

CENTRO UNIVERSITÁRIO UNIDADE DE ENSINO SUPERIOR DOM BOSCO – UNDB
CURSO DE DIREITO

THIAGO MARTINS ALMEIDA

PROTEÇÃO DE DADOS PESSOAIS E DEMOCRACIA: os impactos do tratamento de
dados nas eleições brasileiras de 2018

São Luís

2021

THIAGO MARTINS ALMEIDA

PROTEÇÃO DE DADOS PESSOAIS E DEMOCRACIA: os impactos do tratamento de dados nas eleições brasileiras de 2018

Monografia apresentada ao Curso de Graduação em Direito do Centro Universitário UNDB como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientadora: Profa. Ma. Manuela Ithamar Lima.

São Luís

2021

Dados Internacionais de Catalogação na Publicação (CIP)
Centro Universitário – UNDB / Biblioteca

Almeida, Thiago Martins

Proteção de dados pessoais e democracia: os impactos do tratamento de dados nas eleições brasileiras de 2018. / Thiago Martins Almeida. — São Luís, 2021.

72 f.

Orientador: Prof^ª. Ma. Manuela Ithamar Lima.

Monografia (Graduação em Direito) - Curso de Direito – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2021.

1. Direito digital. 2. Democracia. 3. Proteção de dados pessoais.
4. Eleições 2018. I. Título.

CDU 342.8:004.738.5

THIAGO MARTINS ALMEIDA

PROTEÇÃO DE DADOS PESSOAIS E DEMOCRACIA: os impactos do tratamento de dados nas eleições brasileiras de 2018

Monografia apresentada ao Curso de Graduação em Direito do Centro Universitário UNDB como requisito parcial para obtenção do grau de Bacharel em Direito.

Aprovado em 16/6/2021

BANCA EXAMINADORA

Profa. Ma. Manuela Ithamar Lima (Orientadora)
Centro Universitário UNDB

Profa. Dra. Heloísa Gomes Medeiros
Centro Universitário UNDB

Procurador Esp. Bruno Tomé Fonseca
Procuradoria Geral do Estado do Maranhão

A mim mesmo, a minha família, meus amigos e a minha orientadora. Essa monografia é nossa. Obrigado pelo companheirismo de sempre que faz com que momentos tão difíceis sejam vividos com uma leveza necessária. Obrigado.

AGRADECIMENTOS

Inicialmente, gostaria de agradecer a minha orientadora por ter aparecido em um momento necessário e proposto exatamente o que eu queria escrever, ter embarcado nessa jornada prontamente e acompanhado todo esse caminho até o final da monografia sempre de forma alegre e descontraída, obrigado por tudo Manu, você é luz!

A minha mãe e meu pai por terem investido em mim e sempre me apoiado em tudo que eu escolho fazer, assim como às minhas irmãs que sempre foram inspiração para mim, vocês moram em meu coração e sou muito grato por isso.

Ao meu sobrinho, Ian José, por me cerca de alegria todos os dias. Mesmo que brigando comigo diariamente, saiba que eu te amo batatinha.

Queria agradecer a Carolina Sousa, minha companheira de jornada acadêmica, minha dupla de paper e que curiosamente compartilhou a mesma orientadora que eu nesse processo de escrita de monografia. Obrigado pelos momentos vividos, pela parceria e por tudo mais que está por vir, te amo.

Gostaria de agradecer ainda Adriano Henrique e Sofia Gianessi, outros companheiros nessa trajetória acadêmica e que compartilharam comigo esse momento de escrita da monografia, vocês são duas pessoas extremamente competentes e que moram em meu coração, obrigado pela confiança e pela parceria de sempre.

Agradeço à minha panelinha: Adriano, Carol, Sofia, Luiza, Allana, Daniel, João e Guilherme por me acompanharem desde o dia 01, seja em nossos milhares de debates de case ou em nossas fofocas vocês sempre estiveram presentes e sem vocês talvez eu não estivesse chegado até o fim desse curso, obrigado.

A Giovanna Melo e a Guilherme Melo, amizades construídas ao longo da graduação que me fizeram sentir como se família fosse, são meus primos de coração e que guardo muito apreço e admiração. Para sempre com vocês, obrigado.

Gostaria de agradecer ainda a Beatriz Melo e a Milena Mota, obrigado pelas risadas e pelo companheirismo, morro de saudade de vocês, é um tipo de conexão que não evapora com o tempo, sou muito grato pela amizade de vocês.

Ao PAJUP, por ter sido o grupo de extensão que eu precisava, por ser um espaço de extrema necessidade e importância ao longo da vida acadêmica de muitos estudantes – o direito é um elemento transformador. Em especial meu apreço pelos meus companheiros de jornada ajupiana: Brenda Lessa, Beatriz Alves, Artur Andrade, João Miguel, Karol Fernandes e Layse. Vocês foram muito importantes para meu crescimento.

A eterna coordenação da UNDB, representada por Gisele e Samira, muito obrigado por ser um espaço de descontração em meio ao caos que a vida acadêmica nos faz viver. Nunca esquecerei os momentos de desabafos, piadas, fofocas e também de aprendizagens vividas dentro da coordenação de direito. Gisele e Samira vocês são maravilhosas!! Continuem sempre assim, vocês ganham o coração de todos os alunos que passam pela instituição.

Gostaria de agradecer a Rebeca Costa, por ser uma amiga presente em diversos momentos vividos na faculdade, uma pessoa forte e segura de si que contagia as pessoas em sua volta, obrigado pelos conselhos e pela confiança sempre recebida. Você é uma pessoa fantástica!

A minha atlética Tribuna, obrigado por ter me proporcionado os melhores anos da minha vida acadêmica, gerenciar uma atlética não é fácil, existe discussão, conflitos, mas acima de tudo é um espaço livre onde podemos ser quem somos e isso torna tão especial esse ambiente. Obrigado por serem família, serem alegria e serem a descontração necessária dentro da faculdade. Obrigado pelos jogos, pelas festas e pelo trabalho que foi fazer com que tudo isso acontecesse. Não vou me ater a nomes porque são muitos, então querida Tribuna saiba que é um orgulho ter participado do seu nascimento e te ver crescer. Para sempre Tribuna.

Ao meu grupo da academia, “mundinho bt”, por ter proporcionado momentos de descontração tão necessários nesse momento de escrita, Anna Luiza Lindoso, Matheus Santos, Vanessa Souza e Ana Luiza Corrêa vocês são tudo na minha carreira.

Em especial, à Anna Luiza Lindoso por ser minha companheira em todos os momentos, acompanhar meu dia a dia e estar presente, obrigado por tudo amiga, te amo muito.

Ao meu amigo Roberto Costa, por ser o melhor amigo que eu poderia ter, mesmo que em momentos distantes, as vezes, sei que sempre estamos juntos. É inexplicável o quanto te amo e por você ser você, obrigado por alegrar a minha vida. Sempre estarei contigo.

Ao meu grupo chamado “illepozão” por serem um presente na minha vida, todas nossas conversas, nossos encontros, vocês são importantíssimos para mim e agradeço muito por estarem presente. Clarice Moraes, Ana Luiza Fernandes, Laura Maia, Natália Frota, Hênio Antonio, Paulo Evangelista, Roberto Costa, Maurício Seabra e Jg vocês são indescritíveis, tudo pra mim!

Aos meus amigos Matheus Santos e Ciro Moura Fé por me cercarem sempre de boas vibrações e bons momentos, quem tem vocês têm tudo, muito obrigado! Vocês moram em meu coração, amo vocês.

A minha amiga Ana Luiza Feitosa por ser minha companheira desde da 7ª série, por ser meu pulmão e minha bussola moral muitas vezes. Por ter me escutado durante o último ano

sobre diversos temas de monografia e sobre a caminhada que foi chegar até aqui, muito obrigado.

A Paula Arrais, também pelo companheirismo de anos e a presença dessa amizade, lhe amo de montão paulinha.

A Débora Bandeira e Thamires Rodrigues, pela companhia ao longo do estágio em que nós três dividimos tantas coisas, tenho muito apreço e admiração por vocês.

Por fim, gostaria de agradecer ao corpo docente da UNDB, a todos aqueles professores que passaram algo muito além do que somente o conhecimento, transmutaram o meu ser. Obrigado por tudo, em especial ao melhor coordenador de curso possível: Arnaldo Vieira Sousa. Além dele posso citar alguns nomes como Alexandre Ferreira, Thales Lopes, Amanda Thomé, Manuela Ithamar, Tuanny Soeiro, Maira Castro, Aline Froes, Alyne Caldas, Roberto Almeida, Daniel Almeida, Heloisa Medeiros e Thaís Viegas. Meu muito obrigado.

*Let everything happen to you
Beauty and terror
Just keep going
No feeling is final”
— Rainer Maria Rilke*

RESUMO

Ao longo desta monografia serão tratadas as questões sobre o direito digital e a sua relação com o processo democrático, para concluir de que forma o tratamento de dados pessoais impacta na democracia. Inicialmente, será abordado como a sociedade de informação funciona, a partir do novo tipo de negócio e quais as consequências que isso traz para o direito à privacidade. Em seguida, será abordado o nascedouro da democracia e sua evolução até a construção de uma democracia digital, a qual deixa claro que a democracia plena na sociedade de informação depende também do devido tratamento de dados pessoais. Ademais, é estudado o direito à proteção de dados pessoais como um direito fundamental para então abordar como funcionam os bancos de dados. Compreendido o funcionamento deles serão abordados os limites e as possibilidades quanto ao tratamento de dados na democracia – a partir do caso da Cambridge Analytica que impactou o tratamento de dados. Por fim, se adentrará no caso das eleições brasileiras de 2018 e como essas foram conduzidas, levando-se a concluir que o tratamento de dados afetou de certa forma o processo eleitoral com o uso de robôs e de spams no aplicativo *whatsapp*, interferindo assim na liberdade de escolha do eleitor. Além disso, se observará a legislação existente no Brasil à época das eleições analisadas e em seguida o marco normativo futuro com a entrada da Lei Geral de Proteção de Dados (LGPD). Concluindo-se assim, que mesmo sem a vigência de uma LGPD, quando das eleições de 2018 já se poderia haver o reconhecimento de ilegalidade quanto ao uso de microdirecionamento e spams em aplicativos de mensagens e, que com a entrada da LGPD tem-se um futuro ainda incerto para a proteção de dados pessoais em contexto eleitoral, sendo importante observar os princípios e normas que direcionam a lei. Para desenvolver de forma aprofundada e detalhada a presente pesquisa fora utilizado o método hipotético-dedutivo, além de possuir natureza exploratória e de cunho bibliográfico e documental.

Palavras-chave: Big Data. Direito Digital. Democracia. Proteção de dados pessoais. Eleições de 2018.

ABSTRACT

Throughout this undergraduate thesis, some questions will be contemplated about digital law and its relationship to the democratic process, in order to conclude how the treatment of personal data impacts on democracy. Initially, it will be discussed how the information society works, based on the new type of business and what consequences this brings to the right to privacy. Then, will be addressed the birth of democracy and its evolution to the construction of a digital democracy, which makes it clear that full democracy in the information society also depends on the proper processing of personal data. In addition, the right to the protection of personal data is studied as a fundamental right, to then address how databases work. Once understood how they work, will be addressed the limits and possibilities regarding the treatment of data in democracy – starting with the case of Cambridge Analytica that affect the treatment of data. Finally, it will enter the case of the 2018 brazilian elections and how they were conducted, leading to the conclusion that the data processing affected the electoral process in some way with the use of robots and spams in the whatsapp app, thus interfering in the voter freedom of choice. In addition, will be observed the existing legislation in Brazil at the time of the analyzed elections and then the future regulatory framework with the entry of the Brazilian General Data Protection Law (LGPD). In conclusion, thus, that even without the existence of an LGPD at the time of the 2018 elections, there could already be recognition of illegality regarding the use of microdirection and spams in messaging applications, and that with the entry of the LGPD there is a still uncertain future for the protection of personal data in an electoral context, so it is important to observe the principles and norms that guide the law. In order to develop this research in depth and detail, the hypothetical-deductive method was used, in addition to being exploratory, bibliographic and documentary in nature.

Key words: Big data. Digital Law. Democracy. Protection of personal data. 2018 elections.

SUMÁRIO

1 INTRODUÇÃO	12
2 A SOCIEDADE DA INFORMAÇÃO E O PAPEL DA TECNOLOGIA NO SURGIMENTO DO DIREITO À PROTEÇÃO DE DADOS E NA DEMOCRACIA..	16
2.1 Sociedade de informação: conceitos e características	16
2.2 Tecnologia e direito: a origem do direito à proteção de dados pessoais.....	21
2.3 O impacto da tecnologia na democracia	25
3 O TRATAMENTO DE DADOS PESSOAIS NO PROCESSO DEMOCRÁTICO	31
3.1 A proteção de dados pessoais como direito fundamental	31
3.2 Big Data e a técnica de tratamento de dados	37
3.3 Dados pessoais e democracia: limites e possibilidades	41
4 ELEIÇÕES E O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: A SUA CORRELAÇÃO E SEU MARCO NORMATIVO	47
4.1 O papel das mídias sociais e das corretoras de dados no processo eleitoral.....	47
4.2 O marco normativo do tratamento de dados na democracia antes da Lei Geral de Proteção de Dados	52
4.3 Lei Geral de Proteção de Dados e o futuro da democracia na era da informação ..	55
5 CONCLUSÃO	61
REFERÊNCIAS.....	65

LISTA DE ABREVIATURAS E SIGLAS

CA	Cambridge Analytica
CF	Constituição Federal
EUA	Estados Unidos da America
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
STF	Supremo Tribunal Federal
TICs	Tecnologias de Informação e Comunicação
TSE	Tribunal Superior Eleitoral

1 INTRODUÇÃO

A internet trouxe consigo uma reestruturação da sociedade em que se vivia, com os avanços tecnológicos e a criação de smartphones, atualmente é raro encontrar alguém que não tenha acesso a internet na palma de suas mãos. A informação é o elemento que estrutura a sociedade contemporânea, a sociedade de informação, a qual gerou uma alteração do padrão em que as relações sociais se estruturavam.

