

Tratamento de dados pessoais e a propaganda eleitoral na internet.

Os desafios do Direito Eleitoral no atual momento de desenvolvimento tecnológico.

Hélio Freitas de Carvalho da Silveira

Advogado. Membro consultor da Comissão de Direito Eleitoral da OAB-SP. Membro do Conselho da Escola Judiciária Eleitoral Paulista.

Marcelo Santiago de Padua Andrade

Advogado. Mestre em Direito das Relações Sociais pela PUC-SP. Membro da Comissão de Direito Eleitoral da OAB-SP.

Sumário

1. Tratamento de dados pessoais na internet no cenário mundial e no Brasil
 2. A propaganda eleitoral na internet no Brasil e o tratamento de dados dos usuários
 3. Conclusões
- Glossário
Bibliografia

O Direito Eleitoral, à semelhança do que ocorre nos dias atuais com todos os ramos do Direito, tem um grande desafio a cumprir: acompanhar a enorme velocidade das mudanças econômicas, sociais e políticas que as inovações tecnológicas trazem, compreender os impactos que elas geram nos temas que lhes são próprios e, em decorrência disso, adaptar-se a elas para seguir cumprindo seu mister constitucional de garantir isonomia nos pleitos eleitorais. Não é possível imaginar que o Direito permaneça inerte diante de mudanças profundas que aniquilam modelos econômicos e de negócios e criam novas formas de fazer circular riqueza pela sociedade.

A missão é tentar compreender as consequências de mudanças praticamente em tempo real e apresentar as melhores soluções possíveis num

paradoxal cenário em que a construção de regras (seja pelos debates legislativos, pela regulação ou por decisões judiciais) certamente terá um abreviado prazo de validade. A tecnologia vem cumprindo um papel disruptivo e em altíssima velocidade e não reconhece fronteiras ou limites na sua marcha. Já atingiu indústrias poderosas e já afeta claramente o modo como o cidadão se relaciona com a política e com as eleições.

Se a revolução industrial marcou o fim do feudalismo e o início da primeira era industrial num processo consideravelmente longo, a internet marcou o começo de uma era da informação que avança numa velocidade incrivelmente grande na mesma proporção dos espaços que abrevia. Um movimento (como uma proposição de regime político) que antes poderia levar décadas ou séculos para se iniciar, atingir seu ápice e chegar ao declínio, hoje pode ocorrer em lapso temporal muito curto exatamente porque a internet possibilita que a mesma informação esteja ao mesmo tempo em todos (ou vários) locais. E é interessante perceber, especialmente quando se fala na velocidade das ideias e das coisas no momento contemporâneo da sociedade, que já houve inclusive **revoluções dentro da revolução**, como, por exemplo, com a criação dos *smartphones* que funcionam como verdadeiras extensões dos nossos braços, deixando-nos conectados o tempo todo e expostos diuturnamente a uma grande quantidade de informações.

Ainda como um sinal de revolução dentro da revolução, pode-se mencionar também as redes sociais que, por atuarem em escala global e com uma finalidade empresarial muito clara, reforçam a necessidade de que se deixem de lado os resquícios da ideia inicial de uma internet agnóstica e ingênua (retratada, por exemplo, na Declaração de Independência do Cyberespaço de 1996, de John Perry Barlow, de caráter quase anárquico) que deveria ser um espaço livre de regulações, fora do alcance dos governos e no qual todos esta-

riam em condições de igualdade para exercerem sem embaraços sua liberdade de expressão.

Especialmente a partir do início do milênio, grandes conglomerados empresariais transformaram a internet em um negócio muito rentável: o internauta, além de consumir informação, produz conteúdo e disponibiliza (na maioria das vezes sem a clareza que a situação exigiria) seus dados pessoais. Por meio dos algoritmos e em razão da massificação do uso de buscadores e de redes sociais, essas grandes empresas que predominam no cenário da internet têm um grande poder de, inclusive, direcionar o que é visto pelo usuário. Os algoritmos, que são constantemente calibrados, têm o poder de criar *clusters* ou furar o efeito bolha das redes sociais, de forma que não é exagerado dizer que, hoje, o programador detém poder.

A internet passou a ser um espaço que carece de adequada regulação.

