robôs passam seu tempo pesquisando perfis e enviando solicitações de amizade.” Ruediger, M. (2019), “Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018”, FGV, <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/>, acessado em julho de 2019.
- 90 Magrani, Eduardo e Medeiros, R. (2019), “The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018”, *Cyber law*.
- 91 Simões, M. (2018), “Grupos pró-Bolsonaro no WhatsApp orquestram notícias falsas e ataques pessoais na internet, diz pesquisa”, *El País*, https://brasil.elpais.com/brasil/2018/10/23/politica/1540304695_112075.html?id_externo_rsoc=FB_BR_CM&fbclid=IwAR05Mw9zXzmjDbYv5OkjAm1hVipWBURMCPyiOORlaxSsy_qNxEjzrpHKxfQ, acessado em outubro de 2018.
- 92 Leia <https://observa2018.com.br/posts/fraude-nas-urnas-e-kit-gay-tem-maior-impacto-que-outras-noticias-falsas-em-twitter-facebook-e-youtube/>, acessado em outubro de 2018.
- 93 Giannetti, E. (2005), “Auto- Engano”, Companhia das Letras.
- 94 Há projetos de lei no Congresso Nacional brasileiro que criminalizam a divulgação de fatos falsos/*fake news*, como os projetos de lei nº 9973/2018, 10292/2018, 9931/2018 e 9532/2018 na Câmara dos Deputados. O Projeto de Lei do Senado nº 246/2018 é mais amplo e busca inserir no Marco Civil da Internet “medidas para combater a divulgação de conteúdo falso ou aplicativos ofensivos da Internet”. Além disso, há grupos para realizar a verificação de fatos. Mas, em um cenário em que tudo é questionável, a profusão de informações verdadeiras e falsas pode levar ao chamado contexto de “infocalipse”, como afirma o Prof. Aviv Ovadya, comprometendo a possibilidade de consenso em bases racionais e democráticas. Por isso, afirmamos acima que é essencial garantir um nível mínimo de consenso sobre a realidade e o respeito aos princípios éticos fundamentais. Uma enumeração completa e uma apresentação detalhada de todas as leis sobre o assunto exigiriam um estudo próprio e ultrapassariam os limites deste artigo. Leia <https://www.uol/noticias/especiais/ele-previu-o-apocalipse-das-noticias-falsas.htm>, acessado em janeiro de 2020.
- 95 Leia <https://www1.folha.uol.com.br/poder/2018/12/fraude-com-cpf-viabilizou-disparo-de-mensagens-de-whatsapp-na-eleicao.shtml>. Leia também <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml> Leia também <https://www1.folha.uol.com.br/poder/2018/10/entenda-as-irregularidades-envolvendo-uso-do-whatsapp-na-eleicao.shtml>, acessado em janeiro de 2020.
- 96 Leia <https://riotimesonline.com/brazil-news/brazil/whatsapp-admits-to-illegal-mass>, acessado em novembro de 2019.
- 97 O Facebook, que está sob crescente pressão para fazer mais para combater a desinformação, anunciou em janeiro uma atualização do WhatsApp que reduziu para cinco o número de vezes que os usuários podem encaminhar uma única mensagem. Leia <https://www.theguardian.com/world/2019/oct/29/europe-accuses-facebook-of-being-slow-to-remove-fake-accounts>, acessado em janeiro de 2020. Leia também <https://www.theguardian.com/technology/2019/jan/21/whatsapp-limits-message-forwarding-fight-fake-news>. Leia também https://politica.estadao.com.br/blogs/estadao-verifica/limite-de-encaminhamento-no-whatsapp-nao-consegue-frear-desinformacao-na-plataforma-aponta-pesquisa/?amp&__twitter_impression=true&fbclid=IwAR1X_aDEg7Mlz_0OoCE1piZHko_TyyMQVgyw9SH-hT4Vc37Lbfj5By6JumU, acessado em janeiro de 2020.

- 98 Leia https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests?CMP=share_btn_fb, acessado em janeiro de 2020.
- 99 De acordo com Yasodora Cordova e Diego Casaes, em um relatório recente sobre o contexto brasileiro: “Os brasileiros fazem tudo pelo WhatsApp, já que é ‘gratuito’. De aulas de música ao comércio eletrônico e consultas médicas, o aplicativo se tornou essencial para o funcionamento dos negócios e da vida familiar, especialmente para as comunidades mais vulneráveis. Os cidadãos brasileiros são alguns dos maiores usuários de mídia social do mundo, perdendo apenas para as Filipinas. Os cidadãos, no entanto, geralmente são limitados ao conteúdo que recebem via WhatsApp e, portanto, perdem o contexto e a oportunidade de verificar on-line diferentes versões ou expandir seus conhecimentos. O fato de que tudo que passa pelo WhatsApp é gratuito, facilita a difusão de áudios ou vídeos do YouTube (que são abertos no WhatsApp). Devido a esse design, o WhatsApp pode ser considerado um canal para desinformação em muitos formatos, mas é especialmente prejudicial para áudio e vídeos. Juntos, o YouTube e o WhatsApp formaram um fluxo de desinformação, espalhando teorias da conspiração, material de campanha e propaganda política em todo o Brasil.” Casaes, D. e Córdova, Y. (2019), “Weaponized Information in Brazil: Digitizing Hate”, Policy Brief No.63 Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, acessado em janeiro de 2019.
- 100 Evangelista, R. e Bruno, F. (2019), “WhatsApp and political instability in Brazil: targeted messages and political radicalization”, Internet Policy Review, 8(4), acessado em outubro de 2018. Nas palavras de Rafael Evangelista e Fernanda Bruno: Embora o WhatsApp não forneça um serviço para a microsegmentação do público, há evidências de que empresas terceirizadas, dedicadas a campanhas de marketing não político, forneceram esse tipo de serviço no contexto de eleições, às vezes usando bancos de dados ilegais. (...) O caso de uso do WhatsApp nas eleições brasileiras mostra como uma estrutura de vigilância foi construída sobre um serviço de mensagens em grupo que supostamente usa criptografia para proteger a privacidade de seus usuários.”
- 101 Leia https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests?CMP=share_btn_fb, acessado em janeiro de 2020.
- 102 “Internet Policy Review, 8(4)”. Leia também Cesarino, L. (2019), “On Digital Populism in Brazil”, PoLAR: Political and Legal Anthropology Review, <https://polarjournal.org/2019/04/15/on-jair-bolsonaros-digital-populism/>, acessado em janeiro de 2020.
- 103 Recentemente, a Comissão Europeia “reconheceu a exposição dos cidadãos à desinformação on-line e à microsegmentação de eleitores com base no tratamento ilegal de dados pessoais como um dos principais desafios das democracias europeias. Em resposta, a CE adotou várias medidas para formular uma abordagem europeia. (...) As orientações da Comissão sobre a aplicação do RGPD no contexto eleitoral (CE, 2018d) destaca que “ele se aplica a todos os atores ativos no contexto eleitoral”, incluindo partidos políticos nacionais e europeus, fundações políticas, plataformas, empresas de análise de dados europeias e nacionais e autoridades públicas responsáveis pelo processo eleitoral. Qualquer tratamento de dados deve estar em conformidade com os princípios do RGPD, como justiça e transparência, e apenas para fins especificados”. Leia Nenadić, I. (2019), “Unpacking the European approach to tackling challenges of disinformation and political manipulation”, Internet Policy Review, 8(4). Leia também: Comissão Europeia (2018), “Eleições europeias livres e justas – Ficha informativa, Estado da União”, https://ec.europa.eu/commission/presscorner/detail/pt/IP_18_5681. Leia também: Comissão Europeia (2018), “Commission guidance on the application of Union data protection law in the electoral context: A contribution from the European Commission to the Leaders’ meeting in Salzburg”, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf, acessado em janeiro de 2019.
- 104 Westby, J. (2019), “The Great Hack’: Cambridge Analytica is just the tip of the iceberg”, Amnesty Tech, <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>, acessado em janeiro de 2019.
- 105 Westby, J. (2019), “The Great Hack’: Cambridge Analytica is just the tip of the iceberg”, Amnesty Tech, <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>, acessado em janeiro de 2019.
- 106 Leia <https://privacyinternational.org/learning-topics/data-and-elections>, acessado em janeiro de 2019.
- 107 Risso, Linda (2017), “Harvesting Your Soul? Cambridge Analytica and Brexit”, Akademie der Wissenschaften und der Literatur, http://www.adwmainz.de/fileadmin/user_upload/Brexit-Symposium_Online-Version.pdf#page=75, acessado em dezembro de 2019.
- 108 “Os legisladores deveriam ser obrigados a acompanhar as inovações em rápida evolução nos setores de tecnologia e marketing, identificando os usos e abusos de aplicativos digitais para fins políticos, como a maneira como o WhatsApp foi implantado para propaganda computacional nas últimas eleições do Brasil.” Em: Chester, J. e Montgomery, K. C. (2019), “The digital commercialization of US politics – 2020 and beyond”, Internet Policy Review, 8(4), acessado em janeiro de 2019.

- 109 “É justo dizer que os reguladores geralmente demoram a apreciar a complexa variedade de riscos apresentados pelas campanhas baseadas em dados. Até relativamente recentemente, por exemplo, a maioria das autoridades de proteção de dados (APDs) não tinha interesse ativo no tratamento de dados pessoais dentro do processo eleitoral em seus respectivos países. Houve algumas orientações e decisões anteriores sobre campanhas políticas no Reino Unido (ICO, 2014) e uma série de decisões na França (CNIL, 2012). Na maioria dos países da UE e em outros países em que os partidos políticos são regulamentados pela lei de proteção de dados, as decisões se referem a questões bastante restritas, motivadas por queixas individuais sobre as ações de partidos e candidatos específicos durante pleitos eleitorais específicos. Da mesma forma, os reguladores das eleições geralmente se preocupam mais com a execução transparente e eficiente das eleições, juntamente com perguntas sobre financiamento eleitoral, do que com o tratamento de dados pessoais do eleitorado.” Leia Bennett, C. J. e Lyon, D. (2019), “Data-driven elections: implications and challenges for democratic societies”, *Internet Policy Review*, 8(4).
- 110 Comissão Europeia, “Comissão propõe normas rigorosas em matéria de privacidade para todas as comunicações eletrônicas e atualiza as regras de proteção de dados para as instituições da UE”, http://europa.eu/rapid/press-release_IP-17-16_pt.htm, acessado em janeiro de 2019.
- 111 Samuel C. Woolley e Philip N. Howard (2017), “Computational Propaganda Worldwide”, Universidade de Oxford, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-Executive-Summary.pdf>, acessado em outubro de 2019.
- 112 Lane, Julia, et al. (eds.) (2014), “Privacy, Big Data, and the Public Good: Frameworks for Engagement”, Cambridge.
- 113 A Comissão Europeia propõe normas rigorosas em matéria de privacidade para todas as comunicações eletrônicas e atualiza as regras de proteção de dados para as instituições da UE. 2017. Leia http://europa.eu/rapid/press-release_IP-17-16_pt.htm, acessado em janeiro de 2019.