Certo é que, o virtual não é um segundo mundo mas sim uma expressão do mundo de carne osso, a internet é real. Assim, nos últimos anos pode se observar a crescente onda de debates sociais e políticos nas redes sociais, o que antes parecia ser um mundo alternativo se tornou uma fonte indispensável para as relações humanas. Sendo assim, a política ingressou nas telas do celulares e as eleições que antes eram decididas puramente em comícios e “santinhos” espalhados pelas ruas, não são mais assim. Para “fazer política” no século XXI é preciso utilizar das redes sociais, não bastar ter apenas apoiadores locais, é necessário um forte envolvimento no ambiente virtual.

Com isso, tem-se a construção de uma democracia digital, baseada nos mecanismos de Tecnologia de Informação e Comunicação, as manifestações de junho de 2013 são um exemplo claro de como a internet pode reunir as pessoas em prol de uma reivindicação política, todavia, mesmo com esse poder, a internet também trouxe consigo a desinformação já que qualquer pessoa pode falar sobre qualquer coisa, surgiram assim as notícias fraudulentas e quando estas dizem respeito ao processo democrático configura-se um perigo.

A dinâmica do sistema de informação atrelada aos bancos de dados geraram uma arma publicitária capaz de influenciar e manipular os consumidores, o processo de análise dessas informações possibilitaram se precisar o perfil do potencial comprador, assim como seus hábitos e outras informações – técnica chamada de mineração de dados. Essas informações podem calcular os efeitos de uma publicação para determinada pessoa, direcionando publicidades para produzir determinada decisão. A questão é que não demorou para essa estratégia começar a ser utilizada também no campo político.

O escândalo da empresa *Cambridge Analytica*, a qual foi acusada de ter interferido nas eleições presidenciais do Estados Unidos por meio de coleta abusiva e uso de dados pessoais, gerando diversos conteúdos direcionados à eleitores específicos a partir da análise de dados, trouxe à luz as diversas empresas que trabalham no mesmo sentido: utilização de dados pessoais como forma de impulsionar campanhas.

No Brasil não é diferente, existe uma indústria na qual diferentes empresas

fornece dados umas às outras, variados perfis de empresas que usam dados para gerar receita – os chamados “*data brokers*” – reúnem informações de diversas fontes, públicas e privadas, para vender e revender dados dos cidadãos. Uma das maiores fontes de dados do país é o Serasa Experian, banco de dados que segmenta e classifica a população em vários grupos bem detalhados.

Segundo Bruno Bioni (2019, p.51) esses tipos de serviços “extrapolam o campo da publicidade direcionada, consistindo em um modelo de negócio ainda mais intrusivo”. Dentre essas empresas que se apresentam como especializadas em promover marcas e engajamento nas mídias sociais, essas mesmas podem ser contratadas para atuar nas eleições.

Nesse sentido, é razoável a preocupação dos impactos que podem ser causados ao se utilizar da análise de dados pessoais no contexto do procedimento democrático, onde a livre escolha dos candidatos deve ser realizada sem interferências de terceiros. Hodiernamente, tem-se um ambiente onde os candidatos podem ter acesso a todos os dados dos usuários e estes serão utilizados para seu proveito pessoal, sendo possível manipular o eleitor em um ou outro sentido, deixando-os com um dos pilares da democracia afetado: a liberdade de escolha dos candidatos.

A temática traz consigo uma reflexão de extrema necessidade, com os avanços tecnológicos houve a transformação das relações sociais, todavia, grande parte da população ainda desconhece os efeitos do uso da internet. Como já dito acima, as técnicas de mineração de dados que geram conhecimento das informações dos usuários podem ser utilizadas para direcionar propagandas, dentre essas temos a publicidade comportamental e outras técnicas que conseguem definir até mesmo o estado psicológico do usuário ao visualizar um anúncio.

Com isso, as grandes empresas de análise de dados acabam por deter um conhecimento abundante das informações dos usuários de serviços online, enquanto estes não possuem o conhecimento de como esses dados podem ser utilizados. Ao trazer essas técnicas para o ambiente do processo democrático, visualiza-se uma violação à privacidade, liberdade e autonomia, sendo assim, de grande importância social o estudo do tema.

Quanto a academia, vê-se o crescente debate acerca da proteção de dados pessoais, até pela recente Lei Geral de Proteção de Dados, então estudar os impactos da análise de dados no processo eleitoral é um trabalho inovador e de extrema importância para entender as consequências do uso desses dados pelas grandes empresas.

De forma pessoal, a escolha do tema surgiu ao assistir um documentário sobre o escândalo da *Cambridge Analytica*, neste tive o primeiro contato com o debate acerca do uso das informações do usuário na internet e como estas podem ser usadas para traçar um perfil e direcionar publicidades específicas para o usuário. Para quem, como eu, cresceu junto com a

internet e as redes sociais este é um tema de grande relevância, já que pode-se perceber como essa máquina funciona e difundir tais informações àqueles que não estão atentos às consequências do uso de sites/aplicativos, de como estes podem ser usados contra o próprio usuário.

Dado o contexto das eleições brasileiras de 2018, em que houve diversas mensagens direcionadas em aplicativos de mensagens sobre o processo eleitoral, questiona-se: de que modo o tratamento de dados pessoais impacta na democracia.

Para tanto, o objetivo geral dessa pesquisa é compreender sobre a análise de dados pessoais e seu impacto no processo democrático, refletindo sobre como foi modificada a sociedade nos últimos anos com o surgimento das Tecnologias de Informação e Comunicação (TICs) e seu reflexo tanto no ambiente comercial como no ambiente público/democrático.

Para chegar a tal entendimento, foi-se utilizado como método de pesquisa o hipotético-dedutivo. Segundo Marconi e Lakatos (2003), este método consiste em um processo no qual o ponto de partida é o problema, o problema que vai desencadear a pesquisa, portanto, é escolhida uma hipótese como solução provisória que vai ser testada para assim no final conclui-se é ou não a solução para o problema apresentado. Nesta monografia, a hipótese está sendo representada de modo que a mineração de dados realizada para fins de atuação em um processo eleitoral infringe o direito à liberdade e autonomia dos eleitores, afetando o processo democrático.

A construção dessa monografia mostrou-se possível graças a vasta bibliografia acessível sobre o tema da sociedade de informação e a questão do tratamento de dados pessoais, com a leitura de livros acadêmicos, artigos, dissertações e relatórios. Logo, é correto afirmar que a monografia construída tem natureza bibliográfica e documental. Ademais, a pesquisa se caracteriza, enquanto seus objetivos, como exploratória, buscando um melhor esclarecimento do tema proposto. (GIL, 2002)

Em rumo ao modelo organizacional dessa monografia, a mesma será dividida em três capítulos, cada um contando com três subseções. No primeiro capítulo será introduzida a ideia de uma sociedade de informação amparada pelos meios digitais e que alterou a organização dos modelos de negócio, os dados são a nova moeda de troca nesta sociedade, a qual é operada pelo capitalismo de vigilância – forma de prever e operar o comportamento humano por meio de controle do mercado. Concluindo-se que ao mesmo passo que houve uma mudança no mercado, também se tem uma mudança no ambiente político. Em seguida, é estudada a privacidade e como as Tecnologias de Informação e Comunicação alteraram esse direito, ainda é relatado o nascimento do direito à autodeterminação informativa e os desenhos

das novas dinâmicas sociais provenientes com a informação. Por fim, será dissertado sobre o nascimento da democracia e sua evolução com o surgimento das TICs – a estruturação de uma democracia digital.

No segundo capítulo, inicialmente, é dissertado sobre o direito à proteção de dados pessoais como direito fundamental, compreendendo a existência da cláusula de abertura para interpreta-lo como um direito fundamental implícito. No mais, é abordada a distinção entre dado e informação para poder se dissertar sobre as dimensões do direito junto com seus titulares e destinatários, além disso é relacionado o direito à proteção de dados com outros direitos como o direito de personalidade. Em seguida, é apresentada a ideia de Big Data e como funciona o tratamento de dados, comprovando como esse processo pode interferir na vida das pessoas. Ademais, é analisado como o tratamento de dados pode intervir na democracia, utilizando do exemplo da *Cambridge Analytica* para demonstrar o poder do big data em um processo eleitoral.

Já no terceiro capítulo, se ingressa no objeto do problema, a corrida eleitoral de 2018, assim é analisado o papel das mídias sociais e das corretoras de dados no processo eleitoral brasileiro e sua conexão com o processo eleitoral estadunidense de 2016. Após compreendido os reflexos do big data nas eleições brasileiras, será estudado o marco normativo brasileiro anterior à 2018, ou seja, antes da promulgação da LGPD, como eram tratados a responsabilização por danos gerados ao conteúdo publicado na internet e a regulação do micro direcionamento durante as eleições de 2018. Por fim, irá se discutir acerca da promulgação da Lei Geral de Proteção de Dados e seus princípios estruturantes, como essa lei vai regular a responsabilização do conteúdo publicado na internet, concluindo-se qual o futuro da democracia na era da informação.

2 A SOCIEDADE DA INFORMAÇÃO E O PAPEL DA TECNOLOGIA NO SURGIMENTO DO DIREITO À PROTEÇÃO DE DADOS E NA DEMOCRACIA

Neste capítulo será abordada a compreensão da sociedade de informação como modificadora das relações sociais, estudando diversas conceituações para esta sociedade. Após esta compreensão, há de se conhecer como funciona o novo tipo de negócio, o qual alterou o sistema mercadológico.

Com isso, tem-se o debate acerca do capitalismo de vigilância, o modo como o capital é operado atualmente e o impacto que isso causou no espaço público. Ademais, será abordado o caráter do direito à privacidade e seus reflexos a partir das novas tecnologias para caracterizar o surgimento do direito à proteção de dados pessoais.

Além disso, será discutida a compreensão de democracia, desde o seu nascedouro no século V a.C até a construção de uma democracia digital, de modo que são ressaltadas as grandes mudanças advindas junto à internet, tanto as positivas como as negativas, que influem diretamente no contexto do jogo democrático.

2.1 Sociedade de informação: conceitos e características

A sociedade de informação é a melhor forma de caracterizar os anos 2000, com o conhecimento digitalizado e de fácil acesso a vida é baseada nas redes de comunicação digital que estão sendo operadas por tecnologias. De acordo com Manuel Castells (2005, p.18): “as redes de comunicação digital são a coluna vertebral da sociedade em rede”, tal afirmação transpassa a ideia de que essa rede ultrapassa limites históricos, sociais e globais, o mundo encontra-se conectado. Pode-se concluir a partir desta leitura que a era da informação constitui o núcleo da sociedade.

A tecnologia transmutou o modo como o homem opera diversas tarefas diárias, assim como impactou em diversas áreas como no direito e na educação. Ressalte-se assim duas teorias relacionadas: a teoria do determinismo tecnológico e a teoria da construção social da tecnologia. Aquela primeira entende que a *techne* corresponde ao conjunto determinante da tecnologia, a qual não tem participação do contexto, ou seja, ela guia as escolhas do homem como sendo apenas em uma direção já acertada. Já a segunda teoria ao contrário do que pensa a primeira, acredita que as escolhas tecnológicas podem ser direcionadas pelo ser humano,

influenciadas pelo contexto e que podem ser também de cunho político, econômico, histórico, dentre outros. (LIMA; COSTA, 2019)

Deste modo, a sociedade de informação é fruto do sistema tecnológico interligado com os conceitos culturais e institucionais existentes, isso quer dizer que a tecnologia opera dentro das relações sociais e pessoais, assim como no mercado e na democracia. Ou seja, o desenvolvimento da ciência age de acordo com as necessidades do mundo exterior. Pode-se verificar tal desenvolvimento dentro do direito, a partir de exemplos como a criação de Lei de Biossegurança, a qual regula as pesquisas com células-tronco embrionárias de seres humanos, tática somente possível graças a tecnologia advinda de trabalhos científicos. (LIMA; COSTA, 2019)

É inegável o fato da vida cotidiana ter se tornando muito mais conveniente com o desenvolvimento das tecnologias, uma pessoa hoje em dia resolve a maior parte dos seus compromissos com um celular na mão ou em frente de um computador. Além disso, viu-se a evolução na medicina com descobrimento de tratamentos para doenças antes incuráveis, no direito com a virtualização dos processos e audiências online, enfim todas as esferas da sociedade foram modificados com a ciência e a tecnologia. (SARLET; MOLINARO, 2017)

No início dos anos 90 já era claro que a grande tendência em Tecnologias de Informação e Comunicação (TICs) eram os microcomputadores com internet, mesmo em países como o Brasil em que o acesso ainda era limitado. A popularização dos computadores abriu porta para o uso da web, assim o século XXI iniciou tendo como característica o padrão de computadores domésticos com internet, alterando a vida da sociedade que ingressou na “era da internet”. (GOMES, 2018)

Manuel Castells (2005) leciona que a sociedade do conhecimento não caracteriza a sociedade emergente, por mais que o conhecimento seja elemento fulcral desta, porque em todas as sociedades historicamente conhecidas sempre se prezou pelo conhecimento e informação. O que em sua visão seria novo à sociedade são as redes tecnológicas (base microeletrônica), as tecnologias, que são voltadas para a difusão do conhecimento/informação.

Para Bruno Bioni (2019), a informação seria uma nova característica pois assume o papel central dentro da sociedade, diferentemente de antes quando tivemos o poder da terra, seguida pelas máquinas a vapor e a eletricidade, agora é a informação que estrutura a sociedade.

Outra visão sobre essa era informacional seria a de que, diferente do que muitos pensam, não se está diante de mais uma fase da terceira revolução industrial, mas sim experimentando-se uma quarta revolução industrial conceituada por 3 razões: velocidade,

profundidade e impacto sistêmico¹. Isso porque o mundo está evoluindo em uma velocidade exponencial, modificando “quem somos” e ainda impactando toda a sociedade em grande escala. (SCHWAB, 2016)

Já o sociólogo Ulrich Beck (2018) leciona sobre a “metamorfose do mundo”, a qual traz consigo a ideia de que atualmente os espaços de ação são cosmopolizados, são globais e desintegrados, para ele o mundo está sofrendo uma metamorfose por conta de todas as tecnologias e reações emergentes, o que modifica a natureza humana desafiando o modo de pensar sobre o mundo, de imaginar e fazer política. Assim, para o autor estaria-se vivendo em uma sociedade de risco, onde os bens advindos com o avanço da sociedade hoje são contrabalanceados com os males – as externalidades advindas com o poder nuclear e químico e outras situações de riscos globais.