E não se pode mesmo duvidar do enorme poder de impactar eventos democráticos que a rede mundial de computadores apresenta. Além das denúncias de vazamento de dados, da difusão de *fake news*, há indicações de que empresas como a Cambridge Analytica teriam capacidade de, a partir do exame de *big data*, realizar uma propaganda **personalizada** e **quase irresistível** ao eleitor, por meio do *microtargeting* ou microdirecionamento da propaganda.

Bem se vê que a internet deixou de ser apenas uma grande praça pública virtual em que qualquer um poderia criticar um homem público, ou expor suas preferências políticas e eleitorais. Com o surgimento das grandes empresas, dos recursos persuasivos e do *marketing* produzido a partir das **pegadas digitais** do usuário da rede, a internet passou a ser um espaço que, especialmente do

ponto de vista do Direito Eleitoral, carece de adequada regulação.

1 Tratamento de dados pessoais na internet no cenário mundial e no Brasil

À medida que cresce o uso e o acesso à internet, cresce em igual escala a necessidade de tutelar os dados dos usuários que são coletados pelos provedores de aplicação e de acesso na internet. Os cadastros preenchidos, os registros de navegações, os *logs* feitos e os *cookies* constituem, como já dito, **pegadas digitais** que têm considerável valor de mercado porque possibilitam, quando analisados por consultorias e profissionais de marketing digital, não apenas identificar o usuário, mas também conhecer seus desejos, suas necessidades e suas preferências, inclusive políticas.

A relevância da questão do tratamento de dados pessoais (termo técnico que engloba todas as atividades de coleta, armazenamento, transmissão, análise, classificação, segmentação, organização e exclusão de dados) vem fazendo com que diversos países produzam suas Leis Gerais de Proteção de Dados Pessoais (em 2018, estima-se que cerca de 120 países do mundo já tenham suas leis) que buscam remediar, em essência, a **assimetria informacional**, que é o descompasso entre os poderes dos que tratam dados pessoais e os poderes dos titulares desses mesmos dados.

Quando se colocam os olhos sobre os arranjos normativos existentes mundo afora, é fácil perceber que existe uma diferença no trato do tema no modelo dos Estados Unidos e da União Europeia.

Nos Estados Unidos, a proteção da privacidade (*right to privacy*) é baseada primordialmente pela Quarta Emenda, que na sua origem buscava impedir mandados e buscas sem uma causa provável (*probable cause*). O que se queria com ela, portanto, era a contenção do Estado no seu avanço (físico) sobre os indivíduos. A Quarta Emenda somente

passou a reconhecer alguma proteção para os dados a partir do julgamento pela Suprema Corte do caso *Katz vs. United States*, em 1967 e, na década de 1980, já era evidente que a proteção dada por ela já era insuficiente frente às novas tecnologias.

A proteção de dados nos Estados Unidos se dá especialmente por meio de normas infraconstitucionais, tais como a *Children's Online Privacy Protection Act* (COPPA) (que regula a coleta de dados de crianças menores de 13 anos no ambiente da internet); a *Health Insurance Portability and Accountability Act* (HIPAA); a *Gramm-Leach-Bliley Act*; a *Tax Reform Act*; *The Fair Credit Reporting Act*; o *Electronic Communications Privacy Act*; além da existência de iniciativas estaduais, como a presente na Constituição do Estado da Califórnia ou de Nova Jersey.

Mas apesar de não ter o direito à proteção de dados um viés claramente jusfundamental nos Estados Unidos (na visão da maior parte da doutrina), não se pode dizer que o cidadão daquele país não tenha nenhuma proteção. Eles são protegidos pela aplicação de normas infraconstitucionais por meio de ações coletivas (*class actions*), bem como pela fiscalização do Federal Trade Commission (FTC), que incentiva a autorregulação e o uso de tecnologias em benefício da proteção de dados. O modelo dos Estados Unidos, como se percebe, encontra base em diversas normas infraconstitucionais, inexistindo uma Lei Geral de Proteção de Dados.

O modelo europeu, por sua vez, parte da premissa de que a proteção dos dados pessoais tem a natureza de um direito fundamental. A Convenção Europeia de Direitos do Homem (CEDH) de 1950 já previa o direito ao respeito à vida privada e familiar, do domicílio e de sua correspondência. O direito à privacidade como liberdade negativa, com os surgimentos dos bancos de dados e avanços da tecnologia, desenvolveu-se também para contemplar a proteção das informações pessoais coletadas.