A woman with dark hair, wearing a white shirt and a black backpack, is holding a smartphone. Overlaid on her face is a white wireframe mesh, representing facial recognition technology. The background is a blurred city street. The image is framed by a teal and blue geometric design with white L-shaped corner markers.

2. Conformidade dos regulamentos de proteção de dados nas eleições

Uma análise comparativa entre a UE e o Brasil (RGPD vs. LGPD)

Para analisar a aplicação dos regulamentos de dados pessoais aos processos eleitorais no Brasil e na UE, esta seção explora as semelhanças e diferenças mais relevantes entre o Regulamento Geral de Proteção de Dados europeu (RGPD) e a Lei Geral de Proteção de Dados (LGPD) brasileira. As considerações a seguir exploram como esses intrincados sistemas determinam os limites da capacidade de tratamento de dados de candidatos e partidos em cada jurisdição, além de apresentar instrumentos normativos relevantes relacionados especificamente aos processos eleitorais.

A Lei Geral de Proteção de Dados do Brasil foi amplamente baseada no Regulamento Geral de Proteção de Dados da UE. Portanto, há muitas semelhanças entre os dois. Em primeiro lugar, existem sobreposições entre os princípios gerais de ambas as leis. O RGPD lista, no artigo 5, seis princípios relacionados ao tratamento de dados pessoais. A LGPD lista, no artigo 6, dez princípios. Ambos fornecem como principais valores: finalidades claras e específicas, transparência, qualidade (precisão) dos dados, segurança, responsabilização, legalidade e justiça. O cabeçalho do artigo brasileiro sobre princípios diz:

Art. 6º As atividades de tratamento de dados pessoais devem observar a boa-fé e os seguintes princípios...

A “boa-fé” mencionada pode ser interpretada como sendo análoga ao princípio da justiça do RGPD. “Boa-fé” é um princípio geral do direito civil no Brasil. Sua menção explícita no caput do artigo, relativa aos princípios do tratamento de dados pessoais, reforça seu papel como eixo interpretativo na aplicação da lei. Na prática, isso significa levar em consideração o contexto da coleta de dados para determinar os usos razoavelmente esperados e justos dos dados. Isso é o que os juristas descrevem como “privacidade contextual”¹¹⁴:

Em resumo, a teoria da privacidade contextual consiste, portanto, em considerar que o titular dos dados tem expectativas legítimas (de privacidade) sobre como seus dados devem fluir adequadamente. O tráfego de dados, portanto, não acontece no vácuo, mas sob um conjunto de circunstâncias que determinam sua integridade.

Apesar das muitas semelhanças, como o princípio de justiça acima mencionado, há, no entanto, casos em que os dois regulamentos diferem. Um desses casos é a definição de responsáveis conjuntos pelo tratamento (“controladores” na redação da LGPD). Os responsáveis conjuntos pelo tratamento estão descritos no artigo 26 do RGPD, que diz:

Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respectivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respectivos deveres de fornecer as informações referidas nos artigos 13.º e 14.º, a menos e na medida em que as suas responsabilidades respectivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contato para os titulares dos dados.

É importante observar que o mesmo conjunto de dados pode ter muitos responsáveis pelo tratamento distintos, quando eles o usam para propósitos distintos, ou responsáveis conjuntos pelo tratamento, quando eles decidem conjuntamente sobre os propósitos do tratamento¹¹⁵. A lei brasileira, por outro lado, não possui uma categoria explícita de controladores conjuntos. A controladoria ainda é determinada com base na capacidade de decidir sobre os propósitos do tratamento, mas não há menção à controladoria conjunta. A lei, no entanto, sugere isso em uma instância.

No artigo 42, II, o LGPD declara que os controladores diretamente envolvidos em uma atividade de tratamento devem ser solidariamente responsáveis por quaisquer violações. Este artigo sugere a controladoria conjunta, afirmando que atores distintos podem ser agrupados sob os efeitos da lei, uma interpretação que deve ser considerada ao determinar a estrutura de governança dos esforços de campanha política. Nesses casos, isso é especialmente verdade devido a outra lei sobre a responsabilidade de candidatos e partidos políticos. A lei brasileira n. 9.504/1997 afirma, no Artigo 6º, § 5º:

§ 5º A responsabilidade pelo pagamento de multas decorrentes de propaganda eleitoral é solidária entre os candidatos e os respectivos partidos(...)

Deste modo, a LGPD é totalmente aplicável ao tratamento de dados pessoais realizado por partidos e candidatos, bem como suas estruturas de campanha. Na lei brasileira, isso é ainda mais enfatizado pela caracterização dos partidos políticos como associações privadas, ou seja, entidades que se enquadram no mesmo regime jurídico geral das empresas privadas e organizações não governamentais.

A controladoria é uma questão crucial em ambas regulamentações, uma vez que o controlador é responsável pela implementação de um amplo conjunto de requisitos e, em última instância, é responsável por quaisquer violações. Na prática, definir o controlador de dados pessoais pode ser um desafio, ou seja, encontrar a(s) pessoa(s) com a capacidade de decidir substancialmente os propósitos e os meios de tratamento. No contexto de campanhas eleitorais, isso pode ser uma avaliação complexa:

O papel de responsável pelo tratamento de dados ou subcontratante deve ser avaliado em cada caso individualmente. No contexto eleitoral, vários atores podem ser responsáveis pelo tratamento de dados: partidos políticos, candidatos individuais e fundações são, na maioria dos casos, responsável pelo tratamento de dados; as empresas de plataformas e de análise de dados podem ser responsáveis (conjuntos) ou subcontratantes de um determinado tratamento, dependendo do grau de controle que elas têm sobre o tratamento em questão; as autoridades eleitorais nacionais são responsáveis pelo tratamento dos registros eleitorais¹¹⁶.

Além dos responsáveis pelo tratamento, as campanhas eleitorais também devem prestar atenção a mais duas entidades envolvidas nos relacionamentos de tratamento de dados pessoais. O tratamento de dados é conduzido por um “subcontratante” (RGPD; chamado de “operador” na LGPD), que realiza a vontade e a estratégia do responsável pelo tratamento. Enquanto o responsável pelo tratamento possui poder de decisão substancial, o subcontratante apenas implementa as atividades de tratamento planejadas. O outro é o encarregado da proteção de dados (RGPD;

chamado de “Encarregado” na lei brasileira), que serve como canal de comunicação entre o titular dos dados, a Autoridade de Proteção de Dados e a empresa ou organização.

As funções do subcontratante e do encarregado da proteção de dados são muito diferentes. O subcontratante está envolvido nas atividades de tratamento e possui o conhecimento técnico necessário para implementar as decisões do responsável pelo tratamento, agindo segundo as ordens deste. O encarregado da proteção de dados, por outro lado, tem sido descrito como “a manifestação da autoridade de controle em uma organização¹¹⁷”. O ideal é que essa função seja independente do responsável pelo tratamento e do subcontratante, para realizar uma avaliação abrangente das atividades de tratamento de dados e informar à autoridade e aos titulares sobre qualquer problema quando necessário¹¹⁸.

Embora tenha conceito semelhante, o encarregado da proteção de dados e o “Encarregado” são desenvolvidos de maneira ligeiramente diferente no RGPD e na LGPD. Uma distinção importante é que a nomeação de um “Encarregado” é geralmente obrigatória e sua renúncia exige especificação adicional pela Autoridade Brasileira de Proteção de Dados (Art. 41, § 3º, da LGPD). O RGPD, por outro lado, lista os casos em que o encarregado da proteção de dados é necessário, embora nomear um encarregado da proteção de dados seja considerado uma prática recomendada¹¹⁹.

A legislação brasileira tratou, até certo ponto, de dados pessoais em campanhas eleitorais antes da LGPD. Um exemplo refere-se ao compartilhamento de dados com terceiros. Segundo o Artigo 7º, I e § 5º, da LGPD, se dados foram coletados e tratados com base em consentimento e precisaram ser comunicados a outro controlador, isso exigiria um novo ato de consentimento específico da parte do titular dos dados. Se fossem amparados por qualquer outra base jurídica, os deveres de transparência e responsabilização, e todos os direitos do titular e os princípios da lei, ainda seriam aplicáveis, mas não seria necessária comunicação prévia ao titular. Isso significaria registrar cuidadosamente a transferência e seus propósitos. Dependendo do caso (mas preferencialmente), em um relatório de Avaliação de Impacto sobre a Proteção de Dados (AIPD)¹²⁰. Caso a base jurídica para o tratamento seja o interesse legítimo, é recomendável fazer uma avaliação do interesse legítimo (em inglês, Legitimate Interest Assessment – LIA)¹²¹.

No entanto, antes da LGPD já existia o Artigo 57-E da lei n. 9.504/97 (Regulamento dos Partidos Políticos), que proíbe o compartilhamento ou a compra de listas de informações de contato para fins de propaganda política. O artigo dispõe:

Art. 57-E. São vedadas às pessoas relacionadas no art. 24 a utilização, doação ou cessão de cadastro eletrônico de seus clientes, em favor de candidatos, partidos ou coligações.

§ 1º É proibida a venda de cadastro de endereços eletrônicos.

Com essa proibição geral de compartilhamento de informações de contato, o cenário é ainda mais complicado. “Cadastros eletrônicos” não podem ser comunicados por uma lista de entidades, incluindo entidades ou governos estrangeiros; escritórios

de administração pública; prestadores de serviços públicos; sindicatos; organizações sem fins lucrativos que recebem financiamento estrangeiro; organizações não governamentais que recebem financiamento público; entre outros. Empresas privadas em geral foram adicionadas a essa lista após uma decisão do Supremo Tribunal no caso ADI 4650, que tratava de doações privadas a campanhas eleitorais¹²². Além disso, é proibida qualquer comercialização de cadastros de endereços eletrônicos.