Percebe-se assim, diversas conceituações para a sociedade de informação, porém, não restam dúvidas quanto à mudança que ocorreu dentro da sociedade atual, a transformação advinda junto com a tecnologia, independente da nomenclatura adotada. Manuel Castells (2005, p.19) define:

A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes.

Pelo conceito exposto acima, é possível compreender o papel das redes na difusão de informação. Segundo o autor essas redes tiveram um papel modificativo em todas as estruturas da sociedade, aqui é possível citar a comunicação, esta foi alterada de forma perceptível e dentro dela é possível encontrar o espaço das opiniões e comportamentos políticos, estes ingressaram nas redes de forma que “a presença de mensagens no espaço midiático é essencial para construir uma hegemonia ou contra hegemonia”. (CASTELLS, 2005, p. 25)

Deste modo, pode-se compreender o uso das mídias como sendo essencial para a formação de opiniões, assim como voltadas a posicionamentos políticos, tema este que será destrinchado posteriormente.

Sendo assim, a sociedade está funcionando de acordo com essa nova forma de

¹ Segundo o autor, a palavra revolução denota algo abrupto e radical, assim a quarta revolução teria início na virada do século e se baseia na revolução digital. A mudança sistemática e profunda diz respeito a velocidade da inovação em termos de desenvolvimento e ruptura, aplicativos que não existiam há pouco mais de cinco anos hoje em dia são determinantes – Airbnb, Uber, etc. A digitalização e os progressos com IA para assistentes virtuais e outros softwares são impulsionados pelo aumento exponencial na capacidade de se processar e disponibilizar dados: “Cada vez mais, nossos dispositivos se tornarão parte de nosso ecossistema pessoal, nos ouvindo, antecipando nossas necessidades e nos ajudando quando necessário — mesmo que não tenhamos pedido.” (SCHWAB, 2016, p.16)

organização – a informação como elemento central. Essa forma foi construída de acordo com o surgimento das novas tecnologias que criaram os mecanismos necessários para processar e transmitir informações com uma velocidade inédita.

A guinada para o estágio atual do processamento de informações se deu a partir da transição entre o modelo de acúmulo e processamento de informações na forma de papel e o modelo binário, o qual consegue armazenar as informações em pequenas unidades (dígitos 1 e 0). Com esta linguagem, o computador pode armazenar e processar informações de maneira muito mais prática, fornecendo até mesmo o uso das ferramentas de busca. (BIONI, 2019)

Bruno Bioni (2019, p.35) afirma que todo tipo de informação se tornou digitalizada, “os bits desmaterializaram a informação”, essa linguagem binária permitiu um acúmulo de informações exponenciais em comparação ao antigo modelo de papel, o qual era impossibilitado de tamanha velocidade e profundidade. Para além dessa mudança quantitativa, o autor identifica ainda uma mudança qualitativa, a técnica binária permitiu maior organização das informações, podendo-se alocar estas em pastas e subpastas dentro de uma única tela de computador.

Um exemplo quanto essas mudanças qualitativas e quantitativas pode ser visto nas empresas, atualmente tem-se que a informação dos compradores são valiosas para o mercado, com isso pode-se observar a influência direta ao marketing e ao ambiente virtual que está sendo usado como tela pelos consumidores. Kris Shaffer (2019) afirma que a atenção é a matéria principal sendo negociada online e que os consumidores assumem um papel econômico central mesmo sem ter dinheiro envolvido.

O que o autor quer dizer com essa afirmação refere-se ao denominado *trade-off* da economia de dados, que seria a ideia de que o usuário troca seus dados pelo uso daquele site ou aplicativo. Sendo assim, a atenção é a verdadeira barganha dentro desse sistema – o que o autor denomina de “*attention economy*”. Essa ideia sugere que, as informações, e mais precisamente a atenção dos usuários, são um elemento fulcral dentro do ambiente econômico.

Relaciona-se aqui com a sociedade da classificação de Rodotà (2008, p.113), está se baseia na ideia de que a contrapartida para se obter um bem ou serviço não se limita mais a dinheiro, mas a uma cessão de informações, o usuário é obrigado a se expor com consequências que criam uma “posse permanente da pessoa por parte de quem detém as informações a seu respeito”. O verdadeiro objetivo dessa sociedade é a classificação do indivíduo, o qual tem suas próprias informações utilizadas por empresas para construção de perfis que vão ser base para impulsionar os negócios.

Assim, vale dissertar sobre os modelos de negócio, Bruno Bioni (2019) ensina que

no modelo tradicional existe a troca de pecúnia por um bem, como exemplo basta ir até a padaria mais próxima e comprar dez pães massa grossa em troca do valor de dez reais, supondo. Já o novo modelo de negócio funciona de outra maneira, os consumidores não pagam pelo produto mas cedem seus dados pessoais em troca de publicidade direcionada (os tipos de publicidade serão tratadas especificadamente no próximo capítulo).

Como exemplo tem-se o *facebook*, o usuário utiliza esse site para postar fotos e trocar mensagens mas isso funciona de forma gratuita, então os donos não faturam com isso, certo? Errado, os dados pessoais que são disponibilizados pelos próprios usuários naquela rede social são utilizados pelo *facebook* para direcionar conteúdo publicitário e assim eles recebem pecúnia dos patrocinadores (em troca dos dados).

Dessa forma tem-se uma relação plurilateral, uma vez que esse modelo de negócio envolve os anunciantes de conteúdo publicitário para haver ganho financeiro, os dados do consumidor fazem parte da relação econômica. O termo *zero-price advertisement business model* traduz exatamente essa relação, os usuários não pagam uma quantia para utilizar determinado site mas, ao fornecer seus dados pessoais possibilita o direcionamento publicitário, o que indiretamente paga pelo bem de consumo. (BIONI, 2019)

Confirma-se assim, a monetização dos dados pessoais, tem-se a utilização dos dados dos consumidores sendo utilizada por diversos sites “gratuitos”. Tal afirmação reflete diretamente no objeto da presente pesquisa, qual é o preço que o usuário paga pela utilização de uma rede social ou um site? Pode esse uso afetar o titular e até mesmo a coletividade? A primeira dessas perguntas já foi respondida.

A americana Shoshana Zuboff (2019) leciona sobre o denominado “Capitalismo de Vigilância”, este seria uma nova forma de procurar prever e modificar o comportamento humano por meio do controle do mercado, a partir da vigilância no sistema de informação. A autora leciona que cada época do capitalismo seguiu em direção ao rumo dominante, o *Google* inventou e aperfeiçoou o capitalismo de vigilância da mesma maneira que a *General Motors* inventou e aperfeiçoou o capitalismo século passado.

Shoshana Zuboff (2019, p. 15) faz a seguinte análise: “*Consider that the internet has become essential for social participation, that the internet is now saturated with commerce, and that commerce is now subordinated to surveillance capitalism*”². Viu-se que a internet funciona de acordo com o novo modelo de negócio então se a informação e a atenção impactam diretamente na economia, o comércio está subordinado ao capitalismo de vigilância. Assim, o

² “Considere que a internet se tornou essencial para a participação social, a internet agora está saturada com o comércio e o comércio é agora subordinado ao capitalismo de vigilância”.

surveillance capitalism seria uma condição e uma expressão do big data, tema este que será destrinchado no próximo capítulo.

Desta forma, pode-se concluir que o uso de sites e aplicativos acaba por disponibilizar uma gama de informações gerais e pessoais do usuário àquela rede, informações estas que serão utilizadas pelos donos desses sites para direcionar conteúdo, em troca de pecúnia. A questão aqui é observar a existência de uma assimetria do conhecimento existente já que enquanto o detentor dos dados possui todas as informações, os usuários não possuem nenhuma informação sobre eles. (BIONI, 2019)

Conceituado e caracterizado o funcionamento da sociedade de informação, pode-se concluir que as tecnologias são a engrenagem para a produção de conhecimento, o que opera a sociedade atual. Ademais, com o conhecimento do novo modelo de negócio, tem-se que o usuário ao aceitar os termos de uso de uma rede social estaria efetivamente pagando aquele uso com a disponibilidade aos seus dados pessoais, o que pode parecer algo inofensivo, entretanto, como será demonstrado posteriormente é de extrema periculosidade.

Sendo clara a incorporação da internet e dos meios digitais à vida das pessoas, tem-se como consequência que isso também afeta a vida política, o surgimento dessa nova sociedade no espaço público é um exemplo como o surgimento do e-governo com os governos inteligentes, o governo aberto e as campanhas online. O governo digital é proveniente da relação das novas tecnologias com o ser humano, não tinha como haver a mudança dos modelos de negócio e não haver a mudança também no espaço público, ambos caminham lado a lado. (AVELINO; POMPEU; FONSECA, 2021)

2.2 Tecnologia e direito: a origem do direito à proteção de dados pessoais

Para dissertar sobre a origem da tutela da proteção de dados pessoais é importante analisar o prisma da privacidade, que foi alterado drasticamente desde o início do uso das Tecnologias de Informação e Comunicação (TIC's).

Com o nascimento da sociedade de informação, tem-se uma aproximação entre pessoa e corpo eletrônico, este é aquele desenvolvido dentro do ambiente virtual, o qual está à mercê de análise a todo tempo. As informações dispersas em bancos de dados caracterizam perfis dos usuários, assim cada vez mais as pessoas são conhecidas por meio de seus dados, adentrando-se na esfera privada do ser humano. (RODOTÀ, 2005)

Engana-se quem ainda pensa estar protegido dentro da sua própria casa, hoje em dia basta um aceite em um aplicativo para conceder acesso a câmara/galeria de fotos e pronto, o acesso a todas as suas imagens estão nas mãos de um terceiro. De qualquer maneira, falar de privacidade não é algo puramente novo, a tutela da privacidade é própria da era da informação, todavia, começou a ser moldada no final do século XIX e assumiu as feições atuais nas últimas décadas. (DONEDA, 2006)

O famoso artigo de Brandeis e Warren (1890), *the right to privacy*, pode ser considerado como o início da doutrina moderna sobre privacidade, neste foi abordada a privacidade como sendo o isolamento. No artigo é introduzida a ideia do *right to be let alone*, o próximo passo para a doutrina da privacidade seria o direito do indivíduo de ser deixado só, tendo este sua privacidade respeitada no momento em que tivesse seu espaço pessoal respeitado.

Stefano Rodotà (2008, p.144) leciona que a interpretação do artigo de Brandeis e Warren deve ser a de que, atualmente, *privacy* compreende algo muito mais complexo, não apenas aquele direito de ser deixado sozinho. O direito à privacidade torna-se o direito de “controlar o uso dessas informações em qualquer momento e em qualquer lugar”, ou seja, o usuário tem a palavra final quanto a utilização e disponibilização de seus dados.

Isso porque, após o marco do direito de ser deixado sozinho, começaram a ser desenvolvidas outras definições igualmente importantes como o direito de controlar os dados pessoais e de controlar como as pessoas utilizam esses dados. Com o reconhecimento de que a coleta de dados sensíveis pode levar a discriminação, conclui-se que a privacidade deve ser vista como a proteção contra qualquer forma de controle, o direito de manter o controle de suas informações e de determinar se elas serão acessadas ou não. Dessa forma nasceu o direito a auto determinação informativa. (RODOTÀ, 2008)

Tem-se com isso, a primeira manifestação de um direito à autodeterminação informativa com uma decisão da Corte Constitucional alemã em 1983. Nesta, a Corte julgava aspectos da Lei do Censo, foi realizada então uma interpretação conjugada do princípio da dignidade humana com o direito ao livre desenvolvimento da personalidade, gerando o princípio implícito da autodeterminação informativa, autorizando a cada indivíduo decidir sobre divulgação e utilização de seus dados pessoais. (SARLET, 2020)

A internet trouxe consigo transformações para a intimidade, contribuindo assim para o nascimento de um homem mais flexível, mais sensível a autorizações envolvendo seus dados, tornando a privacidade cada vez mais frágil e necessária. O objetivo do direito à privacidade é evitar discriminações ou exclusões, ou seja, não é favorecer a solidão mas garantir a igualdade, se a determinado direito é atribuída uma tutela particularmente forte é para proteção

do mesmo. (RODOTÀ, 2008)

As novas dinâmicas sociais desenharam-se a partir da informação, inicialmente era o Estado que detinha o poder de utilizar de informações pessoais, a partir da realização de censos e pesquisas, por exemplo. Estas informações coletadas acabavam por aumentar o poder de controle do Estado sobre os indivíduos, assim tal atividade começou a ser largamente utilizada no ambiente público, enquanto no ambiente privado a atividade não era tão atraente por conta de altos custos. (DONEDA, 2006)

Com o desenvolvimento de novas tecnologias para coleta e processamento de dados, o custo para realização da atividade diminuiu e novas maneiras surgiram, sendo assim, os interessados privados começaram a utilizar desses mecanismos para seu proveito, como o Estado já fazia. Assim, o professor Danilo Doneda (2006) conclui que a informação vai aumentar na medida em que a tecnologia passa a oferecer novos meios para transformá-la em utilidade, por um custo acessível – portanto o que tornou essa forma de invasão viável é ser possível a coleta.

Além disso, fortaleceu-se os problemas quanto a ideia de que a privacidade estava com os dias contados, problemas associados com escritos como o Big Brother de Orwell, do seu livro 1984, o qual disseminou um alarme quanto ao fim da privacidade, tendo simbolizado pela tela de uma televisão (algo presente em todas as casas) uma câmera de uso estatal, ecoou como um grande sinal do que poderia vir nos próximos anos. (ORWELL, 2009)

Danilo Doneda (2006) faz menção à alguns “mitos da privacidade” que seriam as noções da sobrevalorização da tecnologia, em que esta seria uma arma perigosa, enquanto na realidade, para o autor, o arsenal de controle democrático continua funcionando e se renovando, fazendo com que essas histórias continuem sendo apenas mitos.