Especialmente importantes para o debate são a Diretiva 95/46/CE (Diretiva de Proteção de Dados ou DPD) e a Diretiva 2002/58/CE, devendo ser lembrado que elas sofreram alterações após a aprovação de nova normativa geral de proteção de dados pessoais em 27 de abril de 2016 (Regulamento 2016/679), que buscou atualizar a normativa europeia de proteção de dados pessoais ao progresso da TI e da comunicação após 1995 e aos novos modelos de negócio da *digital economy*. O modelo europeu protetivo também é reforçado pela atuação de entidades administrativas fiscalizatórias e consultivas, como a Autoridade Europeia para Proteção de Dados e as autoridades nacionais existentes em diversos países sobre a matéria. Há, ainda, as normas dos países europeus, que são exemplificadas pelo Data Protection Act 1998, no Reino Unido, e pelo Bundesdatenschutzgesetz, na Alemanha.

Na Europa, como se vê, a tendência é dar à proteção dos dados um caráter de direito fundamental, com o reconhecimento de direitos aos titulares dos dados e de fortes deveres aos mantenedores dos dados a fim de favorecer a noção de autodeterminação informativa.

Já no cenário brasileiro, o tratamento/proteção de dados, a despeito de ter envergadura constitucional (art. 5º, incisos X, XI e LXXII, da Constituição Federal (CF) de 1988), tem uma proteção jurídica fragmentária para os dados pessoais e encontra-se atrasada na tarefa de conceber sua lei geral de tratamento de dados e informações pessoais, especialmente se considerarmos que vizinhos como a Argentina, Chile e Colômbia já se desincumbiram dessa tarefa.

Além do art. 5º, incisos X e XII, a CF previu no seu art. 5º, inciso LXXII, o *habeas data*, que é remédio que visa garantir ao cidadão o acesso e a retificação de seus dados pessoais existentes em bancos de dados de caráter público, conforme regulamentação da Lei nº 9.507/1997.

No plano infraconstitucional, o tratamento de dados é tangido com alguma profundidade pelos arts. 43 e 44 do Código de Defesa do Consumidor (CDC) (Lei nº 8.078/1990), que objetivou proteger as pessoas em face dos bancos de dados criados notadamente com a finalidade específica de proteção de crédito. O Código Civil destinou apenas o art. 21 à disciplina do direito à privacidade e ignorou a proteção de dados pessoais, que foi abordada pela Lei nº 12.414/2011 (Lei do Cadastro Positivo), pela Lei nº 12.527/2011 (Lei de Acesso à Informação) e ainda pela Lei nº 12.964/2014 (Marco Civil da Internet).

Na Europa, a tendência é dar à proteção dos dados um caráter de direito fundamental.

Tramita no Congresso Nacional o Projeto de Lei nº 5.276/2016, que pretende ser uma Lei Geral de Proteção de Dados Pessoais. A conclusão e o sucesso da tramitação do projeto de lei, contudo, são incertos especialmente se for considerado que existem interesses que podem ser contrariados com a adoção de um modelo normativo muito semelhante ao da União Europeia e já reproduzido por países vizinhos da América do Sul.

2 A propaganda eleitoral na internet no Brasil e o tratamento de dados dos usuários

A todo ano, é perceptível o aumento do protagonismo da internet nos debates políticos e eleitorais pelo mundo. Com relação às eleições presidenciais norte-americanas de 2016, discute-se o grau de eficácia da estratégia da campanha vitoriosa de Donald Trump de fazer uso massivo de *microtargeting* pelas análises da empresa Cambridge Analytica. A mesma empresa também teria tido protagonismo no referendo do Brexit, também ocorrido em 2016,

embora até hoje não seja conhecida a extensão de seu envolvimento com a Leave.EU (a campanha mais radical pelo Brexit).