O RGPD não toca explicitamente na comercialização de dados. No entanto, uma interpretação de acordo com as regras e princípios do regulamento determina que o responsável pelo tratamento trate dados pessoais conforme os propósitos inicialmente previstos¹²³. Isso significa que a transferência de dados – seja através de doação ou venda – para terceiros deve atender ao propósito original da coleta de dados.

Na prática, essas considerações significam que as campanhas eleitorais devem ter cuidado com a fonte de seus dados e com quem tem acesso a eles. Se a coleta inicial de dados foi feita diretamente pela campanha, por meio de associação on-line ou física, todos os usos futuros das informações – incluindo marketing por e-mail e definição de perfis – devem ser divulgados ao titular dos dados. Se a coleta inicial de dados não estiver relacionada a campanhas eleitorais, por exemplo, se um candidato tiver informações de contato de seus eleitores para ajudá-los com questões específicas no exercício regular de suas atribuições políticas, deve-se perguntar se outros usos seriam razoavelmente esperados pelo titular dos dados¹²⁴. Isso vale para os contextos europeu e brasileiro. Além disso, no Brasil, as campanhas eleitorais não devem aceitar doações nem comprar listas de contatos, pois isso é explicitamente proibido pela lei eleitoral.

O caso que foi descrito anteriormente a respeito das mensagens políticas divulgadas via WhatsApp durante as eleições brasileiras é um bom exemplo de uma prática que contraria esses deveres. Empresas especializadas foram então contratadas para enviar tais mensagens em larga escala para listas de números – sob condições incertas¹²⁵. É possível argumentar que as pessoas nessas listas não tinham uma expectativa razoável de receber propaganda eleitoral ou notícias políticas via WhatsApp e os ativistas teriam dificuldade em fornecer evidências de consentimento específico ou qualquer outra base jurídica para tais atividades.

Semelhante a essa questão é a coleta e o tratamento de dados disponíveis ao público. Tal coleta de dados em escala pode ser usada para atividades de definição de perfis¹²⁶, por meio do qual é possível cruzar fontes e pontos de dados distintos para permitir inferências e criar o perfil detalhado de uma pessoa. Todos os dados assim coletados e inferidos estão sujeitos a regulamentos de proteção de dados, pois se trata de “informação relativa a uma pessoa singular identificada ou identificável” (Art. 4, RGPD), ou “informação relacionada a uma pessoa natural identificada ou identificável” (Art. 5º, LGPD). Essa foi a base do caso Cambridge Analytica supracitado, segundo o qual, com o uso de técnicas de análise de dados, a empresa conseguiu categorizar os eleitores em grupos distintos, mesmo aqueles que não deram consentimento explícito à coleta de seus dados¹²⁷. Com base no que poderia ser percebido como informação “publicamente disponível” (coletada através dos perfis dos usuários e dos seus amigos), a CA distorceu efetivamente o processo democrático por meio de psicomетria e big data.

Na LGPD brasileira, dados “disponíveis ao público” são mencionados em três instâncias: Parágrafos 3º, 4º e 7º do Artigo 7º. A primeira descreve o tratamento de “dados pessoais disponíveis ao público”, declarando que este deve observar o propósito original e o interesse público que fundamentou sua publicação, bem como a boa-fé. A segunda instância trata de “dados tornados públicos pelo titular manifestamente”, neste caso, criando uma exceção para o consentimento. A terceira, uma alteração tardia da lei, permite o tratamento desses dados para novos propósitos. Existe um conflito aparente entre os parágrafos 3 e 7, uma vez que o primeiro limita o tratamento diferente do contexto original e o segundo permite o tratamento para novos fins. Provavelmente, esse é um problema com o qual a nova Autoridade Nacional de Proteção de Dados (ANPD) terá que lidar.

Nesse ponto, o RGPD é muito mais preciso que a LGPD. O Artigo 14.º do RGPD refere-se a “informações a facultar quando os dados pessoais não são recolhidos junto do titular”, a partir de dados disponíveis ao público, por exemplo. O artigo contém uma série de especificações dos deveres do responsável pelo tratamento a respeito do tratamento de dados. Esses são deveres de informação que incluem: os usos pretendidos dos dados, o período de tratamento, a identidade do responsável pelo tratamento, as categorias de dados coletados, os propósitos do tratamento, os destinatários e as fontes dos dados, os direitos do titular de retificação e de reclamação a uma autoridade de controlo, entre outros.

Com base tanto na LGPD como no RGPD, as possibilidades de tratamento com base em “dados pessoais disponíveis ao público” devem ser cuidadosamente abordadas pelas autoridades, levando em consideração o que ocorreu em situações específicas, como a distribuição de mensagens em massa do WhatsApp, no Brasil, ou o Caso da CA. Embora possa haver isenções de consentimento em relação a dados pessoais disponíveis ao público, em muitos casos, o tratamento pode ser considerado ilegal por não serem adotadas etapas fundamentais de conformidade, como informar o titular dos dados sobre o tratamento e garantir princípios e direitos básicos de proteção de dados.

Devido à total aplicabilidade dos regulamentos de proteção de dados pessoais, é importante que partidos e candidatos tomem todas as precauções para garantir a observância de todos os princípios e direitos. Isso geralmente começa com um mapeamento completo dos fluxos de dados na estrutura da campanha, um trabalho estreitamente relacionado às responsabilidades de um encarregado da proteção de dados. Especialmente quando dados sensíveis estão sendo tratados, o que geralmente ocorre em campanhas eleitorais. Como os dados com os quais eles lidam geralmente incluem opiniões políticas dos titulares dos dados, o papel do encarregado da proteção de dados se torna ainda mais crucial. Campanhas diferentes têm necessidades e formatos diferentes, especialmente em contextos amplos e diversos, como os cenários políticos brasileiro e europeu. Uma justificativa ponto a ponto de todas as instâncias em que dados são coletados, comunicados, armazenados ou tratados, de todas as maneiras; de quem tem acesso a quais tipos de dados; qual é a base jurídica para o tratamento de dados, sejam eles normais ou sensíveis; e a duração e o propósito das atividades de tratamento, é um primeiro passo inestimável.

Uma diferença substancial entre os dois regulamentos é como tratam a Avaliação de Impacto sobre a Proteção de Dados (AIPD). Há referência às AIPDs no Artigo 35.º do RGPD e nos Artigos 10.º, 32.º e 38.º, entre outros, da LGPD. O primeiro estabelece a obrigação de realizar uma AIPD sempre que houver “elevado risco para os direitos e liberdades das pessoas singulares”. Isso pressupõe que deve ser conduzida, pelo menos, uma avaliação preliminar de riscos para todas as atividades de tratamento, a fim de determinar se há alto risco e, conseqüentemente, a obrigação de realizar uma AIPD¹²⁸. O artigo é extenso e determina não só deveres para o responsável pelo tratamento, mas também o envolvimento do encarregado da proteção de dados e os deveres da Autoridade de Proteção de Dados, responsável por determinar casos específicos em que é obrigatória uma AIPD.

A lei brasileira, por outro lado, trata o assunto das avaliações de impacto de maneira mais resumida, simplesmente mencionando que a Autoridade Brasileira de Proteção de Dados (ANPD) pode solicitá-las aos controladores e determinar o conteúdo exigido. A esse respeito, o Artigo 38.º da LGPD dispõe:

Art. 38.º A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Ao passo que o Artigo 35.º, n.º 7., do RGPD assim declara:

A avaliação inclui, pelo menos:

- a)** *uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;*
- b)** *Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;*
- c)** *Uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados a que se refere o n.º 1; e*
- d)** *As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.*

Como acontece em muitos assuntos, a lei brasileira optou por deixar as especificidades da regulamentação da AIPD à ANPD. Isso envolverá, por exemplo, decidir quais agentes serão obrigados a realizar AIPDs e em que circunstâncias. Isso é reforçado por pelo menos dois itens da lei, a saber, o Artigo 55-J, XIII e XVIII. O primeiro afirma que a Autoridade Nacional é competente para elaborar regulamentos e determinar

procedimentos para as AIPDs nos casos em que haja um alto risco aos princípios e direitos garantidos na lei. O último afirma que é de competência da autoridade definir procedimentos especiais e simplificados para pequenas empresas e startups.

Outra distinção importante entre os regulamentos europeu e brasileiro está relacionada ao tratamento automatizado de dados. No RGPD, o titular dos dados tem o direito de não ser incluído em processos automatizados de tomada de decisão, incluindo definição de perfis. Este direito atende a três exceções, a saber:

Art. 22º O n.º 1 não se aplica se a decisão:

- a) for necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;*
- b) for autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou*
- c) for baseada no consentimento explícito do titular dos dados.*

No entanto, mesmo que alguma das exceções se aplique, o regulamento europeu garante o direito do titular a uma intervenção humana no processo automatizado para que possa “manifestar o seu ponto de vista e contestar a decisão” (Art.º 22, n.º 3). A LGPD brasileira teria incluído uma disposição semelhante, se tivesse sido aprovada em sua forma original. Porém, a lei foi modificada por um decreto presidencial e, em sua forma atual, o Artigo 20º garante apenas o direito de “revisão” das decisões automatizadas. Ou seja, esta revisão não precisa ser feita por um agente humano.

É importante uma observação final sobre um preâmbulo específico a respeito do tratamento de dados pessoais sobre opiniões políticas de partidos durante as atividades eleitorais. Esse tratamento, que, conforme explicado acima, estaria coberto pelas proteções e restrições estabelecidas pelos regulamentos, é interpretado pelo preâmbulo 56 do RGPD¹²⁹, que permite um tratamento mais flexível com base no interesse público. Contudo, essa possibilidade deve ser abordada com cuidado, a fim de manter o processamento das opiniões políticas dos partidos políticos no espírito da lei.

As opiniões políticas são classificadas pelo Artigo 9.º do RGPD como uma categoria especial de dados pessoais, merecendo proteção mais forte. Seu tratamento é expressamente proibido (Art. 9.º, n.º 1) e permitido apenas em casos excepcionais (Art. 9.º, n.º 2). A lei brasileira não tem equivalente a preâmbulos e não faz referência expressa ao tratamento de opiniões políticas, exceto por sua categorização como dados pessoais sensíveis, o equivalente a dados de categorias especiais no RGPD. Essa aparente contradição será explorada na próxima seção, onde discutiremos a implementação com o propósito de garantir um processo democrático eficaz nas eleições em relação à proteção de dados pessoais.