Todavia, uma leitura mais atual acaba por compreender essa tese de que estaria-se vivendo o “fim da privacidade”, isso por conta da massiva auto exposição nas mídias sociais, na utilização de aplicativos que solicitam o acesso a informações de várias naturezas (como câmera e localização), entre outros aspectos de vigilância e monitoramento. (SARLET, 2019)

Stefano Rodotà (2008, p.144) leciona que há mais de trinta anos já era possível encontrar títulos anunciando a morte da privacidade e outros adjacentes, entretanto, existem duas diferenças entre esse debate com o que vem sendo feito hoje em dia. Antes, o fim da privacidade era abordado em livros acadêmicos, enquanto hoje é parte do debate leigo.

A segunda mudança seria a forma como se reage à esse fim, hoje em dia é espalhado que a privacidade deve ser considerada “como um parêntese da modernidade”, ou seja, os interesses do mercado acabam eliminando os espaços privados. Para o autor essa ideia deve ser

criticada já que existem muitas regras que buscam proteger esse espaço pessoal e as pressões contra a auto regulamentação em países como os Estados Unidos. (RODOTA, 2008)

A questão aqui é a de que, mesmo com normas regulando a privacidade, seria o mercado que controlaria até que ponto tem-se a liberdade de definir esses parâmetros. Na sociedade atual em que as informações são ouro, a tutela da privacidade é essencial para o equilíbrio dos poderes, o fim da privacidade apresenta um risco não somente às liberdades individuais mas também um risco à democracia, já que o acúmulo de informações pessoais gera discriminações e contribui decisivamente para o desequilíbrio de poder. (RODOTA, 2008)

Ingo Wolfgang Sarlet (2019, p.639) afirma que até o momento não temos como definir com precisão em que consiste o direito à privacidade, podendo apenas identificarmos alguns parâmetros. A Constituição Federal de 1988 foi a primeira a trazer expressamente o direito de proteção da vida privada e da intimidade, um dos mais relevantes atualmente, para o autor a preservação da esfera da vida privada “é essencial para à própria saúde mental do ser humano e lhe assegura as condições para o livre desenvolvimento de sua personalidade”.

O direito à privacidade opera em dupla dimensão: uma objetiva e uma subjetiva, isso quer dizer que enquanto direito subjetivo tem-se um dever do estado e de terceiros de se absterem, não interferirem na vida privada do cidadão, além deste poder dispor livremente sobre suas escolhas de vida. (SARLET, 2019)

Quanto a dimensão objetiva, temos um dever de ação do Estado no sentido de proteção da privacidade e no sentido de garantir “condições constitutivas da fruição da vida privada”. Sendo assim, o Estado possui dois deveres ambivalentes quanto ao direito à privacidade, devendo se abster ou agir dependendo do caso. (SARLET, 2019)

Com isso, pode-se entender a importância do direito à privacidade dentro de um estado democrático de direito como algo essencial para o desenvolvimento da personalidade e diversas outras liberdades fundamentais. O caráter eminentemente burguês do direito à privacidade era existente, proveniente da ideia de que somente os burgueses poderiam ter direito ao isolamento e relacionada diretamente com a questão da propriedade.

Entretanto, com o crescente fluxo de informações e sua demasiada importância, não são apenas as pessoas de grande relevo social que estão em risco de ter sua privacidade violada, mas sim grande parte da população em variadas situações. (DONEDA, 2006)

Nos últimos anos, essas variadas situações foram expandidas já que cada vez mais tecnologias introduzem objetos de sistema automatizado que funcionam praticamente sozinhos, como assistentes virtuais como a *Alexa* da *Amazon*, ou relógios inteligentes que disponibilizam com outros usuários informações diversas.

Essas novas tecnologias são denominadas de Internet Coisas (*IoT – Internet of Things*)³ e são mais um exemplo de como apenas com acesso a determinada tecnologia é possível serem adquiridos dados sobre o adquirente, de forma indiscriminada e sem motivo aparente, os dados são coletados e guardados para discriminar aquele sujeito dos outros.

Não é fácil distinguir os níveis de proteção do direito à privacidade, todavia, o que pode ser levado deste tópico é que atualmente a *privacy* é muito mais do que apenas o direito *to be let alone*, existem diversos problemas e características em jogo sendo necessária salvaguarda-la como direito fundamental importantíssimo. A privacidade na era da informação foi impactada, assim como todo o sistema social, político e econômico com o ingresso dos computadores e da internet.

Da privacidade ao reconhecimento de um direito à autodeterminação informativa, tem-se o surgimento de um direito à proteção de dados pessoais, este deve ser visto como uma promessa – o *habeas corpus* – que deveria ser transmutada do corpo físico para o corpo eletrônico. Assim, a inviolabilidade da pessoa deve ser arguida na dimensão digital, o direito fundamental à proteção de dados deve ser defendido e garantido expressamente como se verá no próximo capítulo. (RODOTÀ, 2008)

2.3 O impacto da tecnologia na democracia

A Constituição Federal de 1988 traz em seu bojo o princípio do Estado Democrático de Direito, a democracia como forma de governo, caracterizada como “governo do povo”. Isso quer dizer que o Estado é formado por uma lei fundamental escrita (Constituição) e pressupõe um modelo de legitimação (a vontade da maioria). (CANOTILHO, 1993)

A democracia não foi inventada de uma vez, seu surgimento é rodeado de bastante incerteza mas seu primeiro registro vem a ser na Grécia Antiga, por volta do século V a.C, esta foi a primeira experiência em que uma parcela do povo (homens adultos livres) participou ativamente das decisões políticas. (DAHL, 2012)

Na visão grega, as pessoas são seres sociais e por isso, para existir plenamente era preciso participar das decisões na ágora, reuniões em que se decidiam os assuntos públicos.

³ Esse é um ambiente de objetos interconectados com a internet que criam “um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia” (MAGRANI, 2018, p.20)

Ademais, o ideal seriam cidades não muito grandes, já que o tamanho interferiria na participação do povo e para a polis grega, a vida política é uma extensão da pessoa – uma harmonia necessária. Entretanto, sabe-se que esse ideal por mais que influente às democracias modernas, não é possível em sua totalidade. (DAHL, 2012)

Para começar, as pessoas não vivem mais em cidade-estado mas em um país – temos assim um território inimaginável para o exercício da democracia dos atenienses. Além disso, o estado democrático moderno é caracterizado pelo conflito político e não pela harmonia nas relações.

A questão é que, a democracia atual é muito mais que a vontade da maioria, para começar tem-se um governo representativo e não direto como era a ideia do século V, a.C. Para destrinchar essa ideia é necessário introduzir a ideia de república, os republicanos defendem uma separação institucional dos três poderes: legislativo, judiciário e executivo, assim caso um destes poderes se concentre em uma só pessoa, tem-se a tirania. (DAHL, 2012)

Mais tardar, os cidadãos começaram a viver cada vez mais distantes da polis, dificultando sua ida as reuniões públicas, assim na prática as assembleias foram transformadas em “corpos representativos”, foi preciso então encarar como a democracia funcionaria em uma república de grandes proporções. Nasceu assim a possibilidade de um poder consistir em representantes eleitos e não em cada um do povo, em estados de grandes proporções (como é o caso dos países) devem ser escolhidos representantes por meio da eleições, podendo “descartá-los nas eleições seguintes”. (DAHL, 2012, p. 42)

A democracia moderna brasileira é composta por um governo representativo onde a população escolhe os representantes por meio do voto e estes tomarão as decisões em nome do povo.

Noberto Bobbio (1999) realiza uma leitura da ideia de democracia em que afirma que é o modo pelo qual um conjunto de regras estabelece quem está autorizado a tomar decisões, fazendo-se uso da “regra da maioria”, o que trazendo para o campo eleitoral atual significa que ganham as eleições quem detêm maior número de votos. No Brasil, funcionam pelo sistema majoritário (critério quantitativo) as eleições dos cargos do executivo – prefeito, governador, presidente – e do senado.

Conceituar a democracia moderna é uma tarefa árdua, mas etimologicamente pode-se entender como a lógica da soberania popular (eleição de representantes que concorrerão a cargos políticos), sendo a democracia de fato ainda mais que isso, incluindo uma proteção sobre: “a supremacia da Constituição, a existência de direitos fundamentais, da legalidade das ações estatais; um sistema de garantias jurídicas e processuais”. (FERNANDES, 2017, p.299)

J.J Gomes Canotilho (1993, p.54) leciona que a política “é o campo das decisões obrigatórias” que buscam a conservação da sociedade, como a paz, a segurança, a saúde e outras decisões de cunho social importante. Para o autor, além das regras constitucionais dispostas existe um espaço de jogo aberto para o uso da criatividade e estratégia dos jogadores – um jogo político. Ora, isso quer dizer que a política pressupõe a possibilidade de escolha, pode-se escolher quem irá tomar àquelas decisões obrigatórias.

Ademais, como decorrido ao longo de tópico anterior, a era da informação modificou todas as áreas da vida moderna, alterando o meio em que se fazem compras, em que se realizam reuniões e conseqüentemente alterando o meio em que se elegem candidatos. (GOMES, 2018)

Nos últimos anos, observa-se uma crescente modificação no modo de participação popular no Brasil e em diversos outros países, durante muito tempo o exercício do voto se concentrou em um debate preguiçoso já que dominado por oligarquias, entretanto, com a entrada da internet e das redes sociais houve uma maior politização dos cidadãos. Em contrapartida, na mesma crescente da politização também teve-se da desinformação.

Wilson Gomes (2018) leciona que a democracia digital seria a filha da curva do milênio, ou seja, seria uma herança advinda com os anos 2000 e que reflete a velocidade da internet e dos meios de comunicação eletrônicos. Assim, tem-se o debate quanto a democracia na era da tecnologia, o que futuramente se denominou de democracia digital ou e-democracia.

A internet trouxe consigo grandes mudanças, todavia, não pode se dizer que essas mudanças geraram uma reconfiguração pelas multidões. As manifestações no início da década, como a primavera árabe e as jornadas de junho de 2013 no Brasil, são demonstrações de como a rede conseguiu unir os eleitores em prol da busca de direitos, entretanto, ao mesmo tempo que as forças democráticas foram exercidas, também se obteve o crescimento de manifestações fascistas e discursos antidemocráticos na web. (SILVEIRA, 2019)

As eleições norte americanas de 2016 e brasileiras de 2018 são um exemplo disso, como será aprofundado posteriormente, com a segmentação de publicidade eleitoral e divulgação de notícias falsas, é crescente a dúvida quanto a sobrevivência da democracia na era da pós verdade⁴. (SILVEIRA, 2019)

Stefano Rodotà (2008, p.141) afirmou “Mudam os tempos, transforma-se a democracia”, é claro que ao passo do desenvolvimento tecnológico essas mesmas tecnologias

⁴ O dicionário Oxford definiu pós-verdade como “circunstâncias nas quais os fatos objetivos são menos influentes na formação da opinião pública do que os apelos à emoção e à crença pessoal” < <https://dictionary.cambridge.org/pt/dicionario/ingles/post-truth> >.

podem afetar diretamente o ambiente democrático. O que antes era possível somente em ambiente físico, transmutou-se ao ambiente virtual, um ambiente sem fronteiras em que tem-se um debate aberto e constante sobre qualquer tipo de informação.

Com o crescimento do espaço na internet, tem-se o crescimento de rumores, rumores que em seguida se transformam em notícias e quando essas notícias dizem respeito ao processo democrático tem-se um perigo iminente.

Nos anos 70 começam as especulações sobre as inserções futuras entre democracia e tecnologia, na época ainda sem a internet ter se tornado algo relevante, os efeitos das novas tecnologias diziam respeito aos satélites, televisão interativa, computadores, entre outros. Deste modo, a primeira fase da ideia de democracia eletrônica consiste na “teledemocracia”, a qual no sentido mais rápido se referia ao telefone e a televisão. Este termo guardava a ideia de uma tecnologia que permitiria aos grupos se comunicassem uns com os outros para produzir decisões, sem a necessidade de sair de casa. (GOMES, 2018)

Alguns anos depois, a ideia de democracia tecnológica foi amadurecendo e entre críticas e desconfianças não se pode mais negar o potencial desse modelo, o professor Wilson Gomes (2018, p.50) lecionando sobre as dimensões da democracia digital disserta sobre o caso da:

[...] informação, temos a questão de como os cidadãos podem obter informação sobre políticas públicas, governo e sistema político para, justamente, tomar as decisões políticas que lhe concernem no regime democrático, como a decisão eleitoral, o acompanhamento da política e o engajamento na defesa de seus interesses.

Tem-se assim, a preocupação com a obtenção de informação dos cidadãos por meio das tecnologias já que isso afeta as decisões políticas, como a decisão eleitoral. É claro desde da década de 90, com a popularização da internet, que as TICs modificariam as relações sociais e também as relações políticas, já que elas facilitam o acesso às informações de maneira mais veloz do que a mídia tradicional.

Pierre Levy (1999, p.30) leciona sobre o ciberespaço como suporte de uma inteligência coletiva, o que isso transpassa é que com o crescimento das tecnologias se tem um espaço propício a essa inteligência. Entretanto, o autor afirma que surgiriam nas redes outras formas de crescimento como a do que ele optou chamar de “bobagem coletiva”, que seriam rumores, conformismo e acúmulo de dados sem qualquer informação. Realizando uma leitura contemporânea, podemos relacionar essa forma de crescimento com o que hoje vemos com a desinformação e as “fake news”⁵.

⁵ O dicionário de Oxford definiu *fake news* como sendo: “histórias falsas que possuem aparência de notícias, espalhadas na internet ou usando outra mídia, normalmente criada para influenciar eleitores ou usada como piada”.

Atualmente, tem-se diversas tentativas de manipulação com notícias falsas e imagens adulteradas, fora do contexto, e estas são expostas também dentro do processo eleitoral, como foi visto no Brasil em 2018. Existe uma legítima preocupação com os entornos desses acontecimentos, já que podem levar a existência de posicionamentos e ações contra uma pessoa/um candidato que influem diretamente na liberdade de escolha do eleitor quando é transbordado com desinformação. (SILVEIRA, 2019)

Wilson Gomes (2018) afirma que a partir de 1996 a democracia digital decola, com a chegada dos anos 2000 a tendência se consolida com os sites de relacionamento e mídias sociais e é a partir de 2006 que a conexão se liberta dos computadores e passa a ser portátil, a partir dos celulares, o que leva a presente década marcada por uma hiperconexão (utilização excessiva dos meios de comunicação).