Empresas como a Cambridge Analytica servem-se do *big data*, que é um conjunto enorme de dados decorrentes dos registros de tudo o que uma pessoa faz *on-line* ou *off-line*, tais como suas compras, usos de cartão de crédito, pesquisas em buscadores, localizações por GPS capturadas por seu *smartphone* e sua atuação em redes sociais. E de posse dessas informações, há o emprego da **psicometria**, que é uma técnica (criada na década de 1980) que busca medir traços psicológicos de um indivíduo, como sua personalidade, por meio de um modelo chamado *Big Five* ou *Ocean*, que analisa cinco características do eleitor:

openness (abertura): abertura da pessoa a novas experiências;

conscientiousness (nível de consciência): preocupação da pessoa com organização e eficiência;

extroversion (extroversão): nível de sociabilidade e tendência de ver as coisas por uma perspectiva positiva;

agreeableness (amabilidade): cooperação e sensibilidade com questões de outras pessoas;

neuroticism (instabilidade emocional ou neurose): intensidade emocional com que a pessoa age ao receber informações.

Por muito tempo, acreditava-se que o problema para se implementar eficazmente a psicometria seria a dificuldade na colheita de dados, problema que restou superado com a vasta gama de dados hoje existentes (*big data*). Apenas para se limitar ao Facebook, estudos de Michal Kosinski (cocriador da psicometria por meio de dados daquela rede social) de 2012 demonstrariam que com 68 curtidas é possível prever a cor da pele do usuário com 95% de precisão e sua orientação sexual com 88% de acerto. Esse número de curtidas traria revelações sobre a inteligência da pessoa, sua religião, o uso de álcool, cigarros ou drogas e até mesmo se os pais da pessoa seriam divorciados.

Pela evolução de pesquisas, chegou-se à conclusão de que 70 curtidas seriam suficientes para cientistas de dados conhecerem a pessoa mais que seus próprios amigos; com 150 curtidas mais do que seus pais e 300 curtidas mais que seus próprios parceiros. Com mais curtidas, chegaria-se a um nível de conhecimento superior ao que a própria pessoa tem de si.

Um conhecimento em nível tão elevado sobre a própria personalidade do eleitor, suas preferências e tendências possibilita que se faça uso do *microtargeting* (que pode ser traduzido como microdirecionamento), que consiste na elaboração de uma propaganda eleitoral quase personalizada e irresistível ao eleitor, apresentando o candidato ou suas propostas sob uma perspectiva que já de antemão se sabe capaz de convencer o destinatário da mensagem.

A Lei das Eleições (Lei nº 9.504/1997), entre seus arts. 57-A e 57-J, cuida da propaganda eleitoral na internet e a Resolução TSE nº 23.551 regulamenta a questão entre seus arts. 22 e 34. A grande novidade que se anuncia para as eleições de 2018 decorre da atribuição, por meio da Lei nº 13.448/2017, de redação do art. 57-C, que possibilita a propaganda eleitoral paga na internet consistente no impulsionamento de conteúdo, devidamente identificado como propaganda eleitoral, feito exclusivamente por partido político, coligação ou candidato. A novidade legislativa é um convite que se torna especialmente sedutor em razão da tendência de restrição quanto ao uso de mídias tradicionais da propaganda eleitoral e da diminuição do tempo do período de propaganda eleitoral e das campanhas. Mas ao mesmo tempo em que se chama o debate eleitoral para as novas mídias (como a internet), a legislação eleitoral não demonstra preocupação com a tutela de dados pessoais dos eleitores que são sindicáveis pelas empresas especializadas em *marketing* digital. Mas deveria.

A regulamentação contida na Lei Eleitoral e na resolução que regulamenta a propaganda elei-

toral para as eleições de 2018 e seguintes é tibia e somente trata da questão da doação, cessão ou venda de cadastros com endereços de eleitores para partidos políticos, coligações e candidatos (prática que é vedada pelo art. 57-G da Lei nº 9.504/1997) e da necessidade de que as mensagens com propaganda eleitoral sejam dotadas de mecanismo que permita o descadastramento do destinatário. Isso não quer dizer, todavia, que não haja qualquer regra no sistema jurídico brasileiro que busque controlar minimamente a questão do tratamento de dados (da sua coleta ao seu exame).

O tratamento de dados foi destinatário de regulamentação normativa pelo Marco Civil da Internet.