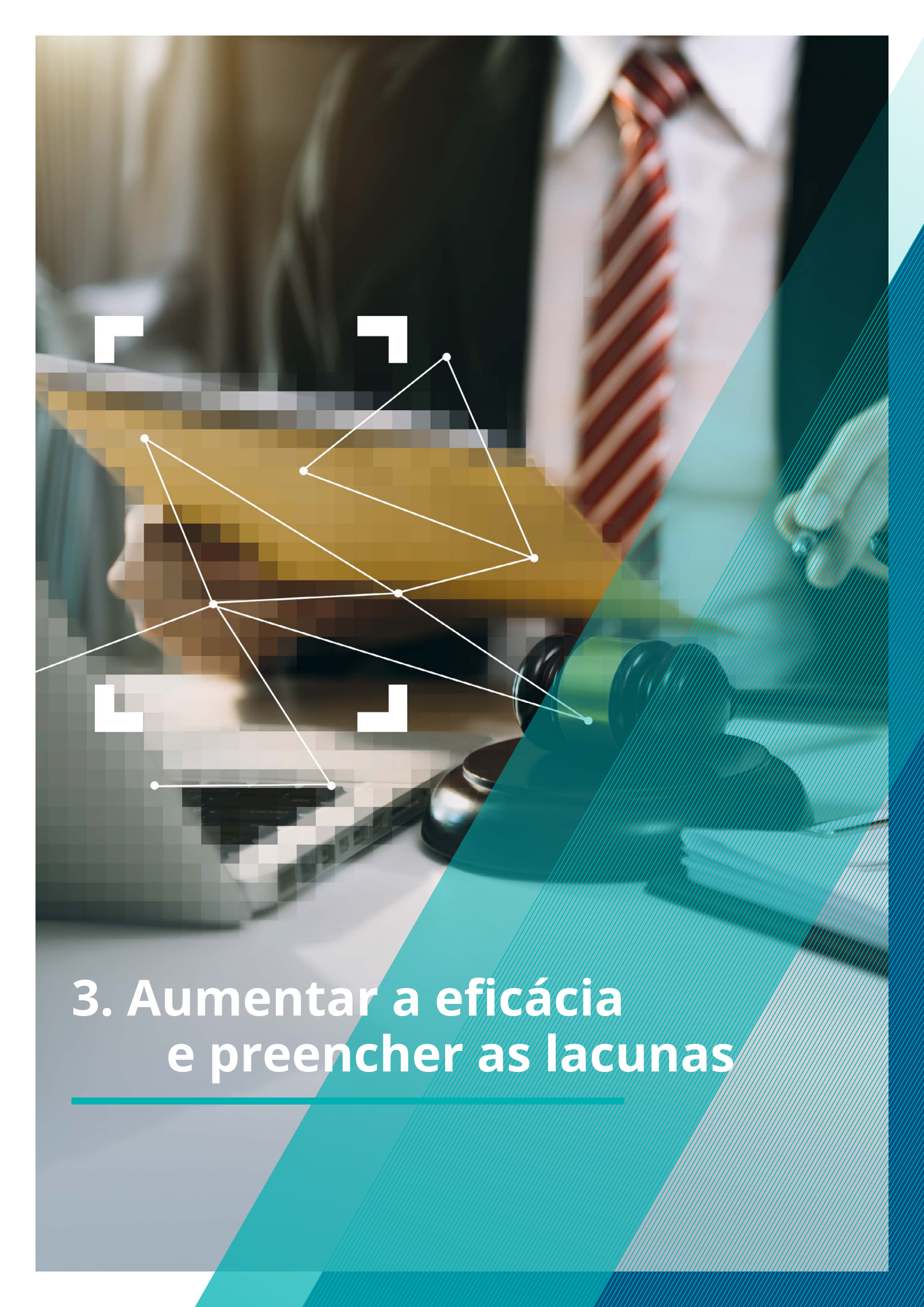
Antes de fazermos isso, no entanto, é importante destacar que, ao comparar a qualidade da regulamentação europeia com a da brasileira, não há uma resposta clara. A regulamentação brasileira é geralmente mais flexível que o RGPD e essa flexibilidade aparece quando abordamos o número de bases jurídicas para atividades de

tratamento, o sistema de notificação após a ocorrência de uma violação, o valor das multas administrativas, entre outros. Por um lado, isso pode ser percebido como um fator positivo, pois dá à indústria mais espaço para se adaptar às regras. Por outro lado, contudo, esse nível de flexibilidade pode gerar ineficácia da lei, uma vez que os parâmetros estabelecidos para os controladores são muito subjetivos e as disposições não são rígidas o suficiente para estabelecer limites claros. Além disso, coloca ainda mais responsabilidade nas costas das autoridades de proteção de dados. Nesse caso, no Brasil, diferentemente das Autoridades de Proteção de Dados (APDs) da UE, a Autoridade Nacional não é independente nem autônoma, pois está subordinada à Presidência da República. Além disso, sua estrutura e corpo ainda estão sendo projetados e formados. Considerando a importância da APD para garantir a eficácia e fornecer regulamentação específica em complemento à lei, todos esses elementos trazem incertezas quanto ao cumprimento e eficácia do cenário de proteção de dados no Brasil.

Apesar de ser semelhante à LGDP, o RGPD é claramente mais direto e objetivo em relação à regulamentação da proteção de dados. Esta é, novamente, uma razão para elogios e críticas. Por um lado, a rigidez cria um ambiente de segurança jurídica, guiado por altos parâmetros de proteção dos direitos fundamentais. Ou seja, como há um espaço mais controlado para escolhas discricionárias das Autoridades de Supervisão, é mais fácil ter uma aplicação harmonizada da lei em toda a União Europeia. Por outro lado, tentando traçar tais parâmetros, a regulamentação pode conter disposições inviáveis, como a declarada no Art. 33.¹³⁰, que podem tirar parte de sua credibilidade por sobrecarregar os responsáveis pelo tratamento e gerar custos desnecessários para eles.

Portanto, à luz das semelhanças e diferenças de abordagem de ambos os regulamentos (que podem inspirar comentários positivos e negativos), a questão não deve ser qual regulamento contém disposições melhores, pois isso pode ser subjetivo, mas como garantir conformidade e responsabilização nos dois cenários. Com isso em mente, o próximo capítulo é dedicado a uma análise prática e indicação de quais etapas devem ser adotadas para esse propósito.

- 114 BIONI, Bruno (2019), “Proteção de dados pessoais: A função e os limites do consentimento”, Forense, p. 319.
- 115 ICO (2019), “Guidance on political campaigning: Draft framework code for consultation”, <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>. Acessado em dezembro de 2019.
- 116 Comissão Europeia (2018), “Commission guidance on the application of Union data protection law in the electoral context: A contribution from the European Commission to the Leaders’ meeting in Salzburg”, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf, acessado em janeiro de 2019.
- 117 HEWARD-MILLS, D (2019), “The DPO must be independent, but how?”, <https://iapp.org/news/a/the-dpo-must-be-independent-but-how/>, acessado em novembro de 2019.
- 118 Na seção a seguir, serão descritas etapas mais práticas para a função de encarregado da proteção de dados.
- 119 CNIL (2019), “Devenir délégué à la protection des données”, <https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees>, acessado em novembro de 2019.
- 120 EDPB (2019), “Guidelines on Data Protection Impact Assessment (DPIA)”, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, acessado em novembro de 2019.
- 121 ICO (2019), “How do we apply legitimate interests in practice?”, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/>. Leia também <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>, acessado em novembro de 2019.
- 122 Britto, Cruz et al. (2019), “Internet e eleições no Brasil: Diagnósticos e recomendações”, InternetLab, pp. 32–33.
- 123 Art. 5, I, b, do RGPD.
- 124 ICO (2019), “Guidance on political campaigning: Draft framework code for consultation”, <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>. Acessado em dezembro de 2019.
- 125 Leia “WhatsApp Admits Illegal Mass Messaging Used in Brazil’s 2018 Elections”, The Rio Times, <https://rio-timesonline.com/brazil-news/brazil/whatsapp-admits-to-illegal-mass>, acessado em novembro de 2019.
- 126 O preâmbulo nº 71 do RGPD define definição de perfis como “qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar.”.
- 127 REVELL, T. (2018), “How Facebook let a friend pass my data to Cambridge Analytica”, <https://www.news-scientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica/>, acessado em novembro de 2019.
- 128 ICO (2019), “Guidance on political campaigning: Draft framework code for consultation”, <https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf>, acessado em dezembro de 2019.
- 129 Preâmbulo 56: “Sempre que, no âmbito do exercício de atividades eleitorais, o funcionamento do sistema democrático num Estado-Membro exigir que os partidos políticos recolham dados pessoais sobre a opinião política dos cidadãos, o tratamento desses dados pode ser autorizado por motivos de interesse público, desde que sejam estabelecidas garantias adequadas.”
- 130 Art. 33.º: “Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo Artigo 55.º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.”



3. Aumentar a eficácia e preencher as lacunas

A importância de manter a higiene e a conformidade dos dados nas campanhas eleitorais é múltipla. Da perspectiva das instituições democráticas, como discutido anteriormente, é uma condição para processos eleitorais saudáveis. Em um tempo de conexão onipresente, de compartilhamento instantâneo e indiscriminado de dados, ideias e crenças podem ser moldadas por filtros on-line e a esfera pública se torna necessariamente interligada com as novas tecnologias de informação e comunicação. Falha no funcionamento, seja por erro ou em consequência de um sistema estruturalmente defeituoso, pode colocar em risco a capacidade das pessoas de gerar consenso e encontrar um meio termo de maneira pacífica e equilibrada, como demonstrado recentemente pela interferência nos processos eleitorais em várias partes do mundo.¹³¹

Do ponto de vista dos controladores de dados e, neste caso específico de partidos políticos e políticos, seguir as regras com precisão não é apenas uma obrigação legal, mas deve ser um requisito básico para se apresentar à sociedade como uma pessoa ética que merece atenção, confiança e voto. Isso se torna ainda mais verdadeiro, levando em conta os casos recentes em que técnicas de tratamento de dados foram aplicadas a campanhas eleitorais, como no caso da CA e do WhatsApp nas eleições brasileiras, trazendo a questão à tona e aumentando a atenção dos eleitores. Não respeitar a privacidade, o direito à proteção de dados e o direito à autodeterminação informativa das pessoas deve ser cada vez mais injustificável em marketing e imagem pública, especialmente à medida que mais e mais pessoas se conscientizam sobre essas questões.