Sendo assim, chega-se ao que seria uma democracia digital, Wilson Gomes (2005) em um artigo de mais de uma década atrás já lecionava que está democracia seria uma experiência, da internet e outros dispositivos, voltados para o incremento da participação civil dentro de assuntos do Estado, ou seja, a soberania popular sendo exercida por meio das TIC's.

A globalização se concretizou como um estímulo à urbanização e metropolização das cidades, as conhecidas hoje como cidades inteligentes são produto das ondas tecnológicas, é o digital a serviço do urbano. O conceito de cidade inteligente nasceu das gigantes da tecnologia da informação e comunicação, com intuito de remediar os erros do passado com a informatização, tem-se que onde existisse altos índices de criminalidade se implantariam câmeras de monitoramento, onde houvesse desperdício se empenharia eficiência. Sendo assim, as cidades inteligentes se articulam em torno de eixos: o desenvolvimento econômico, a redução da pegada ambiental e a melhoria da qualidade de vida dos cidadãos a partir das TIC's. (SOUPIZET, 2017)

Além do fenômeno das cidades inteligentes, existem outros tipos de mudanças na estrutura política como a forma em que a interação dos cidadãos tanto com o ambiente público como com o privado foi alterada. Agora essa relação é mediada pela tecnologia e com o acesso aos dados dos usuários, estes ficam cada vez mais expostos ao poder de manipulação que podem certos atores exercer. Em relação a propaganda política, por exemplo, estas estão cada vez mais segmentadas de acordo com o perfil de cada eleitor, sendo produzidas de acordo com suas afinidades e preconceitos. Deste modo, as novas tecnologias colocam em xeque a privacidade e autonomia dos indivíduos. (ANTONIALI; CRUZ, 2017)

Por fim, Robert A. Dahl (2001) em sua obra “Sobre a democracia” se debruça sobre o porquê as eleições devem ser livres, justas e frequentes. Para o autor, livres significaria que os cidadãos poderiam ir às urnas sem temor de represálias, justas significaria que todos os votos devem ser contados igualmente e frequentes significa que deve sempre haver a renovação do representante. Permita-me aqui fazer uma leitura conjunta à ideia de democracia digital exposta e o panorama político-social em que se vive.

Eleições livres e justas atualmente seriam concretizadas somente com o exercício do direito do voto secreto e da igualdade? Bem, eleições livres e justas vão ser mais que isso, são aquelas em que não há medo de represálias no momento do voto nem diferenciação entre as pessoas mas, também aquelas em que não há a manipulação da vontade popular, como por meio de direcionamento de conteúdo realizado a partir de informações obtidas sem transparência, como com o uso intenso de *bots* e com a propagação de *fake news*. Não há eleições livres e justas sem transparência e proteção à dados pessoais.

Sendo assim, pode-se compreender a partir deste tópico que a democracia também foi afetada com o avanço tecnológico, a democracia digital acontece a partir do uso dos meios digitais, como as redes sociais, em que debates e manifestações políticas podem ocorrer. Certo é que isso alterou o modo como se “fazia política” e construiu um novo mundo, voltado a uma nova compreensão do que são eleições e como estas funcionam.

3 O TRATAMENTO DE DADOS PESSOAIS NO PROCESSO DEMOCRÁTICO

Neste capítulo, será introduzida a ideia de um direito fundamental à proteção de dados pessoais na ordem jurídica brasileira, compreendendo a existência da cláusula de abertura para a interpretação de um direito fundamental implícito e a recente decisão do Supremo que reconheceu a autonomia do direito. Também será abordada a distinção entre dado e informação para poder se entender a dupla dimensão subjetiva e objetiva do direito, além da compreensão de quem são os titulares e destinatários desse direito fundamental. Ademais, será discutida a relação do direito à proteção de dados com outros direitos, como o direito de personalidade.

Em seguida, será compreendida a ideia de Big Data e como funcionam os bancos de dados para a realização do tratamento de dados pessoais, visualizando com exemplos como a coleta de dados pode inferir na probabilidade de acontecimentos futuros. Por fim, analisar-se-á como o tratamento de dados pode interferir na democracia, utilizando do caso da *Cambridge Analytica* para demonstrar o poder do big data em um processo eleitoral.

3.1 A proteção de dados pessoais como direito fundamental

Como já pincelado anteriormente, os avanços tecnológicos e a ampla digitalização da vida moderna assumiram um “caráter onipresente”, impactando em diversas esferas da sociedade. O crescente uso dessas redes trouxe consigo a importância da proteção dos dados pessoais, proteção esta que ainda hoje não encontra observância expressa em diversas Constituições, como é o caso do Brasil. (SARLET, 2020)

Historicamente, a primeira vez que o direito à proteção de dados adquiriu caráter de direito fundamental autônomo foi na Convenção de Estrasburgo (1981) e dois anos depois ocorreu o primeiro reconhecimento ao direito de autodeterminação informativa na Alemanha, com uma decisão do Tribunal Constitucional alemão, já dissertada no capítulo anterior. (SARLET, 2020)

A Constituição Federal brasileira em seu artigo 5º menciona o direito ao sigilo das comunicações de dados, o que para muitos significaria uma aproximação ao direito à proteção de dados pessoais, entretanto, é preciso observá-lo com cautela. O objeto protegido no direito do art. 5º, inciso XII, diz respeito a troca de informações que não pode ser infringida e não sobre a proteção aos dados em si. (DONEDA, 2011)

A existência de uma decisão do Supremo Tribunal Federal leciona em tal sentido, relatada pelo Ministro Sepúlveda Pertence, a decisão reconheceu expressamente a inexistência da garantia de inviabilidade de dados armazenados em computador. Esta então foi utilizada diversas vezes para afirmar que a natureza da proteção de dados estaria restrita a sua comunicação, de acordo com a Constituição. (DONEDA, 2011)

Ainda, o direito à proteção de dados encontra salvaguarda no inciso LXXII do artigo 5º da Constituição Federal, este prevê a Ação de Habeas Data, ação constitucional que busca assegurar o conhecimento e a retificação de dados constantes de registros ou bancos de dados públicos. Esta também não se confunde com um direito explícito mas trata de uma ação que busca proteger o conhecimento de dados. (BRASIL, 1998)

Certo é que, o Brasil nada dispõe em sua Constituição Federal sobre um direito à proteção de dados pessoais, entretanto, este pode ser lido a partir da interpretação de outros direitos explicitamente consagrados na Carta Magna, assim como ocorreu em outras ordens constitucionais. São estes o princípio da dignidade humana, o direito ao livre desenvolvimento da personalidade, bem como os direitos à privacidade e à intimidade. (SARLET, 2020)

Isso porque, o artigo 5º §2º da Constituição Federal determinou a abertura do catálogo de direitos fundamentais. Os direitos fundamentais em sentido formal são todos aqueles dispostos na Constituição, enquanto os direitos fundamentais em sentido material são aqueles que apesar de não estarem no catálogo podem ser equiparados aos direitos formalmente fundamentais. (SARLET, 2019)

Portanto, a Constituição Federal se apresenta como um processo aberto para aquisição de novos direitos fundamentais, dessa forma é possível classificar os direitos implicitamente positivados como aqueles decorrentes de uma extensão de determinado direito fundamental e é aqui que se encontra o direito à proteção de dados. (SARLET, 2019)

Ingo Sarlet (2020) leciona que o direito à autodeterminação informativa guarda relação direta com o direito à proteção de dados, aquele decorrente do direito ao livre desenvolvimento da personalidade. Tal direito à autodeterminação informativa veio disciplinado na recente Lei Geral de Proteção de Dados brasileira como um de seus fundamentos. O entendimento consagrado na literatura brasileira é o de que o direito à proteção de dados pessoais foi consagrado na Constituição Federal de 1988 como um direito fundamental implicitamente positivado.

Ademais, cumpre relatar recente decisão do Supremo Tribunal Federal que teve como relatora a Ministra Rosa Weber e suspendeu a Medida Provisória 954/2020, esta obrigava empresas de telecomunicação a ceder dados pessoais dos seus clientes para que o IBGE os

utilizassem em uma pesquisa por amostragem de domicílios. Esta MP foi impugnada por diversos partidos por conta da violação à intimidade, vida privada e ao sigilo de dados. Além disso, haviam claros vícios na medida como os de finalidade e necessidade para realização da pesquisa e também falta de supervisão para garantir que não houvessem abusos – a ausência de uma Autoridade Nacional de Proteção de Dados. (DATAPRIVACY BRASIL, 2020)

Então, o STF em maio de 2020, ainda com a LGPD em vacância, por 10 votos a 1 suspendeu essa MP e relatou que mesmo sendo para fins estatísticos, o que preocupa quanto a coleta de dados seria a eventual reutilização dos dados, como exemplo para otimização de disparos de mensagens. Assim, os ministros foram claros quanto ao fato de que não existe dado insignificante, os dados merecem proteção independentemente de serem públicos ou privados. Esta decisão concretizou a autonomia do direito de proteção de dados no Brasil, assim como àquela decisão do Tribunal Constitucional Alemão consagrou o direito à autodeterminação na Alemanha, ambas são decisões paradigmas ao se tratar do direito fundamental à proteção de dados. (DATAPRIVACY BRASIL, 2020)

Assim como o direito à privacidade, mencionado no capítulo anterior, o direito fundamental à proteção de dados pessoais também possui uma dupla dimensão subjetiva e objetiva. A dimensão subjetiva diz respeito a existência de uma atuação negativa ou positiva do poder público, enquanto a dimensão objetiva perpassa àquela perspectiva e coloca os direitos fundamentais como um norte que fundamenta todo o ordenamento jurídico, sendo assim, o direito fundamental é uma orientação a ser seguida para aplicação e interpretação de todas as outras normas, sejam elas constitucionais ou infraconstitucionais. (FERNANDES, 2017)

Aqui cumpre estabelecer o que é a informação e o que é dado, este último diz respeito a uma espécie de “pré-informação”, seria anterior ao processo de elaboração e interpretação. Já a informação é algo além da representação do que está no dado, esta já transmite uma identificação, um sentido. Portanto, pode-se concluir que o dado sozinho não leva a uma cognição, diferente da informação, cada um possui seu significado, mesmo a doutrina muitas vezes tratando-os indistintamente. (DONEDA, 2011)

Danilo Doneda (2006, p.157) aborda a teoria jurídica da informação, a qual subdivide está em categorias, uma delas sendo a da informação pessoal: “o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta”. Ademais, essa informação pessoal também é agrupada em subcategorias, dando origem a categoria dos dados sensíveis. Os dados sensíveis seriam aqueles sobre sexo, raça, orientação sexual, posicionamento político, religião, enfim qualquer dado que possa identificar um indivíduo e de certa forma resultar em

discriminação deste⁶. Sendo assim, quando tratar-se de dados sensíveis é necessária maior cautela, destinando-os sempre a fins lícitos e transparentes.

Quanto a dimensão subjetiva do direito à proteção de dados, Ingo Wolfgang Sarlet (2020) verifica que tal proteção, mesmo que não explícita no texto constitucional, encontra fundamento na legislação infraconstitucional, como nos artigos da Lei Geral de Proteção de dados, da Lei de Acesso à Informação ou do Marco Civil da Internet. A leitura dos artigos 17 e 18 da LGPD ao tratar sobre os direitos do titular trazem provas que concretizam tal direito como negativo e positivo; o direito da pessoa ter sua privacidade e intimidade respeitada e ao mesmo tempo poder obter do controlador a qualquer momento a confirmação da existência de tratamento, ou outras coisas, mediante requisição. (SARLET, 2020)

Quanto a dimensão objetiva, cumpre tratar primeiramente do seu efeito irradiante, como pincelado anteriormente, essa percepção diz que o direito vai repercutir no ordenamento jurídico, fornecendo diretrizes para o legislativo, executivo e judiciário. Outra função seria o denominado poder de proteção do Estado, este deve zelar pelo direito contra agressões dos poderes públicos e até mesmo de particulares ou de outros estados. Além de claro, a criação e constituição de organizações, como exemplo no que se dá com a constituição de uma Autoridade Nacional de Proteção de Dados. (SARLET, 2020)

Ademais, importante tratar dos titulares e destinatários do direito fundamental à proteção de dados, estes são dois polos que se relacionam juridicamente, o titular é àquele que demanda o direito, enquanto o destinatário é quem é demandado. (FERNANDES, 2017) No caso dos seus titulares, vale realizar a leitura do artigo 5º da LGPD (BRASIL, 2018): “Art. 5º Para os fins desta Lei, considera-se: V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”.

Assim, em primeira linha os titulares do direito são as pessoas naturais, entretanto, isso não significa que são todas as pessoas ou somente estas que podem ser titulares de direitos fundamentais. O artigo 5º da Constituição Federal afirma que são titulares os brasileiros e estrangeiros residentes no país, porém, o Supremo Tribunal Federal reconhece desde os anos 90 que os estrangeiros, mesmo não residentes, possuem a condição de titulares. Outra situação acobertada por decisão do STF é a das pessoas jurídicas, estas são igualmente titulares de alguns direitos fundamentais. (FERNANDES, 2017)

⁶ Existem críticas quanto a essa noção de dados sensíveis, a mais propagada afirma que é impossível definir previamente o impacto de uma informação, seja ela qual for, já que qualquer dado sendo tratado pode revelar aspectos da personalidade de alguém, essa corrente conclui que não seria o dado em si perigoso ou discriminatório, mas tudo depende do seu uso. (DONEDA, 2011)

Quanto às pessoas jurídicas como titulares do direito em discussão, Ingo Wolfgang Sarlet (2020) segue o entendimento majoritário de que o direito à proteção de dados possui apenas pessoas naturais como titulares, isso porque as pessoas jurídicas já seriam protegidas por outros direitos, como pelo sigilo industrial. Mesmo assim, não se nega que as pessoas jurídicas podem ser titulares de direito fundamental quando compatíveis (art. 52, Código Civil), de acordo com cada caso.