O CDC, em seu art. 43 e com inspiração nos *fair information principles* (que são fortes na Europa), ao tratar dos bancos de dados de consumidores, consagrou princípios como: da publicidade (art. 43, § 4º); da exatidão (art. 43, § 3º); livre acesso (art. 43, *caput* e § 1º) e da segurança física e lógica (art. 43, § 3º). A Lei do Cadastro Positivo (Lei nº 12.414/2011) reforçou a existência de princípios sobre dados no Brasil ao prever: o princípio da publicidade (art. 4º); o princípio da exatidão e o princípio da finalidade (art. 7º).

O tratamento de dados ainda foi destinatário de regulamentação normativa pelo Marco Civil da Internet (Lei nº 12.965/2014). O art. 3º, incisos II e III, reconhece que a privacidade e a proteção de dados são princípios do uso da internet no país e, especialmente no art. 7º, incisos VII, VIII, IX e X, do mesmo diploma legal, foram estabelecidas regras a serem observadas no tratamento de dados na internet brasileira. O fornecimento de dados pessoais a terceiros exige consentimento livre, expresso e informado e é instrumento que permite ao

usuário escolher se, como e quando seus dados pessoais poderão ser compartilhados. O consentimento exigido pela lei deve ser livre, de forma a espelhar uma vontade legítima manifestada longe da influência de qualquer coação, deve ser expresso e decorrer de ato de vontade do usuário (não pode ser tácito ou presumido) e deve ser ainda informado, sendo válido apenas se existir clareza ao usuário quanto ao contexto do tratamento de dados e das consequências de sua opção.

Qualquer exceção a essa regra do livre consentimento deve estar expressamente prevista em lei (como pode ocorrer, por exemplo, em questões alusivas a segurança).

O livre consentimento é ainda complementado pela disposição do art. 7º, inciso IX, que indica que, além de expresso, ele deve ser obtido com clareza e transparência, devendo estar destacado das demais cláusulas contratuais.

O art. 7º, inciso VIII, contempla dois princípios caros a um sistema de proteção de dados pessoais: a transparência e a finalidade. É imprescindível que o usuário e titular dos dados tenha informações claras, completas e precisas sobre o que será feito com seus dados, o que é condição *sine qua non* inclusive para que possa haver o exercício do livre consentimento previsto no inciso anterior. Já o princípio da finalidade determina ser inadmissível o uso dos dados pessoais para finalidade diversa daquela que foi informada no momento do consentimento. O uso do dado pessoal para finalidade diversa daquela do contexto da obtenção do consentimento do titular exige nova autorização para o novo uso.

O inciso X, por sua vez, reconhece o direito do titular dos dados de pleitear sua exclusão após o término da relação entre ele e o provedor de aplicação, exceção feita às hipóteses de guarda obrigatória de registros na forma da lei.

É possível concluir, portanto, que existe um sistema de proteção de dados no Brasil que deve repercutir para as relações jurídicas travadas no

ambiente da internet e também do Direito Eleitoral. Ainda que sem o vigor que apresenta contexto europeu, a interpretação sistemática, teleológica e finalística das regras apresentadas sinaliza a existência de um direito à autodeterminação informativa, de modo que deve ter o titular dos dados completo domínio sobre seus dados pessoais a partir de princípios como o do livre consentimento, da transparência e da finalidade.

Voltando mais uma vez a atenção à atuação da Cambridge Analytica, há informações de que a empresa utilizou, nos trabalhos prestados à campanha presidencial de Donald Trump, aproximadamente 7 mil informações sobre cada eleitor para direcionar suas publicidades (número que seria decorrente da possibilidade ampla de compra de informações admitidas no sistema jurídico dos EUA). No Brasil, estima-se que o número de informações utilizadas deve ser cerca de 750, com a empresa apostando em dados oficiais, como os produzidos pelo IBGE.

Considerando-se o ambiente de competição (não só eleitoral, como empresarial), pode-se imaginar que o *microtargeting* seja mais eficiente quanto mais dados se tenha do eleitor. E se as empresas de *marketing* digital (ou qualquer outro ator do processo eleitoral) avançarem sobre dados pessoais dos eleitores?