Candidatos e partidos políticos devem ter cuidado com a maneira como processam dados para suas campanhas durante os processos eleitorais, buscando as melhores práticas atuais, não apenas em seu próprio interesse, mas também no interesse dos titulares de dados e da sociedade como um todo.¹³² Devido à própria natureza desses processos, muitos dos dados pessoais com os quais eles lidam, coletados diretamente ou inferidos por meio de técnicas de análise e definição de perfis, são sensíveis (uma categoria especial de dados que merece proteção diferenciada). Não só é importante garantir a observância de direitos e princípios no interesse dos titulares dos dados, observando o estado de direito, mas também é crucial ser capaz de demonstrar que a privacidade e a proteção de dados estão sendo tratadas da maneira mais ética e legal, especialmente em termos de campanhas eleitorais, onde a imagem pública é um componente primordial.

O aumento de violações de dados atingiu seu ponto alto em 2019, com 5.183 violações de dados e 7,9 bilhões de registros expostos nos primeiros nove meses do ano. Isso representa um aumento de 33,3 % em comparação a 2018¹³³. Se isso for uma indicação das tendências futuras, então a segurança dos dados deveria ser uma das principais preocupações em qualquer iniciativa de tratamento de dados pessoais. As sanções por violações de dados podem chegar a dezenas de milhões de dólares em multas, além de suspensão ou exclusão de ativos. Para evitar tais perdas, o controlador deve seguir as mais recentes normas de segurança. Por exemplo, oferecer treinamento adequado a todas as pessoas envolvidas no tratamento, bem como reduzir o número de pessoas que têm acesso a dados pessoais, são etapas importantes. A autenticação multifatorial também é um requisito básico, pois tem o potencial de reduzir drasticamente as vulnerabilidades do sistema¹³⁴. Reduzir o número de dispositivos onde os dados são armazenados e a transmissão de dados entre dispositivos

são outras duas etapas para maior segurança que os controladores podem e devem executar, preferencialmente por meio de um Diretor de Segurança da Informação (em inglês, Chief Information Security Officer – CISO), que não deve ser a mesma pessoa que o encarregado da proteção de dados/encarregado¹³⁵.

O encarregado da proteção de dados/encarregado tem um papel de liderança para garantir que todo esse sistema esteja funcionando. É de responsabilidade do encarregado da proteção de dados/encarregado acompanhar a conformidade com a legislação de proteção de dados. Isso significa coletar informações sobre onde os dados são tratados e garantir que eles sigam todos os requisitos legais; fornecer aconselhamento ao responsável pelo tratamento/controlador com base em suas observações a respeito de como a conformidade pode ser melhorada; capacitar funcionários quanto às medidas de segurança e práticas recomendadas; e estabelecer um vínculo entre a organização, a autoridade e os titulares dos dados. Essa última atribuição significa que o encarregado da proteção de dados/encarregado deve ser independente, o que pode ser difícil quando contratados internamente.

A prática recomendada é o encarregado da proteção de dados/encarregado não responder ao responsável pelo tratamento/controlador, mas, em vez disso, ser subordinado direto do nível mais alto de tomada de decisão da estrutura de gestão. Para garantir sua independência, eles também devem ter os recursos necessários (pessoal, equipamento e finanças) ao desempenho de suas funções¹³⁶. Por fim, eles não devem ser colocados em uma posição de conflito de interesses, como trabalhar ou ter trabalhado em atividades de tratamento de dados (departamentos de TI ou RH, por exemplo) que os obrigasse a supervisionar a si mesmos¹³⁷. Esses problemas podem ser evitados com a contratação de um encarregado da proteção de dados/encarregado externo. Mesmo assim, é importante que o encarregado da proteção de dados/encarregado possua o acesso, os recursos e os conhecimentos técnicos necessários.

Tudo isso são componentes de uma estratégia de tratamento e segurança de dados que começa com uma avaliação direta do fluxo de dados ao longo de uma operação e dos riscos atuais envolvidos. Para garantir a conformidade com o RGPD e, consequentemente, com a LGPD, já que ambos têm níveis muito semelhantes de proteção de dados, partidos políticos e candidatos devem estar atualizados sobre as práticas recomendadas e ferramentas de gerenciamento aplicadas aos fluxos de dados.

Um responsável pelo tratamento/controlador deve ser capaz de ter uma visão panorâmica dos fluxos de dados pessoais em sua campanha, de preferência por meio de um painel de conformidade que deve ser usado por todos os responsáveis pelo tratamento/controladores e subcontratantes/operadores envolvidos. Esse sistema centralizado de gerenciamento de dados também deve fornecer detalhes de contato e identificar o encarregado da proteção de dados/encarregado na estrutura da campanha, um mapeamento e controle completos dos dados que estão sendo tratados e transferidos e seu propósito legal associado.

Também é necessário lembrar seus deveres de informação de acordo com o RGPD e a LGPD, inclusive informando: (i) identidade e detalhes de contato do responsável pelo tratamento/controlador e do encarregado da proteção de dados/encarregado; (ii) iden-

tificação ou categorias de destinatários dos dados; (iii) os propósitos do tratamento, bem como a base jurídica para realizá-lo; (iv) o período no qual o tratamento será realizado; (v) os direitos do titular dos dados, especialmente de retificação e retirada de consentimento, quando aplicável; entre outros¹³⁸. Além disso, os responsáveis pelo tratamento/controladores devem ser capazes de processar as solicitações de acesso do titular em tempo hábil. Essas solicitações são instâncias em que os titulares dos dados podem exigir acesso, retificação e, em alguns casos, exclusão de seus dados.

O responsável pelo tratamento/controlador também deve adotar meios de manter “rastros do consentimento digital”, ou seja, um registro da linha do tempo do consentimento, ou consentimentos distintos, que um indivíduo tenha dado (ou retirado) para tratamento. Finalmente, a permissão e o controle de acesso devem ser granulares, o que significa que apenas os agentes indispensáveis na estrutura da campanha devem ter acesso aos respectivos grupos de dados. Todos esses aspectos do relacionamento entre o subcontratante/operador e o titular dos dados devem ser traduzidos em interfaces fáceis de usar, como aplicativos e formulários, para que o titular compreenda amplamente seus direitos e o responsável pelo tratamento/controlador possa demonstrar conformidade¹³⁹.

Tudo isso pode parecer muita coisa ser abrangida, e é. Felizmente, além de profissionais capazes, que podem ajudar empresas a terem conformidade, atualmente há ferramentas de autoavaliação em relação à conformidade com o RGPD, que devem se adaptar facilmente aos requisitos da LGPD. O Information Commissioner's Office (ICO) do Reino Unido, por exemplo, possui vários recursos específicos, incluindo listas de verificação de conformidade para responsáveis pelo tratamento/controladores, subcontratantes/operadores, segurança da informação, marketing direto, pequenas e médias empresas e muito mais¹⁴⁰. Outra ferramenta inestimável é o Código de Aviso de Privacidade, que mostra em detalhes como os avisos de privacidade encontrados em sites e aplicativos, uma das ferramentas mais comuns de comunicação entre o responsável pelo tratamento/controlador e o titular dos dados, devem ser estruturados para garantir a conformidade¹⁴¹.

Um resumo dessas ferramentas demonstra que o ponto crucial de um programa eficaz de conformidade de dados pessoais é conhecer os processos envolvidos em uma operação: onde, quando, como e quais dados pessoais são coletados e tratados. Nas campanhas eleitorais, isso não deve ser diferente: é necessária uma abordagem prática, envolvendo especialistas em marketing, designers, juristas, programadores e voluntários para pensar em como proteger melhor os titulares de dados de qualquer tipo de violação ao seu direito à privacidade e proteção de dados. Conforme demonstrado neste estudo, destacando diretrizes legais específicas e situações concretas, os regulamentos de proteção de dados são totalmente aplicáveis a campanhas eleitorais e têm a capacidade de auxiliar na redução do uso instrumental de dados pessoais, além de evitar o impacto de desinformação e propaganda computacional usada para o objetivo da manipulação política.

De forma mais pragmática, as campanhas eleitorais devem seguir pelo menos as seguintes recomendações, com base nos princípios e mais importantes orientações dos regulamentos gerais de proteção de dados, sempre sob a perspectiva de legalidade, justiça, transparência e responsabilidade:¹⁴²

Identifique os atores relevantes: quem são os responsáveis pelo tratamento/controladores e os subcontratantes /operadores e quem é o encarregado da proteção de dados/encarregado, se houver um.

- › Art. 5º da LGPD; Art. 4.º do RGPD.
- › **Exemplo:** em uma determinada campanha política, o candidato contratou uma empresa de marketing para gerenciar sua imagem pública. Todas as decisões relacionadas à coleta e ao tratamento de dados são tomadas pelo diretor de marketing. O diretor pode ser caracterizado como um responsável pelo tratamento/controlador de dados, pois é capaz de decidir o objetivo do tratamento. O candidato também seria um responsável pelo tratamento/controlador, uma vez que, em última análise, é ele quem toma decisões.

Identifique como os dados estão sendo coletados e tratados, isto é, qual é o ciclo de vida dos dados no fluxo organizacional da campanha.

- › **Ação:** mapeie todos os pontos de coleta e tratamento de dados; identifique quanto tempo leva até que um único ponto de dados seja eliminado; identifique quais dispositivos/serviços são usados para armazenar dados; identifique quais terceiros têm acesso aos dados.

Identifique quais dados são coletados e tratados sob qual base jurídica. Defina quais são os dados sensíveis¹⁴³ e preste atenção especial às suas bases jurídicas.

- › Art. 5º, I, II; Art. 7º, Art. 11 da LGPD; Art. 4.º, Art. 9.º do RGPD.
- › **Ação:** se houver pontos de dados em que uma base jurídica não possa ser especificada, eles deverão ser eliminados, pois são um passivo exigível – isso é “higiene de dados” básica.

Lembre-se de que a minimização de dados¹⁴⁴ é uma boa regra geral (e um princípio básico). Se não houver necessidade de coletar um determinado aspecto dos dados pessoais, não o faça; se o propósito da coleta for alcançado, exclua os dados.

- › Art. 15º, Art. 16 doº da LGPD; Art. 5.º, Art. 25.º RGPD.
- › **Ação:** se não houver necessidade de coletar um determinado aspecto dos dados pessoais, não o faça; se o propósito da coleta for alcançado, exclua os dados.
- › **Exemplo:** o candidato coleta dados de indivíduos para enviar cópia digital do plano de governo. Se for dado consentimento estritamente para a distribuição do referido material: 1. o candidato não precisa coletar mais do que o nome e o endereço de e-mail do titular; portanto, ele deve se ater a isso; 2. o candidato deve eliminar os dados após o envio do material, a menos que seja razoável esperar o contrário com o amparo de outras bases jurídicas ou através de um novo consentimento específico.