Ademais, resta conhecer os destinatários do direito, estes são tanto o Estado como os particulares, já que o acesso e utilização de dados pessoais ocorre nos dois ambientes e decorrem de ações e omissões de qualquer ente. Isso significa que os atores devem concretizar o direito assegurando a condição negativa e positiva do direito, assim como sua dimensão objetiva. (SARLET, 2020)

Percebe-se assim, que o direito à proteção de dados pessoais foi e vem sendo identificado em muitos países como um princípio deduzido de outros expressamente veiculados, nos respectivos ordenamentos jurídicos. No Brasil, por mais que já tenhamos o reconhecimento de um direito implícito e uma decisão do STF reconhecendo a autonomia do direito, está em trâmite a PEC 17/2019 que propõe inserir no artigo 5º um direito expresso à proteção de dados pessoais. (BRASIL)

Compreendido o que é o tratamento de dados pessoais, importa reconhecer os impactos que este método possui em outros direitos fundamentais. Ingo Sarlet (2020) leciona que inexistem dados pessoais irrelevantes diante da sociedade da informação e seu processo eletrônico, isso porque os dados são projeções da personalidade, ou seja, qualquer tratamento que obtenha pode vir a ferir direitos fundamentais.

O professor ainda, afirma que o direito mais próximo de um direito fundamental à proteção de dados é justamente o direito ao livre desenvolvimento da personalidade, incluindo assim a livre disposição dos dados pessoais, o direito à livre autodeterminação informativa.

O direito de personalidade nem sempre foi auferido com grande importância ao direito civil, a partir de uma leitura histórica é possível analisar que existiu um momento onde importava apenas a propriedade, a perspectiva era a de que somente era possível proteger o material. Contudo, após a segunda guerra e a proliferação do princípio da dignidade da pessoa humana em diversas constituições, ocorreu a despatrimonialização do direito civil posicionando o ser humano como centro do foco jurídico, a pessoa e em específico sua personalidade também mereciam proteção. (BIONI, 2019)

Necessário se faz caracterizar o que são os direitos de personalidade, para Costa e Oliveira (2019, p.30) estes seriam aqueles “inerentes a elementos corpóreos e incorpóreos que

caracterizam e diferenciam uma pessoa”, ou seja, o direito de personalidade protege aquelas informações que identificam uma pessoa, identificam sua expressão.

Deste modo, um dado conjugado à esfera de uma pessoa pode ser compactuado dentro do direito à personalidade, para tanto o dado deve ser pessoal “caracterizando-se como uma projeção, extensão ou dimensão do seu titular”. Bruno Bioni (2019) utiliza a denominação de Daniel J. Solove: “dossiês digitais” para expressar as novas informações que devem ser corretamente projetadas a personalidade, as informações proveniente das tecnologias de informação e comunicação, e isso acabaria por justificar os dados pessoais como direito de personalidade, tendo como exemplo a retificação de dados pessoais já que estes influem na projeção de uma pessoa. (BIONI, 2019)

A proteção dos dados pessoais, como um novo direito da personalidade, dirige-se a todo e qualquer dado em que se denote o prolongamento de um sujeito. Dados pessoais não se limitam, portanto, a um tipo de projeção imediata, mas, também, a um referencial mediato que pode ter ingerência na esfera de uma pessoa. (BIONI, 2019)

Mediante tal afirmação, pode-se concluir que a proteção de dados pessoais como um direito de personalidade inclui tantos os dados que identificam a pessoa imediatamente como aqueles em que podem vir a ser identificados.

O direito de personalidade embora tenha como objetivo a proteção da esfera pessoal do indivíduo, também é um direito de liberdade já que é o direito de qualquer pessoa não ser impedida de desenvolver sua personalidade e de decidir de acordo com suas próprias opções – direito ao livre desenvolvimento da personalidade. (SARLET, 2019)

Outrossim, é importante dissertar sobre outros direitos do catálogo que fazem inferência junto ao direito à proteção de dados como o direito à intimidade, à liberdade de expressão e à cidadania.

Na CF foi reconhecida a proteção tanto da privacidade como da intimidade, sendo o primeiro sobre relações referentes aos comportamentos pessoais em geral ao passo que o segundo trata de uma esfera mais íntima da vida do indivíduo. Portanto, a intimidade é incluída no âmbito de proteção do direito à vida privada. Outro direito relacionado é o direito à liberdade de expressão, este foi consagrado na CF orientando ser livre a manifestação de pensamento, sendo vedado o anonimato. (SARLET, 2019)

O direito à cidadania também foi consagrado na Constituição Federal, ele se refere a participação política das pessoas na formação da vontade estatal, sendo assim, o cidadão é aquele que participa ativamente e tem seus direitos e garantias assegurados. (FERNANDES,2017)

Ora, o acesso à dados pessoais em processos eleitorais tem ligação direta com o direito à cidadania, à liberdade de expressão, ao livre desenvolvimento da personalidade e à intimidade. Inicialmente, tem-se que ao dispor de dados sobre um usuário por vezes estaria se adentrando na esfera íntima do mesmo, já que trata de um dado sensível envolvendo opinião política. Quando dessa opinião se estabelece um tratamento de dados, isso pode influir diretamente no livre desenvolvimento da personalidade do indivíduo já que direciona a escolha de um certo posicionamento.

Ainda, a liberdade de expressão caminha lado a lado ao direito à proteção de dados já que dispor do pensamento nas redes é essencial para a concretização desta liberdade, além disso a participação política na internet corresponde ao direito à cidadania de todo cidadão, sendo assim, inegável a compreensão de que o direito à proteção de dados possui conexão direta com outros direitos do catálogo.

3.2 Big Data e a técnica de tratamento de dados

Alguns autores conceituam Big Data como sendo o êxtase da era da informação, é um termo usado para descrever bancos de dados cujo o tamanho é gigante, mantidos por empresas, organizações e órgãos governamentais. Este é um processo capaz de fornecer critérios para tomada de decisões, a partir da coleta de dados provenientes de diferentes bases no intuito de produzir informações utilizáveis pelo seu mantenedor. (ARRUDA, 2018)

Os bancos de dados envolvem a entrada e processamento de dados com a saída de informações, para tanto é necessário uma administração sobre a pré-informação (o dado) até que se chegue a um conhecimento (informação). Por conta disso, as TIC's são de extrema importância, já que é a partir da automatização que se tornou possível o processamento desses bancos de dados de forma mais rápida e em grande quantidade. (BIONI, 2019)

Danilo Doneda (2011, p. 2) conceitua:

Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações.

Ou seja, é onde ocorre a acumulação de dados pessoais dos usuários para serem utilizados em proveito de terceiros, algo que o professor comenta não ser algo novo mas sim

existente em qualquer época, o que muda é que hoje tem-se maior capacidade de armazenamento e comunicação – a novidade advinda com os computadores e a internet.

Sendo assim, os bancos de dados são espaços em que circulam informações de diversas pessoas e essas informações são constantes, é uma coleta quase que automática. É nesse ambiente que surgiram os denominados “*data brokers*” que acumulam o maior número possível de dados para oferecer diferentes serviços, sendo a base desses serviços os dados dos usuários. (BIONI, 2019)

Interessa nesse trabalho dissertar sobre um tipo de banco de dados, os chamados *data warehouses*, estes são alimentados por um ser humano e em seguida, o sistema de gerenciamento permite identificar fatores determinantes quanto a tomada de decisões. Bruno Bioni (2019) leciona que essa dinâmica sobre os usuários da internet é manuseada para ser utilizada como direcionamento de mensagens publicitárias, sendo assim possível a publicidade comportamental – a qual será destrinchada em tópico posterior.

O Big Data é atrelado a 6V’s: volume, velocidade, variedade, valor, veracidade e validação. O volume diz respeito a capacidade de organizar uma quantidade antes inimaginável de dados. A velocidade reflete quão rápido pode ser a coleta, análise e armazenamento. A variedade diz respeito aos diversos formatos possíveis de dados e fontes. (ARRUDA, 2018)

Quanto ao valor se refere a importância dos dados coletados, quanto mais antigo o dado menor o seu valor. Já a veracidade diz respeito a precisão de dados coletados para assim assegurar a confiança no resultado. Por fim, a validação diz respeito a utilização das informações obtidas observando os padrões da ética e do direito. Todas essas características dizem respeito ao conceito de Big Data, o qual não terá nenhum valor caso não possua essas 6 características. (ARRUDA, 2018)

Para Vinicius Cervantes Gorgone Arruda (2018) o crescimento das atividades de tratamento de dados traz grandes desafios já que o uso bem sucedido do big data possui barreiras como as consequências ao mercado, a privacidade, propriedade e outros desafios. A questão é que muitas vezes o tratamento de dados é feito de forma indiscriminada, sem serem observados critérios, como o que o autor elenca como a validação, muitas vezes o tratamento de dados é realizado sem a observância aos padrões de ética.

Deste modo, o Big Data é o resultado daquelas mudanças qualitativas e quantitativas referentes ao processamento dos *bits*, agora como tudo é desmaterializado e funciona de forma automatizada, os bancos de dados também operam de forma diferente. Há um novo tipo de linguagem, os dados não precisam mais estar estruturados previamente para que haja o tratamento, estes atualmente são analisados em toda a sua extensão, é possível

estabelecer relações para analisar padrões e assim “inferir, inclusive, probabilidades de acontecimentos futuros.” (BIONI, 2019, p. 59)

Como exemplo tem-se o caso da consumidora americana que começou a receber e-mails da loja em que fazia compras (a Target) indicando que a mesma comprasse fraldas, berços e roupas de bebê. Quando o pai da consumidora olhou esses *e-mails*, dirigiu-se ao gerente da loja e questionou as propagandas que tentavam “incentivar” a filha a engravidar, o gerente imediatamente pediu desculpas. Acontece que algum tempo depois, a consumidora contou para o pai que estava grávida, ou seja, este prontamente se desculpou com o gerente da loja. (KAFFER, 2019)

A questão aqui é a previsibilidade do acontecimento, uma loja de departamento conseguiu, a partir das análises da sua cliente, prever as compras futuras e enviar cupons e propagandas direcionadas.

Kris Shaffer (2019) ainda alerta que não são apenas propagandas que se alimentam desse modelo, o autor relata sobre histórias angustiantes ao se fazer uma pesquisa no *google*, um desses casos seria de uma autora negra que ao pesquisar “garotas negras” no campo de busca acaba se deparando com imagens desumanas, caracterizando-as como objetos sexuais.

Esses preconceitos são usuais dentro das ferramentas de busca, Shaffer (2019) afirma que eles são o retorno do que a maior parte dos usuários querem ver, como exemplo usa a pesquisa de imagens de figuras como cientistas e professores, elas são sempre as mesmas imagens, o mesmo modelo de pessoas que a maioria espera ver como aquele profissional. Recaindo assim em diversos tipos de preconceitos que são fruto da automatização, a qual tenta sempre prevê os próximos passos dos usuários.

Outrossim, milhares de dados são criados e agregados para identificar padrões de comportamento e apostar em um acontecimento futuro. Uma base de dados pode ser utilizada para diversas finalidades, podendo ser reutilizada, sendo capaz de prever qualquer tipo de informação desde uma consumidora grávida até o termino de um relacionamento. Os dados dos cidadãos dizem muito sobre estes e portanto, ao serem tratados transformam-se nessa grande arma publicitária. (BIONI, 2019)

Sabendo que todas as informações deixadas na rede podem ser transformadas em dados, nada é trivial, tudo é coletado, desde curtidas em uma rede social à busca por determinado produto em um site, uma troca de e-mails, fotos, vídeos, localização, tudo isso são dados adquiridos, agregados, analisados e vendidos diversas vezes. (ZUBOFF, 2015)

Shoshana Zuboff (2015) leciona que a *google* é a maior empresa de Big Data do mundo, possuindo a maior quantidade de *data*, assim eles optaram pelo modelo de propaganda

por meio de leilão, sendo os clientes os anunciantes. A *google* vende publicidade online, utiliza todos os dados que recebe e os vende em leilões, que terão seu funcionamento especificado no próximo tópico, importando assim a quantidade de dados que possui.

Certo é que, essa coleta de dados ocorre sem o conhecimento do usuário, na maior parte das vezes, e mesmo se acordando com os termos de um site ou aplicativo não existe transparência, podendo o contrato ser alterado até mesmo depois do ingresso do *user* na plataforma. Como já dito, a coleta de dados ocorre mesmo nos momentos em que se está confortável, com a guarda baixa, como a música que se escuta no caminho para o trabalho e até o próprio caminho escolhido. (SHAFFER, 2019)

Deste modo, cumpre destacar o que é o tratamento de dados, este pode ser qualquer operação utilizada com dados pessoais como a coleta, a transferência, produção, avaliação, modificação, dentre outros verbos inseridos no art. 5º da LGPD brasileira:

Art. 5º Para os fins desta Lei, considera-se:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

O processo de tomada e transformação do big data, também chamado de *big analytics*, tem como objetivo encontrar padrões e retirar informações, o tratamento então é feito por computadores analisados por técnicas algorítmicas⁷, estatísticas e computacionais. (FARIAS, 2020)

Assim, o tratamento de dados traduz-se com o uso do big data, que pode ser utilizado de maneiras diversas, podendo ser usado tanto para expandir o entendimento sobre um consumidor como identificar doenças ou disseminar *fake news*. (OTONNICAR; VALENTIM; JORGE; MOSCONI, 2019)

Klaus Schwab (2016) alerta para a mudança proveniente das tecnologias de grande volume de dados, big data, as quais permitiriam decisões mais rápidas e melhores, além de redução de complexidades e custos. Entretanto, também prevê pontos negativos como as questões ligadas a privacidade e a confiança, como confiar nos algoritmos.