Por dados pessoais pode-se entender o dado relacionado à pessoa natural, identificada ou identificável, inclusive por números identificativos, dados locacionais ou identificadores eletrônicos, quando estiverem relacionados a uma pessoa. Esta definição consta do art. 14, inciso I, do Decreto nº 8.771/2016 (que regulamentou o Marco Civil da Internet) e ainda está reproduzida no art. 5º, inciso I, do PLS nº 5.276/2016. Certamente que a definição desperta críticas e incentiva elogios, já que ela mede, em certa maneira, a extensão da incidência de normas sobre tratamento de dados. Contudo, ela tem a virtude de servir-se do signo **identificável**, de modo a colocar sob a proteção destinada aos dados

pessoais aqueles que podem ser alvo de processos de reversão de anonimização.

Assim, os dados de uma pessoa que revelam não somente sua identidade, mas seu jeito de ser, seus hábitos, costumes e suas características psicológicas são dados pessoais e, se o seu tratamento gerar situação discriminatória (em razão de raça, credo, opiniões morais e filosóficas, de saúde e de hábitos sexuais), poderão ser classificados como dados sensíveis. Aqui a necessidade de proteção é ainda mais aquilatada.

Infelizmente, a coleta de dados pessoais – notadamente durante a navegação da internet – nem sempre respeita a privacidade do usuário e os desdobramentos de sua autodeterminação informativa. Em muitos casos, provedores de aplicações atuam de forma maliciosa para ter acesso a dados pessoais dos usuários que, em muitos casos, nem sequer têm ciência de que informações estão sendo capturadas e tampouco conhecem os fins a que tais dados estão destinados. Apenas como exemplo, pode ser lembrado o caso de um teste que mudava a foto do perfil do usuário para o gênero oposto: após dias de grande sucesso da brincadeira, passou-se a saber que aquele que realizava tal teste permitia o acesso do provedor de aplicação a seus dados pessoais como *sites* visitados, número de cliques dados e tipos de *e-mails* recebidos.

A rigor, a empresa de *marketing* digital que queira servir-se de dados pessoais para potencializar o sucesso da publicidade eleitoral que produz somente poderia utilizar dados que fossem colhidos, armazenados e tratados após o livre consentimento do titular dos dados, manifestado de forma expressa e de maneira clara, com o prévio conhecimento sobre quais seriam o destino e o uso que se dará aos seus dados. Os dados que, porventura, fossem autorizados a pretexto de possibilitar uma melhor experiência de navegação ou para fins de publicidade comercial não poderiam ser utilizados para a propaganda eleitoral.

A possibilidade de uso indevido de dados pessoais, especialmente num cenário de inexistência de uma lei geral de proteção de dados que regule procedimentos e preveja uma autoridade administrativa responsável pela matéria, mostra-se consideravelmente alta. E aqui ainda vale frisar que se paga um preço pela omissão em regular adequadamente a matéria, à luz do que permite e recomenda o art. 57-J da Lei nº 9.504/1997.

Mas o que se pode fazer se, a despeito da dificuldade de se visualizar a prática, ocorrer o uso indevido de dados pessoais na propaganda eleitoral na internet?

O primeiro caminho que se apresenta é esperar que os partidos políticos, coligações e candidatos adversários, no exercício de fiscalização mútua que fazem sobre a propaganda eleitoral em geral, ajuízem representação eleitoral (art. 96 da Lei nº 9.504/1997) para postular que seja exarado um provimento jurisdicional que imponha ao infrator um dever de abster-se da prática ilícita, constituindo uma obrigação de não fazer. Além dos tradicionais atores do processo eleitoral, o Ministério Público também tem legitimidade ativa *ad causam* para essa demanda.

A possibilidade de uso indevido de dados pessoais mostra-se consideravelmente alta.

O segundo caminho que se abre para os casos em que o uso indevido de dados tenha valor econômico e tenha impactado a lisura e normalidade do processo eleitoral é o uso da ação de investigação judicial eleitoral (AIJE) (entre a escolha e registro dos candidatos até a data da diplomação dos eleitos) ou da ação de impugnação de mandato eletivo (AIME) (art. 14, §§ 10 e 11, da CF/1988, no prazo de 15 dias a contar da diplomação dos eleitos). O art. 22, inciso XVI, da LC nº 64/1990,