Mantenha toda a documentação das bases jurídicas arquivada.

- › **Exemplo:** o candidato coletou e processou dados para manter um registro de doações de campanhas individuais, conforme a lei eleitoral brasileira. O candidato deve manter um registro dessas operações com referência às leis e bases jurídicas pertinentes, para o caso de uma auditoria.

Renove o consentimento existente em conformidade com os regulamentos de proteção de dados mais atualizados.

- **Ação:** no caso de um novo texto da política de privacidade, ou em relação a titulares de dados anteriores ao RGPD/LGPD, obtenha novo consentimento ou informe os titulares sobre a nova política e base jurídica.
- **Exemplo:** o candidato já possui uma lista de contatos coletada antes do RGPD/LGPD em eventos públicos e formulários de associação na página da Web. Eles devem enviar a todos os destinatários uma solicitação para confirmar seu desejo de receber comunicações políticas. Algo como “Estamos atualizando nossas práticas de privacidade e proteção de dados de acordo com os regulamentos de dados mais recentes. Se você deseja continuar recebendo nosso conteúdo, clique no botão abaixo/renove sua assinatura em/[adicione alguma forma de confirmação]”.

Forneça informações: lembre-se dos vários deveres de informação que um responsável pelo tratamento/controlador possui em relação ao titular dos dados. O titular dos dados deve ser capaz de discernir quais dados pessoais estão sendo coletados, com que propósito, em que período de tempo, quem terá acesso a eles, qual é o processo para solicitar acesso a esses dados, para corrigi-los, para solicitar sua exclusão ou para transferi-los para outro responsável pelo tratamento/controlador, etc.

- Art. 9º, Art. 18º do LGPD; Art. 13º, Art. 14º do RGPD.
- **Ação:** se o consentimento for a base jurídica, todas as informações pertinentes deverão ser fornecidas no ato do consentimento. Se houver outras bases jurídicas, o titular dos dados deve ter acesso fácil a essas informações por solicitação ou por acesso público [por exemplo, em um site]. Se os dados forem coletados por outros meios que não seja diretamente do titular [por exemplo, dados acessíveis ao público], o responsável pelo tratamento/controlador terá uma série de deveres de informação [ver artigos pertinentes do RGPD].

Mantenha um registro das atividades de tratamento, especialmente se a base jurídica for o interesse legítimo (Art. 30º do RGPD; Art. 37º da LGDP). Quando aplicável, tenha uma AIPD¹⁴⁵ ou LIA¹⁴⁶ em mãos.

- Art. 37º da LGPD; Art. 30º do RGPD.
- **Ação:** mantenha um registro contendo pelo menos: 1. o propósito do tratamento; 2. descrição das categorias de dados e titulares; 3. fluxos de dados externos; 4. medidas de segurança adotadas; 5. identificação e informações de contato do responsável pelo tratamento/controlador; 6. prazos para eliminação de cada categoria de dados¹⁴⁷.
- **Exemplo:** uma pequena campanha em uma eleição local adotou um fluxo organizacional para manter um registro das atividades de tratamento de dados. Todas as informações coletadas sobre os titulares dos dados são registradas em uma planilha com categorias de acordo com a fonte dos dados. Dados de formulários de associação, por exemplo, são categorizados como baseados em consentimento, contendo nome e endereço de e-mail, enviados para um serviço de boletim informativo de terceiros, guardados em um servidor restrito na nuvem, protegido com autenticação de dois fatores, e mantidos indefinidamente, conforme acordado pelos titulares dos dados quando eles deram o seu consentimento.

Informe aos titulares dos dados quem é seu encarregado da proteção de dados/ encarregado, se houver, e forneça a eles um canal de comunicação fácil para solicitações de acesso do titular.

- Art. 18º da LGDP; Art. 12.º do RGPD.
- **Exemplo:** uma campanha possui, em seu site, um formulário para contato direto com o encarregado da proteção de dados/encarregado. Ele também inclui campos específicos para solicitações de acesso do titular, que são priorizadas.

Verifique se o idioma e o design de suas plataformas são adequados para o entendimento ideal dos titulares de dados.

- **Ação:** adote tipografia adequada [tamanho, cor, contraste, tipo etc.], idioma, dicas visuais, ilustração e qualquer outro meio para obter o entendimento ideal, considerando as capacidades específicas do leitor.
- **Exemplo:** uma campanha contratou uma equipe de especialistas jurídicos, profissionais de marketing e web designers que trabalharão juntos na criação de um documento de política de privacidade que contenha não apenas o idioma legal necessário, mas também conteúdo explicativo e simplificado que pessoas de fora da área jurídica sejam capazes de entender.

Informe os usuários sobre sua política de privacidade e quaisquer atualizações subsequentes.

- **Ação:** informe os indivíduos sobre o tratamento que será feito com seus dados, incluindo transferências para terceiros, especificando quem são esses terceiros, ou, pelo menos, suas categorias, e o período durante o qual os dados serão mantidos.
- **Ação:** seja o mais específico possível, pois nenhum dos dois regulamentos reconhece permissões gerais.
- **Exemplo:** uma campanha sabe que usará o Google Analytics em seu site. Além disso, seu site foi feito usando um criador de sites do tipo “arrastar e soltar”, como o Wix ou o Squarespace. Todas essas plataformas coletam dados do usuário, e isso deve ser mencionado para os titulares dos dados.

Gerencie o consentimento: sempre que a base jurídica for o consentimento, verifique se ele foi fornecido sob condições apropriadas. Isso exige uma abordagem multidisciplinar, do Jurídico à TI, passando pelo Design¹⁴⁸, para garantir que o consentimento seja específico, informado, dado livremente e sem ambiguidade.

- **Ação:** solicite permissão para coletar cookies e outras informações de identificação explicitamente [exceto se houver outra base jurídica razoável para a coleta]¹⁴⁹.
- **Exemplo:** o candidato possui um formulário de associação para recebimento de um boletim informativo político no site de sua campanha, o qual coleta cookies. Ele possui uma caixa pré-marcada indicando consentimento para receber o boletim. Isso não é considerado consentimento válido e a caixa não deve ser pré-marcada. Além disso, ele possui um aviso de “consentimento presumido pelo uso deste site” para cookies. Isso também não é considerado consentimento válido¹⁵⁰. A melhor prática seria um aviso informativo que permita ao usuário escolher quais tipos de cookies ele permite e explique quais são necessários para o funcionamento do site; e que exija o consentimento ativo do usuário, ou seja, uma ação que reflita seu consentimento.

Preste atenção especial aos dados de crianças e aos dados de categoria especial (sensíveis), que possuem regulamentos mais rígidos.

- Art. 11º, Art. 14º da LGPD; Art. 8º, Art. 9º do RGPD.
- **Ação:** no caso de crianças, o consentimento deve ser específico e destacado e dado pelos pais ou representantes legais [há especificação de idade no RGPD, consulte o artigo pertinente]. As bases jurídicas para o tratamento de dados sensíveis são mais restritivas [consulte artigos pertinentes].

Observe a portabilidade: verifique se os dados estão em um formato que permita a portabilidade. Este é um direito do titular dos dados, tanto na LGPD quanto no RGPD. Os titulares dos dados devem poder obter seus dados “num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir” (Art. 20º do RGPD).

- Art. 18º da LGPD; Art. 20º do RGPD.

Defina as obrigações do subcontratante/operador: qualquer subcontratante/operador contratado ou designado por um responsável pelo tratamento/controlador deve ter um contrato de tratamento de dados¹⁵¹ que defina suas responsabilidades, padrões de segurança e outros requisitos legais¹⁵².

- Art. 28º do RGPD.
- **Ação:** tenha um contrato de tratamento de dados em vigor determinando responsabilidades e padrões de segurança.

Verifique se os seus provedores de serviços estão em conformidade e gerenciam dados de maneira segura, e se os dados estão armazenados em um servidor localizado em um país que cumpra os regulamentos de proteção de dados mais atualizados.

- **Ação:** verifique se os dados manipulados por esses terceiros estão armazenados em países com status equivalente em termos de proteção de dados. A UE possui um sistema que classifica as legislações dos países como equivalentes ou não.
- **Ação:** peça à sua equipe jurídica que leia com atenção os termos de uso de qualquer serviço de terceiros que você utilize para gerenciar dados pessoais e analise sua conformidade com o RGPD/a LGPD.
- **Exemplo:** a campanha decide coletar dados usando o Google Analytics, exibir anúncios usando a plataforma de anúncios nativa do Facebook, enviar e-mails pelo Mailchimp e gerenciar fluxos internos usando uma solução tecnológica indiana. Eles precisam garantir que cada um desses provedores esteja em conformidade com as leis de proteção de dados, pois eles terão acesso, mesmo que momentaneamente, aos dados pessoais coletados e tratados. No caso da solução tecnológica indiana, se os dados estiverem armazenados em um servidor na Índia, a campanha deve confirmar se a UE reconheceu a conformidade da Índia com o RGPD (em dezembro de 2019, o país estava buscando o status, mas ainda não o havia obtido).

Gerenciamento de violações: deve haver um processo para identificar e notificar a autoridade e os titulares dos dados sobre violações.

- › Art. 48º da LGPD; Art. 33.º do RGPD.
- › **Ação:** assegure que as violações de segurança sejam notificadas à Autoridade Nacional sem demora injustificada (em até 72 horas, de acordo com o RGPD). A notificação aos titulares dos dados é obrigatória apenas na LGPD. No RGPD, ela é necessária apenas se houver um risco substancial aos direitos e liberdades dos titulares.
- › **Exemplo:** a campanha possui uma equipe de segurança voltada a encontrar bugs e falhas no projeto e nas funções de todas as atividades de tratamento de dados. Ela também treinou todo o pessoal pertinente sobre como reagir a uma violação, incluindo quais informações devem ser relatadas à autoridade, através de quais canais e como se comunicar com o público.