Os algoritmos das redes sociais mostram as pessoas o que é mais popular, não o que é correto ou importante e isso acaba gerando uma assimetria nas redes sociais. Assuntos

⁷ “Algoritmo é uma sequência de instruções que informa ao computador o que ele deve fazer. Todo algoritmo tem uma entrada e uma saída visando determinado objetivo: os dados entram no computador, o algoritmo faz o que precisa com eles, e um resultado é produzido.” (FARIAS, 2020, p.18)

populares acabam sendo inundados de informações polêmicas e ninguém gasta o mesmo tempo para escrever o “óbvio” nas redes, isso leva com que essas opiniões de conta senso garantam um destaque maior. (KAKUTANI, 2018)

Durante o governo Temer houve uma tentativa de compra de resultados no mecanismo de busca do google, no que dizia respeito a reforma da previdência, assim quem pesquisasse sobre o tema encontraria posts patrocinados pelo próprio governo falando coisas positivas da reforma. Isso deixa claro como os algoritmos são capazes de definir a ordem de resultados de acordo com quem comprou aquele link patrocinado, assim a formação da opinião pública estaria sendo afetada, assim “As estruturas de dados e seu tratamento algorítmico estão a serviço de quem tiver recursos financeiros suficientes para obter diferentes amostras de segmentos e perfis de usuários com os padrões especificados pelos compradores”. (SILVEIRA, 2018, p.50)

Resta clarividente que o uso do big data é das grandes empresas ou do governo, os quais possuem maior quantidade de capital, sendo assim, a porta de entrada para tratamento de dados pessoais está atrelado aqueles que possuem dinheiro suficiente para tanto.

Ademais, pode-se levar deste tópico que o uso do big data para realização de tratamento de dados pode surtir efeitos na vida dos usuários, positivos ou negativos, já que estes estão produzindo dados a qualquer momento e eles são utilizados em diferentes situações. O tratamento de dados é uma grande arma publicitária, podendo incidir no comércio de forma perceptível, mas também incidindo em outras áreas como na comunicação através da disseminação de notícias falsas, assim como na democracia, área que será observada no próximo tópico.

3.3 Dados pessoais e democracia: limites e possibilidades

Antes de adentrar o campo democrático, insta salientar uma tática utilizada no campo mercadológico, a denominada publicidade direcionada. Esta é uma prática que procura personalizar a comunicação exercida entre fornecedor e consumidor, se dividindo em três espécies: contextual, segmentada e comportamental. A primeira correlaciona a temática em determinado contexto, ou seja, o conteúdo de determinado jornal com o objeto que está sendo anunciado, como exemplo tem-se um livro sobre política sendo anunciado no caderno de política de determinado jornal. (BIONI, 2019)

Já a publicidade segmentada foca no público alvo, não importa necessariamente o ambiente mas sim o público que tem acesso a este, parte de um emissor com objetivo de atingir um número específico de receptores, como uma propaganda na televisão. Quanto a publicidade comportamental on-line, esta permite uma personalização maior já que a internet possui diversas ferramentas como os *cookies*⁸, tornando possível rastrear o usuário e inferir anúncios publicitários relacionados com o seu interesse. Por meio disso cria-se um retrato do consumidor, sabe-se quem está acessando aquele site e no que a pessoa está suscetível a consumir. (BIONI, 2019)

Kris Shaffer (2019, p.16) define propaganda como sendo “[...] the use of one or more media to communicate a message, with the aim of changing someone’s mind or actions via psychological manipulation, rather than reasoned discourse”⁹.

Ou seja, a propaganda serve para influenciar pessoas e se isso funciona no ambiente comercial por que não funcionaria em outros tipos de ambientes? Foi visto que grandes bancos de dados operam no sentido de coletar qualquer tipo de informação e reutiliza-la para gerar lucro, nos últimos anos constatou-se que tal tática não se concentra apenas no ambiente comercial mas também existem as mesmas táticas no ambiente democrático.

Um perfil em uma rede social fornece várias informações como raça, nacionalidade, gênero, idade, enfim seja porque o usuário informou ou porque a plataforma retirou aquelas informações da própria atividade do *user*. A questão é que uma ferramenta de recomendação de conteúdo funciona encaixando o usuário com algum conteúdo e este conteúdo, como já visto, vão ser propagandas pagas. (SHAFFER, 2019)

A partir da coleta e tratamento de dados pessoais é possível segmentar as pessoas por grupos de interesse, proporcionando com que os anúncios apareçam de forma mais eficiente, portanto, quanto mais informações sobre as pessoas – quanto mais usuários aquela empresa tem – maior valor possui aquela para veiculação de anúncios. Além disso, quanto mais a empresa conhece seu usuário, mais dados sobre ele são coletados e assim os anúncios são destinados com maior precisão, maior a relevância e exibidos por um maior preço. (ANTONIALLI; CRUZ, 2017)

A coleta de dados é uma prática que se tornou habitual na internet, especialmente

⁸ “Os *cookies* são pequenos arquivos que podem ser enviados durante a comunicação estabelecida entre o dispositivo do usuário e o servidor do site que está sendo visitado. Esses arquivos nada mais são do que identificadores, que tornam possível reconhecer o dispositivo em visitas futuras e armazenar informações sobre suas preferências, por exemplo”. (ANTONIALLI; CRUZ, 2017, p.15)

⁹ “O uso de uma ou mais mídias para comunicar uma mensagem, com o objetivo de mudar a mente ou ação de pessoas via manipulação psicológica, ao invés de discurso razoável”.

entre aqueles que trabalham com anúncios publicitários, cujo funcionamento é de acordo com leilões, estes foram desenvolvidos para os buscadores como o *google*, já mencionados no tópico anterior.

Funcionam da seguinte forma, um anunciante pode propor um valor para exibição de um anúncio associado a alguma palavra chave e o vencedor é aquele que propõe o valor mais alto, assim os anúncios ficariam organizados de forma decrescente. Hoje em dia, mecanismos diferentes foram adotados para determinar quais anúncios serão exibidos para determinado usuário, existe assim um sistema automatizado de leilões, os quais são administrados por vários intermediários como agências e redes de anunciantes, quem paga mais por pessoas de determinado grupo vão ter aquele anúncio em destaque. (ANTONIALLI; CRUZ, 2017)

No artigo “*Private traits and attributes are predictable from digital records of human behavior*”, Michal Kosinski, David Stillwell e Thore Graepel (2013) mostram como as curtidas do *facebook* podem dar acesso a diversas informações daqueles usuários como gênero, raça, orientação sexual e até mesmo se a pessoa é democrata ou republicano.

Os pesquisadores concluem que essa previsão pode ajudar a melhorar diversos serviços como no marketing, todavia, eles não ignoram que o uso antiético e não autorizado pode levar a grandes perigos. Empresas assim como pessoas físicas ou governos podem vir a utilizar de técnicas de software para descobrir informações que não estão expostas, como orientação sexual ou opinião política que o indivíduo não deseja demonstrar.

Nos últimos anos veio à tona um escândalo de uma empresa que coletou dados de milhões de usuários do *facebook*, de forma ilícita, para manipulação do processo democrático. Esta empresa foi a *Cambridge Analytica* (C.A), agência inglesa especializada em análise comportamental – realizada a partir da obtenção dos dados dos usuários. A C.A ficou famosa por ter interferido nas eleições dos Estados Unidos de 2016 e também na votação do BREXIT. (FORNASIER; BECK, 2019)

Na primeira, foram utilizados testes dentro da plataforma do *facebook* os quais coletavam informações dos eleitores, após isso eram direcionadas propagandas tendenciosas àqueles considerados *indecisos*, afetando assim na livre escolha dos candidatos por parte dessas pessoas. (FORNASIER; BECK, 2019)

O que efetivamente ocorreu foi a utilização de técnicas para identificar a personalidade de um conjunto de usuários do *facebook*, aplicando técnicas de machine learning¹⁰ para replicar um padrão aqueles que responderam o teste “*This Is Your Digital Life*”.

¹⁰ *Machine Learning* é o processo de inserção do conhecimento em software, são algoritmos de aprendizagem de máquina – ela vai entender o que acontece e repetir aquele comando – que correlacionam vários dados em busca

Sergio Amadeu da Silveira (2018, p. 48) explica:

Um ex-professor da Universidade de Cambridge, Aleksandr Kogan, com base numa série de experimentos e pesquisas psicométricas realizadas pelo pesquisador Michal Kosinski, desenvolveu a enquete, que foi respondida voluntariamente por aproximadamente 270 mil usuários do Facebook. Em seguida, a Cambridge Analytica aplicou o padrão psicométrico obtido para classificar 87 milhões de contas, das quais 70.632.350 eram de norte-americanos.

Ao clicar em realizar esse teste, os usuários do *facebook* davam acesso à *Cambridge Analytica* quanto a sua localização, idade, cor, religião, todas as postagens, fotos e arquivos disponibilizados naquela rede social, enfim acesso aos seus dados pessoais. Se não bastasse isso, sem o conhecimento e muito menos consentimento, todos os amigos daquelas pessoas que responderam o teste de personalidade também tinham seus dados coletados. No final, a C.A não apenas obteve um perfil geral de cada usuário mas além disso, a coleta era contínua portanto bastava fazer o teste uma vez que seu perfil era detalhadamente traçado. (FORNASIER; BECK, 2019)

Deste modo, a C.A pode agrupar pessoas relacionando seus traços psicológicos ao que efetivamente era feito nas redes, foi assim que as eleições americanas de 2016 ocorreram, sustentadas e direcionadas a partir da coleta indevida de dados pessoais dos cidadãos, resultando na posse do candidato que recebia apoio da *Cambridge Analytica*: Donald Trump.

Brittany Kaiser (2020) afirma que em sua primeira reunião com Alexander Nix, CEO da *Cambridge Analytica*, ficou surpresa ao descobrir que existia uma empresa que usasse informações privadas das pessoas para influencia-las, e a C.A, por mais que existente somente há um ano na época, era proveniente de um grupo chamado SCL group, criado em 1993 e que realizou mais de duzentas eleições em diversos países. Os bancos de dados da empresa eram gigantescos e esses dados eram divididos em categorias, durante anos o SCL group vinha classificando pessoas com base na psicologia comportamental.

Mateus Fornasier e Cesar Beck (2019) relatam que o objeto de estudo dessas empresas de análise de dados sempre é feito com pesquisa comportamental dos indivíduos, ou seja, observando o comportamento de cada usuário, a sua localização, sua religião, orientação sexual e diversos outros fatores determinantes da personalidade que são utilizados para o objetivo do contratante.

Um dos grupos responsáveis dentro da C.A tinha como objetivo minerar informações do banco de dados em busca dos votos indecisos, assim eram escolhidas pessoas e direcionados ataques frontais a esses “persuadíveis”. Além disso, outro grupo era responsável

de padrões. Esse processo também é conhecido como mineração de dados, modelagem estática, análise preditiva, sistemas auto organizados, etc. (SILVEIRA, 2018)

pela disseminação de notícias falsas e ataques focais em diversos usuários, o objetivo era tirar da pauta os assuntos democráticos e relevantes da campanha para poder incentivar o ódio e a polarização na rede. (FORNASIER; BECK, 2019)

Após o escândalo da *Cambridge Analytica*, o *facebook* declarou seu foco em impedir que o mesmo acontecesse em outros países, como o Brasil, o qual sabe-se que cerca de 440.000 usuários foram expostos ao aplicativo que a C.A usava para coletar dados. No Brasil, a C.A possuía um parceiro chamado Ponte C.A, o qual objetivo era replicar no Brasil as estratégias da Cambridge Analytica aplicadas na eleição de Trump. (CODING RIGHTS, 2018)

O que aconteceu é que o *facebook* ao restringir o acesso de empresas de dados, agências de marketing e pesquisadores aos seus bancos, acabou por tornar mais limitada a possibilidade de uso de sua interface, mais isolada e menos transparente, tudo isso para evitar que houvesse um novo “vazamento” de dados. Com isso, conseguiu monetizar ainda mais, fazendo com que tenham acesso aos dados somente quem obtiver maior capital – quem pode pagar para coletar, organizar e analisar gigantescos dados. (SILVEIRA, 2018)

O fenômeno das plataformas *online* e dos mecanismos de busca na internet não pode ser desconsiderado quando pretendemos discutir a democracia, a formação das preferências políticas e das opiniões da população. O modelo de negócios das corporações proprietárias das plataformas está baseado na coleta de dados de cada um de seus usuários. (SILVEIRA, 2018, p.50)

Sendo assim, resta clarividente a possibilidade de utilização desses mesmos modelos de negócios quando discutimos sobre a democracia, o processo eleitoral também pode vir a ser invadido por publicidade direcionada como ocorreu nos Estados Unidos em 2016.

Nesse sentido, é razoável a preocupação dos impactos que podem ser causados ao se utilizar da análise de dados pessoais no contexto do processo democrático, onde a livre escolha dos candidatos deveria ser realizada sem interferências de terceiros. Ao realizar o tratamento dos dados dos usuários do *facebook* e em seguida direcionar propagandas para aqueles indecisos, a *Cambridge Analytica* interferiu diretamente na liberdade e autonomia dos eleitores americanos.

Outrossim, importante lembrar que há duas décadas atrás as TICs eram apontadas como algo eminentemente positivo para a entrega de serviços eletrônicos aos cidadãos, já que a redução de custos e o acesso aos meios é uma das marcas centrais do que seria um governo eletrônico.

O governo digital traz consigo o uso das tecnologias como forma de incrementar o ambiente público, exemplos positivos disso são a disponibilização dos dados abertos governamentais e o aumento da transparência. Todavia, o Brasil possui algumas ‘brechas

digitais', enquanto a maior parte dos jovens tem acesso à internet, apenas 31,1% dos idosos possuem acesso aos equipamentos tecnológicos, o analfabetismo eletrônico é algo significativo. (AVELINO; POMPEU; FONSECA, 2021)

Daniel Pitangueira de Avelino, João Claudio Pompeu e Igor Ferraz da Fonseca (2021) dissertam que a transparência e o uso de dados abertos constituem um grande avanço ao contexto democrático, com a abertura governamental tem-se maior controle por parte dos cidadãos quanto a decisão de políticas públicas e o uso dos recursos, além de impulsionar a confiança entre estado e sociedade.

Entretanto, importante analisar também o outro lado da moeda, assim como a internet trouxe maior confiabilidade ao cidadão quanto ao acesso a dados públicos, ela também causou maior insegurança quanto ao uso de dados dos usuários.