a partir da LC nº 135/2010 (a Lei da Ficha Limpa), pretendeu alterar os critérios de aferição do caráter abusivo de um ato no contexto eleitoral, abandonando-se a ideia da potencialidade do fato de alterar o resultado das eleições para se determinar o exame da gravidade da conduta (por critérios quantitativos e qualitativos). E, no desenvolvimento do raciocínio jurídico sobre a ocorrência ou não do abuso, certamente deve ser considerada a aquilatada força persuasiva (a capacidade de formar ou alterar o voto) da propaganda personalizada que o microdirecionamento é capaz de produzir. A medida, portanto, não deve ser apenas o montante de recursos financeiros expendidos na operação, mas também a própria força de convencimento que a propaganda eleitoral construída a partir dos dados pessoais apanhados de forma irregular possui.

Aqui, o provimento jurisdicional demandável será de natureza constitutivo-negativa (cassação do registro de qualquer candidato e do diploma ou mandato do eleito) e, ainda, de caráter condenatório, por meio da imposição (para os casos de procedência da ação do art. 22 da LC nº 64/1990) de pena de inelegibilidade cominada potenciada pelo prazo de oito anos a contar das eleições para todos os que, por alguma forma, tenham participado da trama dos fatos considerados abusivos. A legitimidade ativa para estas demandas, à semelhança do que ocorre com as representações do art. 96 da Lei nº 9.504/1997, recai sobre partidos, coligações, candidatos e Ministério Público, sendo cabível o desenvolvimento de uma fase instrutória com contornos nítidos que possibilite oitiva de pessoas, requisição de documentos e informações de posse de terceiros e, inclusive, a produção de prova pericial.

Em todas essas demandas (tanto a representação do art. 96 da Lei nº 9.504/1997 quanto a AIJE ou AIME) poderá ser difícil a prova de que houve o uso de dados pessoais de forma irregular para a produção da propaganda. Uma possibilidade, nesses

casos, é que o Estado-Juiz sirva-se do permissivo do art. 373, § 2º, do CPC/2015 e, aplicando a teoria da distribuição dinâmica no ônus da prova, reconheça que as peculiaridades da demanda indicam que a prova da licitude dos dados deve ser feita pelo réu: afinal de contas, se o livre consentimento deve ser sempre claro, expresso e dado para o uso de informações exclusivamente para os fins indicados, deverá ter o réu, via de regra, prova documental da autorização para o uso (o art. 9º, § 2º, do Projeto de Lei nº 5.276/2016 vai nesse sentido).

O cidadão afetado, enquanto titular dos dados indevidamente utilizados, não tem em linha de princípio legitimidade ativa para acionar a Justiça Eleitoral. A defesa de seu patrimônio jurídico deverá acontecer perante a Justiça Comum, pleiteando-se que o violador de seu direito seja obrigado a abster-se da prática ilícita e, ainda, reparar os dados materiais e morais causados.

Também se pode ver a possibilidade de que, diante da existência de indícios sérios de uso indevido de dados pessoais em larga escala, qualquer colegitimado para as ações coletivas ajuíze ação civil pública em que se pleiteia que o réu comprove a licitude dos dados que utiliza e, reconhecido o ilícito, a reparação do dano causado e a cessação da prática incompatível com o direito.

3 Conclusões

A propaganda eleitoral na forma como conhecemos, com seus comícios, passeatas, reuniões, panfletos, programas de rádio e televisão, começa a transformar-se em algo, diante da revolução tecnológica a que assistimos dia a dia, que ainda não dominamos adequadamente.

Já para as eleições de 2018, ainda que não se prescindam das formas tradicionais de campanha, o fato é que assistiremos a um implemento considerável na propaganda eleitoral através da internet, especialmente pela possibilidade de impulsiona-

mento das mensagens pelos candidatos e pela limitação orçamentária das campanhas. Esse, nos parece, é um processo irreversível, tendente a aumentar, mais e mais, nos próximos anos.

Nesse cenário, consideramos imprescindível uma maior consideração com o tratamento dos dados pessoais dos usuários na rede, como forma de estabelecer os parâmetros adequados para a disputa entre os candidatos e o respeito à privacidade dos eleitores. Nunca é demais lembrar que as principais plataformas na internet são propriedades de grandes conglomerados empresariais em negócios com alto retorno econômico, em que as pessoas voluntariamente participam através da inserção de mensagens, fotos e informações. Embora, na legislação eleitoral vigente, já se possa encontrar formas de proteção judicial contra o mau uso e o abuso nas informações coletadas, conforme acima descrito, é fundamental o debate público e transparente sobre a proteção dos dados dos usuários nos processos eleitorais.