Gerenciamento de riscos de segurança:

- › Art. 46º da LGPD; Art. 32.º do RGPD.
- › **Ações:** minimize a transferência de dados entre dispositivos; Criptografe, pseudonimize ou anonimize os dados sempre que possível; tenha uma política de segurança interna em vigor; treine os membros da equipe em questões de segurança; tenha uma política de senha de segurança obrigatória e autenticação multifatorial¹⁵³; realize uma avaliação de risco da infraestrutura usada para coletar, tratar e armazenar os dados.
- › Conformidade como um processo: A proteção de dados não termina quando um responsável pelo tratamento/controlador escreve uma AIPD ou fornece aos titulares de dados informações sobre suas políticas de privacidade. Ela deve ser constantemente monitorada, revisada, atualizada e adaptada aos contextos de tratamento de dados e aos avanços tecnológicos mais recentes.

Tudo isso são pontos acionáveis direcionados aos responsáveis pelo tratamento/controladores de dados e suas operações de tratamento. No entanto, um paradigma completo de proteção de dados só pode ser alcançado através do envolvimento de muitos atores. Isso significa cuidadosa regulamentação e orientação das autoridades nacionais – especialmente no caso do Brasil, onde a lei deixou muita coisa a critério da Autoridade de Proteção de Dados, que é quem decidirá sobre padrões de segurança, casos que exigem uma AIPD e regimes especiais para pequenas e médias empresas, entre outros assuntos. Também significa um esforço ativo do Judiciário para adaptar sua compreensão aos princípios e espírito da lei, interpretando casos difíceis e dando vida a esses princípios tendo a proteção dos titulares de dados em mente.

Essa iniciativa de fortalecer os regulamentos já começou na Europa e, em matéria de campanha política, é interessante observar os debates jurídicos que surgiram logo após a entrada em vigor do RGPD, relacionada ao preâmbulo 56 do regulamento. O preâmbulo especifica a interpretação relativa ao tratamento de dados pessoais para atividades eleitorais. Em suas palavras¹⁵⁴:

Sempre que, no âmbito do exercício de atividades eleitorais, o funcionamento do sistema democrático num Estado-Membro exigir que os partidos políticos recolham dados pessoais sobre a opinião política dos cidadãos, o tratamento desses dados pode ser autorizado por motivos de interesse público, desde que sejam estabelecidas garantias adequadas.

Os esforços legislativos subsequentes em alguns Estados-Membros, tendo em conta o preâmbulo, colocaram em primeiro plano uma discussão sobre os limites do tratamento em tais casos. A Espanha e a Romênia introduziram em suas legislações nacionais bases para o tratamento de dados pessoais em campanhas eleitorais fundamentadas na interpretação do interesse público. Na Romênia, isso significou uma isenção de consentimento no tratamento de dados pessoais para fins eleitorais, permitindo, por exemplo, que os Correios da Romênia fechassem um acordo com o Partido Social Democrata do país para entregar material de campanha política às populações-alvo, usando os dados dos Correios sobre idosos aposentados¹⁵⁵.

De forma semelhante, na Espanha, uma lei nacional permitiu que os partidos políticos coletassem dados pessoais de fontes disponíveis ao público, como redes sociais, e os utilizasse para a definição de perfis de eleitores. A disposição modifica a lei eleitoral espanhola para acrescentar o artigo 58 bis, que diz¹⁵⁶:

Artigo 58 bis. Uso de ferramentas tecnológicas e dados pessoais nas atividades eleitorais.

1. A coleta de dados pessoais relacionados às opiniões políticas das pessoas, realizada pelos partidos políticos em suas atividades eleitorais, deve estar coberta pelo interesse público somente quando houver garantias adequadas.
2. Partidos políticos, coalizões e grupos eleitorais poderão utilizar dados pessoais obtidos através de páginas da web e outras fontes de acesso público para atividades eleitorais durante o período eleitoral.
3. O envio de propaganda eleitoral por meios eletrônicos ou sistemas de mensagens e a contratação de propaganda eleitoral em redes sociais ou plataformas equivalentes não serão consideradas atividades de comunicação comercial.
4. As atividades publicitárias acima mencionadas identificarão claramente sua natureza eleitoral.
5. O destinatário terá um meio simples e gratuito de exercer seu direito de contestação.

Na prática, os termos da lei espanhola poderiam ser interpretados como mais brandos na proteção de dados pessoais – nesse caso, a categoria especial de dados de opiniões políticas, que é o assunto específico do preâmbulo. O preâmbulo 56 deve ser interpretado como uma especificação do Artigo 9.º do RGPD, que, no n.º 2, alínea g), trata do tratamento “necessário por motivos de interesse público importante”. Assim, os termos do preâmbulo e, especialmente, do artigo devem ser respeitados ao implementar tal disposição na legislação nacional.

O preâmbulo 56 exige que a compilação desses dados de opinião política seja necessária para “o funcionamento do sistema democrático num Estado-Membro” e esteja coberta por “garantias adequadas”. A alínea g) do n.º 2 do Artigo 9.º é mais rigorosa, mencionando a necessidade de interesse público “importante”, bem como o tratamento proporcional aos objetivos buscados, cobertos pela “essência do direito à proteção dos dados pessoais” e estabelecendo “medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados”¹⁵⁷.

A falha na lei espanhola, conforme reconhecido pela Suprema Corte do país em um caso apresentado em março de 2019, foi não estabelecer “medidas adequadas e específicas” nem “interesse público importante”¹⁵⁸.

Na prática, a lei corria o risco de permitir o tratamento indiscriminado de dados sensíveis, em violação direta ao RGPD, e de expor os cidadãos a práticas semelhantes às realizadas no escândalo da Cambridge Analytica. Nesse ponto, diante de tais controvérsias sobre o uso de dados pessoais sensíveis em campanhas eleitorais, o Comitê Europeu de Proteção de Dados (CEPD) publicou, em março de 2019, a “Declaração 2/2019 relativa à utilização de dados pessoais no decurso de campanhas políticas”¹⁵⁹. A declaração traz cinco recomendações e esclarecimentos concretos aos Estados-Membros:

- I. *que os dados pessoais que revelem opiniões políticas são uma categoria especial de dados e, portanto, seu tratamento é proibido e permitido apenas em exceções estritamente interpretadas;*
- II. *os dados que foram disponibilizados ao público pelos titulares ainda estão de acordo com a lei de proteção de dados da UE e devem ser tratados de maneira a respeitar as obrigações relativas à transparência, especificação de propósito e legalidade;*
- III. *mesmo quando legal, o tratamento ainda está sujeito a todas as outras obrigações legais, e os partidos políticos devem estar preparados para fornecer as informações necessárias para responsabilização e transparência;*
- IV. *a tomada de decisão exclusivamente automatizada, incluindo definição de perfis, em que a decisão afete o titular legalmente ou de maneira semelhante, é restrita – o CEPD interpreta afetar o voto de uma pessoa como “afetar legalmente” o titular; e*
- V. *em relação à segmentação, o titular tem o direito de saber quem está enviando o conteúdo segmentado e por quê e quais direitos ele tem em face de tal atividade.*

Através destas recomendações, o CEPD fornece aos legisladores dos Estados-Membros orientações claras sobre a interpretação da alínea g) do n.º 2 do Artigo 9.º e do Preâmbulo 56 sobre processos eleitorais. Isso é crucial, pois uma aplicação incompleta das garantias e requisitos exigidos pelo regulamento pode produzir situações que vão diretamente contra o espírito da lei, como visto nos casos comentados anteriormente. Nesse sentido, é interessante contrastar os casos espanhol e romeno com as abordagens adotadas por Itália e França. Na Itália, os dados pessoais disponibilizados ao público na Internet não podem ser usados para comunicações políticas, exceto se originalmente tornados públicos para esse fim, conforme determinado pela Autoridade de Proteção de Dados do país em 2014. Na França, uma atualização de 2016 das recomendações para comunicação política da Comissão Nacional de Proteção de Dados da França (CNIL), de 2012, exige consentimento específico para agregação e definição de perfis legais dos dados pessoais dos eleitores¹⁶⁰.

O responsável pelo tratamento/controlador deve sempre ter em mente que o foco das leis de proteção de dados são o titular e seus direitos, criando um sistema facilitador para práticas comerciais e inovações em torno dos dados, mas dentro dos limites de privacidade e proteção de dados, garantias profundamente enraizadas na direitos da personalidade e dignidade humana. Portanto, práticas comuns em um cenário pré-regulamentação da proteção de dados, como compra de listas de corretores de dados e definição de perfis de indivíduos indiscriminadamente, inclusive para fins eleitorais¹⁶¹, devem ser evitadas sob esse novo paradigma. Além disso, como afirmado

anteriormente, a proteção de dados pessoais tem um impacto direto na qualidade dos processos eleitorais, uma vez que esses dados são necessários para a psicometria e outras técnicas que, quando aplicadas às campanhas eleitorais, têm um efeito real nos resultados eleitorais.

Na Europa e no Brasil, as autoridades estão se conscientizando desse risco, conforme demonstrado pelas ações do CEPD para harmonizar as legislações nacionais e uma interpretação adequada do preâmbulo 56; e no Brasil, onde recentemente o Tribunal Superior Eleitoral incluiu no mais recente esboço do regulamento das próximas eleições municipais termos que visam coibir a disseminação de desinformação, especialmente por meio de mídias sociais e aplicativos digitais.

A harmonização dos regulamentos gerais de proteção de dados com as resoluções eleitorais, bem como a conformidade no tratamento de informações, deve ser vista como uma prioridade, com a capacidade de garantir mecanismos eficazes contra o uso indevido de dados pessoais em períodos eleitorais, ajudando a promover um ambiente eleitoral justo.