Glossário

Algoritmos – “Algoritmos são formas de automatizar processos decisórios, que estão por detrás de muitas coisas que acontecem também na Internet, como decidir qual anúncio será exibido para você ou quem é a próxima pessoa a aparecer em um aplicativo de relacionamentos. Por meio deles, a sua experiência de navegação pode mudar e, com isso, o seu acesso a determinadas informações, ofertas ou até mesmo oportunidades de emprego”. Fonte: InternetLab, <<http://www.internetlab.org.br/pt/opiniaao/especial-em-um-mundo-de-big-data-quais-tipos-de-controle-temos-em-relacao-a-nossos-dados/>>.

Big data – “Atualmente, uma série de funcionalidades e serviços são disponibilizados graças à possibilidade de armazenar, tratar e analisar enormes quantidades de dados de maneiras inovadoras – o chamado **big data**. A partir de tais capacidades de armazenamento, tratamento e análise de dados

pessoais coletados a partir de nossos hábitos, torna-se plausível inferir tendências e traços de personalidade, predizer possíveis comportamentos e estabelecer perfis bastante detalhados de todos nós”. Fonte: <<http://www.internetlab.org.br/pt/opinioao/especial-em-um-mundo-de-big-data-quais-tipos-de-controle-temos-em-relacao-a-nossos-dados/>>.

Cambridge Analytics – “[...] empresa pioneira no uso da psicologia comportamental com base em grande base de dados em campanhas

políticas”. Fonte: <<http://www1.folha.uol.com.br/poder/2017/12/1940938-empresa-que-atuou-na-campanha-de-trump-chega-ao-brasil.shtml>>.

Cookies – Pequenos arquivos armazenados por um navegador de internet (*browser*) que guardam metadados, ou seja, informações como a data da última visita, o estado do *login*, isto é, se a opção de “lembrar minha conta” estiver ativada, além de outras informações que permitem a prática do *microtargeting*. ■

Bibliografia

DONEDA, Danilo. *Da Privacidade à Proteção de Dados*. Rio de Janeiro: Renovar, 2006.

_____; MONTEIRO, Marília. O Sistema de Privacidade e Proteção de Dados no Marco Civil da Internet. In: ARTESE, Gustavo (Org.). *Marco Civil da Internet, Análise Jurídica sob uma Perspectiva Empresarial*. São Paulo: Quartier Latin, 2015.

MENDES, Laura Schertel. *Transparência e Privacidade: Violação e Proteção da Informação Pessoal na Sociedade de Consumo*. 2008. Dissertação (Mestrado em Direito) – Faculdade de Direito, UnB, Brasília.

MORGADO, Laerte Ferreira. *O Cenário Internacional de Proteção de Dados Pessoais*. Necessitamos de um Código Brasileiro? Disponível em: <http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA SOBRE_PROTECAO_DE_DADOS_PESSOAIS_UMA_ANALISE_DE_SEUS_ASPECTOS_GERAIS.aspx>. Acesso em: 16 mar. 2018.

REINADO FILHO, Demócrito. *A Diretiva Europeia Sobre Proteção de Dados Pessoais – Uma Análise de seus Aspectos Gerais*. Disponível em: <http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA SOBRE_PROTECAO_DE_DADOS_PESSOAIS_UMA_ANALISE_DE_SEUS_ASPECTOS_GERAIS.aspx>. Acesso em: 16 mar. 2018.

VASQUES, Rafael Ferraz. *A Proteção de Dados Pessoais nos Estados Unidos, União Europeia e América do Sul: Interoperabilidade Com a Proposta de Marco Normativo do Brasil*. Disponível em: <<http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>>. Acesso em: 16 mar. 2018.

VAZ, Ana Carolina. Neutralidade, Proteção de Dados Pessoais e Marco Regulatório da Internet no Brasil. In: *Revista Democracia Digital e Governo Eletrônico*. (ISSN 2175-9391), n. 5, p. 147-171, 2011.