-
- 131 Do ponto de vista dos titulares dos dados, os novos regulamentos de proteção de dados parecem obviamente benéficos, pois visam aumentar a autonomia dos titulares dos dados. No entanto, ser autônomo carrega a responsabilidade de ser autossobrerano sobre a própria identidade. Isso enriquece a liberdade, além de exigir uma mudança fundamental na maneira como as pessoas veem sua relação com os controladores de dados, os serviços e produtos que eles oferecem e, finalmente, como entendem que a economia e a sociedade de dados deveriam ser.
- 132 Embora os regulamentos gerais de proteção de dados já sejam aplicáveis em muitos países, muitos tomadores de decisões políticas ainda não entendem claramente o que é permitido em termos de tratamento de dados, nem as implicações e importância desse assunto de modo geral. Portanto, a conscientização e capacitação, visando não apenas os cidadãos, mas também os tomadores de decisões políticas, é um esforço importante e contínuo que deve ser fortalecido para garantir a correta compreensão e aplicação dos regulamentos aplicáveis.
- 133 Leia Risk Based Security (2019), Data Breach QuickView Report: 2019 Q3 trends.
- 134 AMIGORENA, F. (2019), "The Myths of Multifactor Authentication. DARKReading", <https://www.darkreading.com/endpoint/authentication/the-myths-of-multifactor-authentication/a/d-id/1336262>.
- 135 GDPR Informer (2017), "Data Security 101: Access Controls & Planning", <https://gdprinformer.com/gdpr-articles/data-security-101-access-controls-planning>.
- 136 HEWARD-MILLS, D. (2019), "The DPO must be independent, but how?", <https://iapp.org/news/a/the-dpo-must-be-independent-but-how/>, acessado em novembro de 2019.
- 137 Leia GDPR-Info, <https://gdpr-info.eu/issues/data-protection-officer/>, acessado em novembro de 2019.
- 138 Leia o Art. 13.º do RGPD e os Art. 9º e 18º da LGPD.
- 139 FINUCANE, B. (2018), "A Post-GDPR Checklist for Political Parties", CPO Magazine, <https://www.cpomagazine.com/data-protection/a-post-gdpr-checklist-for-political-parties/>, acessado em novembro de 2019.
- 140 Encontre uma lista de verificações aqui: <<https://ico.org.uk/for-organisations/data-protection-self-assessment/>>.
- 141 Encontre o código aqui: <<https://www.pdpjournals.com/docs/88625.pdf>>.
- 142 Essa lista é baseada principalmente nos recursos citados anteriormente, como as listas de verificação do ICO e a lista de verificação de Finucane para partidos políticos. Também reflete os termos do RGPD ou da LGPD e a análise do autor de ambos os documentos legais. Onde foram consultadas outras fontes, elas deverão ser indicadas em uma nota de rodapé.
- 143 Os "dados de categoria especial" do RGPD são chamados de "dados sensíveis" na LGPD.
- 144 ICO, (2019), "Principle (c): Data minimization", <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>, acessado em novembro de 2019.
- 145 O ICO forneceu um modelo de AIPD aqui: <https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf>.

3. Aumentar a eficácia e preencher as lacunas

- 146 O ICO recomenda a realização de uma avaliação de interesse legítimo sempre que depender do interesse legítimo para o tratamento de dados. Isso contribui para haver responsabilização e transparência, e é uma garantia para a empresa no caso de uma auditoria. A LIA abrange os três aspectos principais da base de interesse legítimo, ou seja, propósito, necessidade e o equilíbrio entre esses interesses e os interesses, direitos ou liberdades do titular. Para mais informações sobre a LIA, e um modelo de LIA, leia <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/>, acessado em janeiro de 2020.
- 147 BIONI, Bruno (2019), “A obrigação de registro das atividades de tratamento de dados”, GEN Jurídico, <http://genjuridico.com.br/2019/08/27/registro-tratamento-de-dados/>, acessado em dezembro de 2019.
- 148 ICO (2019), “Privacy notices, transparency, and control: Data protection: a code of practice on communicating privacy information to individuals”, <https://www.pdpjournals.com/docs/88625.pdf>, acessado em novembro de 2019.
- 149 USTARAN, Eduardo (2019), “Getting cookie consent right”, Infolaw, <https://www.infolaw.co.uk/newsletter/2019/11/getting-cookie-consent-right/>, acessado em dezembro de 2019.
- 150 Tribunal de Justiça da União Europeia (2019), “Acórdão do Tribunal de Justiça (Grande Secção) de 1 de outubro de 2019, Processo C-673/17”, <http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-673/17>, acessado em dezembro de 2019.
- 151 Leia “What is a GDPR data processing agreement?”, <https://gdpr.eu/what-is-data-processing-agreement/>, acessado em novembro de 2019.
- 152 Encontre um modelo de acordo de tratamento de dados aqui: <https://gdpr.eu/wp-content/uploads/2019/01/Data-Processing-Agreement-Template.pdf>.
- 153 RGPD.EU. Lista de verificação de conformidade: <https://gdpr.eu/checklist/>, acessado em novembro de 2019.
- 154 Preâmbulo 56. Disponível em: <<https://gdpr-info.eu/recitals/no-56/>>.
- 155 Leia <https://www.hotnews.ro/stiri-politic-23066729-exclusiv-contractul-prin-care-posta-livreaza-plantale-psd-sunt-vizati-toti-pensionarii-inclusiv-cei-care-primesc-pensia-cont-card-posta-obligat-trimita-psd-informatii-din-baza-date-pensionarii.htm>, acessado em novembro de 2019.
- 156 «Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales. 1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas. 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral. 3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial. 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral. 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»
- 157 GONZÁLEZ, E. G. (2019), “The good, the bad and the ugly: Spanish electoral system act: A tale with a happy ending. Secuoya”, <https://secuoyagroup.com/2019/06/the-good-the-bad-and-the-ugly-spanish-electoral-system-act-a-tale-with-a-happy-ending/>, acessado em dezembro de 2019.
- 158 “De lo anterior se concluye que la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. [...] La declaración de inconstitucionalidad y nulidad se basa, como se ha dicho en el fundamento jurídico anterior, en que la Ley Orgánica 3/2018 no ha fijado por sí misma, como le impone el Art. 53.1 CE, las garantías adecuadas por lo que respecta específicamente a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. Ello constituye una injerencia en el derecho fundamental a la protección de datos personales de gravedad similar a la que causaría una intromisión directa en su contenido nuclear”. Sentencia. Recurso de Inconstitucionalidad núm. 1405-2019. Disponível em: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/2019-1405STC.pdf, acessado em novembro de 2019.
- 159 Leia a Declaração 2/2019 do CEPD relativa à utilização de dados pessoais no decurso de campanhas políticas. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/ostalo/statement-22019-use-personal-data-course-political-campaigns_pt. Acessado em novembro de 2019.
- 160 Leia o parecer da Autoridade Europeia para a Proteção de Dados de 3/2018: Parecer da AEPD sobre manipulação on-line e dados pessoais. Disponível em: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf, acessado em dezembro de 2019.
- 161 Leia “Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election”, EFF, <https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election>, acessado em novembro de 2019.

Considerações finais

A cultura de hiperconectividade em que vivemos, apesar de gerar inúmeros e inquestionáveis benefícios para os cidadãos, também traz desafios significativos para as esferas democráticas. Nesse contexto, é importante prestar especial atenção à nova maneira de fazer campanha no atual mundo dos dados em que vivemos, propondo regulamentos apropriados e eficientes para garantir eleições justas.

Embora a campanha política baseada em dados não seja um fenômeno novo, as ferramentas utilizadas, a quantidade de dados acessíveis e a potencial capacidade de influenciar os eleitores representam um cenário novo e desafiador para o estado de direito.

Nos últimos anos, partidos políticos de todo o mundo investiram pesado em publicidade on-line, demonstrando o potencial de alcançar mais pessoas de maneira eficiente e segmentada. No entanto, experiências recentes, como no caso envolvendo a Cambridge Analytica e as últimas eleições no Brasil, demonstram como estratégias para a manipulação política dos eleitores através de desinformação, manipulação algorítmica, microsegmentação comportamental e bots sociais têm sido amplamente utilizadas nesse cenário. Além disso, essas estratégias são baseadas principalmente no tratamento não autorizado de dados pessoais, como observado no caso da Cambridge Analytica, na campanha eleitoral brasileira em 2018, entre outros.

Nas palavras de Colin Bennett e David Lyon:¹⁶²

Perguntas sobre o tratamento legítimo de dados pessoais no eleitorado estão no centro da resposta para cada uma dessas perguntas maiores. A condução da análise de eleitores e a microsegmentação de mensagens políticas, incluindo o envio das chamadas “fake news”, tem uma relação direta com a publicidade programática e com os algoritmos impessoais que segmentam cidadãos individualmente, muitas vezes sem seu conhecimento e consentimento. Conhecidas questões de privacidade estão sendo inseridas neste caloroso debate internacional sobre práticas democráticas e reguladores, como autoridades de proteção de dados (APDs), agora se encontram no centro de uma discussão global sobre o futuro da democracia. Assim, “no passado, privacidade e proteção de dados raramente foram questões políticas de grande importância. Agora são”

Portanto, considerando a importância que o tratamento de dados pessoais tem nesse contexto, parte dos possíveis abusos e riscos decorrentes do uso indevido pode ser mitigada pela aplicação de estruturas legais robustas para a governança de informações pessoais, como o RGPD na Europa e a recém-sancionada Lei Geral de Proteção de Dados (LGPD) brasileira, que entrará em vigor em breve.

Conforme demonstrado ao longo deste estudo, destacando diretrizes legais específicas e situações concretas, ambos os regulamentos de proteção de dados são totalmente aplicáveis a campanhas políticas e têm a capacidade de auxiliar na redução do uso instrumental de dados pessoais, além de evitar o impacto da desinformação e propaganda computacional usadas para fins de manipulação política. Portanto, uma abordagem de proteção de dados pode resumir estrategicamente outras iniciativas, por exemplo, provenientes do setor privado, ajudando a reduzir a desinformação nas campanhas eleitorais ao sancionar o tratamento ilegal de dados personalizados, servindo como um instrumento jurídico eficaz e útil no contexto atual.

Por um lado, é papel das instituições públicas, por meio de suas resoluções e sanções, reforçar o cumprimento e a eficácia das diretrizes da LGPD e do RGPD. Por outro lado, é dever dos partidos políticos cumprir os requisitos legais, tendo total responsabilidade, transparência e boa-fé no tratamento dos dados pessoais dos eleitores.

O tratamento não autorizado de dados pessoais, juntamente com técnicas de desinformação e uso injusto de bots, definição de perfis, *deepfakes*, e outros, prejudica a confiança dos eleitores e a integridade dos processos políticos, e deve ser visto pelas instituições como ameaças à democracia.

162 Bennett, C. J. & Lyon, D. (2019). Data-driven elections: implications and challenges for democratic societies. *Internet Policy Review*, 8(4).



Embora as campanhas políticas orientadas por dados não sejam um fenômeno novo por si só, as ferramentas utilizadas, a quantidade de dados disponíveis e a capacidade potencial de influenciar os eleitores representam um cenário novo e desafiador para o princípio do Estado de Direito em todo o mundo. O presente estudo explica como este desafio pode ser enfrentado e de que forma as normas legais para a proteção de dados pessoais podem desempenhar um papel aqui, usando o exemplo da estrutura legal europeia e brasileira.