4 ELEIÇÕES E O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: A SUA CORRELAÇÃO E SEU MARCO NORMATIVO

Neste capítulo será aprofundado o papel das mídias sociais e das corretoras de dados no processo eleitoral brasileiro, em foco utilizar-se-á de pesquisas realizadas pré e pós eleições de 2018 no Brasil e sua conexão com as eleições de 2016 nos Estados Unidos. Descobrimos assim, se houve impactos a partir do tratamento de dados nas eleições brasileiras de 2018. Além disso, será estudado o marco normativo brasileiro anterior à 2018, ou seja, antes da promulgação da LGPD, como eram tratados a responsabilização por danos gerados ao conteúdo publicado na internet e a regulação do micro direcionamento.

Por fim, irá se discutir acerca da promulgação da Lei Geral de Proteção de Dados e seus princípios estruturantes, como essa lei vai regular a responsabilização do conteúdo publicado na internet e o micro direcionamento, concluindo-se qual o futuro da democracia na era da informação.

4.1 O papel das mídias sociais e das corretoras de dados no processo eleitoral

Como já pincelado anteriormente, o ano de 2016 foi um marco para os partidos populistas de extrema direita, com a eleição de Donald Trump tem-se uma vitória do novo jeito de fazer política: através das ferramentas do big data, as eleições anteriormente plurais tornaram-se individuais – com a análise de dados e o micro direcionamento foram emitidos diversos anúncios para cada segmento específico. (EMPOLI, 2019)

Com tal método foi possível redirecionar votos e fazer com que pessoas deixassem de votar utilizando-se da técnica de desestabilizar seu opositor: as “*negative campaigns*”, na ocasião o opositor foi Hillary Clinton, esta teve diversas informações falsas compartilhadas nas redes sociais. O fato é que nos Estados Unidos os critérios de avaliação dos políticos tornaram-se relativos a capacidade de chamar a atenção. (EMPOLI, 2019)

Em verdade, Trump não foi o primeiro e nem o último político de extrema direita a se eleger utilizando das ferramentas do big data. Giuliano Da Empoli (2019) em seu livro “Os engenheiros do caos” conta a história de diversos sujeitos que utilizando-se da tecnologia e decifrando os códigos compreenderam que a raiva era a fonte de energia correta para realizar o objetivo de captar o voto popular.

Seja o Brexit (movimento de retirada do Reino Unido da União Europeia) ou Bolsonaro, todos tiveram a internet como um movimento de controle em que estavam por trás ideólogos e cientistas especializados em big data.

Pode-se dizer que a primeira vez que as redes sociais foram usadas como elemento central em uma campanha política foi na eleição de Obama em 2008, a equipe do presidente gastou na época cerca de 643 mil dólares, desde então a utilização das mídias sociais cresceu de forma exponencial no campo político. Com o sucesso de Obama e o crescente uso das redes, já em 2016 Donald Trump investiu cerca de 44% do seu orçamento para propaganda nas mídias sociais e suas consequências são notórias, como se vê detalhadamente no capítulo anterior. (PINTO; MORAES, 2020)

A questão é que, no Brasil não foi diferente. Desde as eleições de 2014 se enxerga o uso das redes sociais como ferramenta dentro do jogo político, a disputa entre Dilma Rousseff e Aécio Neves nas eleições presidenciais foi marcada por uma polarização agressiva e uso intenso de robôs nas redes.

Eles são usados para propagar informações falsas ou gerar um debate artificial e foram observadas diversas interações desses perfis tanto em favor de um candidato como de outro. Posteriormente, em 2015 quando do impeachment da Presidenta Dilma, pelo menos 10% das interações no assunto foram impulsionados por robôs, demonstrando assim a influência desse tipo de conta no debate público. (FGV/DAPP, 2018)

Em meio a uma turbulência política, após um processo de impeachment e o mandato de Michel Temer, chega-se à 2018 o ano das eleições gerais brasileiras, entretanto, este ano é rodeado de entraves. No decorrer do ano, um dos candidatos à Presidência da República, o ex-presidente Lula, foi preso após uma votação controversa do Supremo Tribunal Federal, acontece que esse candidato era o 1º lugar nas pesquisas de intenção de voto. (CODING RIGHTS, 2018)

Em seguida encontrava-se o candidato ultraconservador de direita Jair Bolsonaro, o qual vinha desde 2014 crescendo nas redes sociais, muitas vezes como “alívio cômico” ou alguém que era totalmente inviável para o cargo, já que acompanhado de diversas polêmicas com afirmações LGBTfóbicas, racistas e machistas.

Bolsonaro é um populista de direita e angariou seus votos com um discurso anti política, como se fosse de uma classe diferente e por isso fosse dar certo, com milhões de seguidores nas redes sociais e sempre produzindo conteúdos polêmicos elegeu-se Presidente do Brasil. (CODING RIGHTS, 2018)

Uma das técnicas utilizadas por Bolsonaro foi apostar em grupos do *whatsapp*, uma

rede social de troca de mensagens a qual quase dois terços dos eleitores no Brasil possuem conta e desses eleitores, segundo pesquisa realizada pelo Coding Rights e publicada como relatório brasileiro para o projeto internacional ‘Dados Pessoais e Influência Política’, desenvolvido pela Tactical Technology Collective para a plataforma “Our Data, Our Selves” (2018), 36% leem e 21% compartilham notícias sobre política e as eleições. No Brasil, diferente dos outros países, o *whatsapp* teve grande influência já que eram feitas listas de transmissões para mobilizar os cidadãos e compartilhar *fake news*¹¹, as quais tiveram grande incidência durante as eleições de 2018.

Em outubro de 2018 uma reportagem da Folha de São Paulo¹², destacou que empresários estavam investindo em campanha política contra o Partido dos Trabalhadores com contratos de mais de 3,5 milhões de dólares, tudo isso visando a distribuição em massa de mensagens via *whatsapp*.

O Internetlab (2019), grupo de pesquisa em direito e tecnologia, coletou a partir de um formulário digital 78 spams políticos recebido por eleitores por *whatsapp* e SMS, ambas plataformas de envio de mensagem direta. Nessas mensagens estavam conteúdos diversos como “santinhos” virtuais, vídeos, mas em sua maioria comunicavam conteúdo com teor de ataque a um candidato ou seu respectivo partido com intuito de fazer uma “contra-campanha”. Foi constatado ainda, material contestando os resultados do primeiro turno das eleições de 2018, afirmando conteúdo inverídico sobre os votos nulos e assim propagando desinformação.

O que o relatório concluiu é que a adoção de *spam* como marketing político pode ter sido tanto uma estratégia institucional das próprias campanhas como uma prática descentralizada dos seus apoiadores, não sendo possível identificar com precisão já que a maior parte das mensagens não faz ligação direta com um candidato ou partido.

Uma outra conclusão é a de que parte dessas mensagens tenham sido resultado de disparos massivos, já que constatada a presença de números de envios estrangeiros. Com isso, ressalta-se que o spam não é uma técnica utilizada pelas redes sociais de massa, entretanto, é possível ser realizada por meio do *whatsapp*, sms e email – ferramentas de troca de mensagem direta. Sendo esta uma das principais diferenças entre as eleições dos Estados Unidos de 2016 e as eleições brasileiras de 2018, no Brasil houve a presença massiva de spam por meio do *whatsapp*. (INTERNETLAB, 2019)

¹¹ No sentido amplo do termo são: “notícias falsas, teorias da conspiração, material ofensivo e calunioso contra certas pessoas ou grupos, avisos urgentes e alarmistas, enunciados distorcidos ou retirados de contexto.” (CESARINO, 2020, p.5)

¹²<https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml>

Ademais, cumpre dissertar no presente tópico sobre os denominados “*data brokers*” ou corretoras de dados, que são uma indústria que consiste na troca de dados entre diversas empresas, elas fornecem dados umas às outras, seja vendendo ou combinando-os.

Certo é que essas empresas especializadas em troca de dados não são específicas para o campo eleitoral no Brasil, entretanto, elas também trabalham com eleições e antecedendo a corrida eleitoral de 2018 tem-se diversas empresas cotadas como possíveis protagonistas nas eleições, assim a pesquisa realizada pelo Coding Rights e publicada como relatório brasileiro para o projeto internacional ‘Dados Pessoais e Influência Política’, desenvolvido pela Tactical Technology Collective para a plataforma “Our Data, Our Selves” (2018) entrevistou algumas dessas empresas.

Dentre as empresas entrevistadas tem-se a Ponte Estratégia (ex representante da *Cambridge Analytica* no Brasil), Grupo Numbr, Ideia Big Data e Stilingue. Nas entrevistas verifica-se o engajamento das empresas em uma ampla diversidade de atividades, algumas trabalham na varredura das redes sociais para criação de propaganda direcionada, outras fazem parte do processo de marketing político das candidaturas. (CODING RIGHTS, 2018)

Durante as conversas a maioria das empresas destacaram que o contexto brasileiro difere do estadunidense já que não seria favorável a expansão do uso do big data de maneira generalizada como ocorreu nos EUA. Entretanto, a maioria das empresas também mencionou que as informações geradas na internet são um fator importante para os negócios por conta da quantidade de dados disponíveis, as informações legalmente coletadas nas redes quando cruzadas com bases de dados públicos já são suficientes para construir estratégias eficientes. (CODING RIGHTS, 2018)

Falando em base de dados públicos, vale a pena dissertar sobre o Serasa Experian, ela é uma empresa com a função principal de centralizar e organizar os dados de cadastro para análise de crédito das pessoas, atuando em três frentes sendo uma delas o marketing e certificações digitais. Atualmente é uma das maiores corretoras de dados atuantes no Brasil, ela comercializa os dados completos dos consumidores ao seus clientes, uma das soluções de segmentação apresentada pela empresa é o Mosaic – ferramenta que segmenta e classifica a população criando grupos bem detalhados. (SAMPAIO, 2017)

As informações estão divididas em 4 perfis iniciais (promissores, batalhadores, experientes, empreendedores) ou, mais detalhadamente, divididas em 11 segmentos distintos, classificados por grupos de A a K: elites brasileiras, experientes urbanos de vida confortável, juventude trabalhadora urbana, jovens da periferia, adultos urbanos estabelecidos, envelhecendo no século XXI, donos de negócio, massa trabalhadora urbana, moradores de áreas empobrecidas do sul e sudeste, habitantes de zonas precárias, habitantes de áreas rurais. Como exemplificado a seguir, esses grupos são

descritos e classificados pela área em que vivem, idade, sexo, escolaridade, força de trabalho, acesso à internet e estilo de vida. (SAMPAIO, 2017, p. 80)

Verifica-se o potencial da Serasa Experian em relação a publicidade direcionada e tratamento de dados pessoais, o Mosaic apresenta dados de mais de 140 milhões de brasileiros e por mais que o produto seja oferecido como uma solução de marketing voltado para marcas, nada impede que se volte a partidos políticos também. (CODING RIGHTS, 2018)

Isso porque, enquanto nos Estados Unidos houve a empresa *Cambridge Analytica* atuando nas eleições, no Brasil foi realizada parceria com uma representante da C.A: a Ponte Estratégia. Antes do escândalo da C.A vir à tona, a Ponte Estratégia estava se preparando para atuar nas eleições brasileiras de 2018 e seu objetivo era segmentar as pessoas permitindo-se a micro segmentação e desenvolvimento de conteúdo de acordo.

Além disso, seria implantada distribuição de conteúdo eleitoral no *whatsapp*, propondo-se enviar até 10 mensagens por dia no aplicativo, afirmando assim que seria possível eleger um deputado quase 100% pelas redes. Todavia, após o escândalo da C.A, a parceria com a empresa no Brasil foi encerrada. (CODING RIGHTS, 2018)

O marketing político, atualmente, emprega uma atuação entre análise de dados e campanha política personalizada – o microtargeting político – nela os rastros do comportamento online de cada indivíduo é coletado e vendido para outras empresas. Esse modo de funcionamento coloca em cheque a autonomia do eleitor, isso porque a pessoa tem seu espaço pessoal invadido por um terceiro que sem consentimento utiliza daqueles dados para criar propagandas direcionadas ou mensagens pontuais as quais irá refletir em quem a pessoa vota ou não. (PINTO; MORAES, 2020)

Mateus Oliveira Fornasier e Cesar Beck (2020) alertam que ao entrar na nova década novas formas de coletas de dados assim como de *fake news* irão se popularizar e que, por mais que a *Cambridge Analytica* não exista mais, diversas outras empresas estão surgindo com o mesmo propósito de interferir nas eleições favorecendo aquele candidato com maior capital que contrata tal empresa. A interferência na autonomia e na liberdade de escolha do cidadão é afetada na medida em que práticas como micro direcionamento nas redes sociais são utilizadas.

Certo é que, as eleições de 2016 nos Estados Unidos sofreram ataques mais frontais, os testes realizados pela *Cambridge Analytica* foram massivos e influenciaram uma gama enorme de eleitores. Entretanto, não se pode negar que no Brasil em 2018 também existiam empresas corretoras de dados e houveram diversas tentativas de contragolpes eleitorais seja no *facebook* ou no *whatsapp*, principal veículo de spam e *fake news* durante a corrida eleitoral.

Sendo assim, as eleições brasileiras também foram influenciadas pelas novas tecnologias e o uso de big data de certa forma recaiu sobre os eleitores brasileiros que foram bombardeados com mensagens e anúncios referentes aos partidos/candidatos.

4.2 O marco normativo do tratamento de dados na democracia antes da Lei Geral de Proteção de Dados

Foi discutido no tópico anterior as repercussões do uso do big data nas eleições brasileiras de 2018, sabendo-se que em 2018 a Lei Geral de Proteção de Dados ainda não estava em vigor insta dissertar sobre as normas vigentes à época quanto à proteção de dados pessoais e seu reflexo nas eleições como com as propagandas direcionadas e os spams no *whatsapp*.

A Constituição Federal de 1988 é clara ao prever a inviolabilidade da intimidade, da vida privada e da imagem como direitos fundamentais, além de incluir a inviolabilidade do sigilo de correspondência e das comunicações de dados em seu rol. Como dissertado anteriormente, esse sigilo de comunicação de dados não deve ser visto como uma garantia ao direito à proteção de dados já que tutela apenas a comunicação daquele. Sendo assim, em 2018 não tem legislação em vigor que estabeleça um regime geral sobre a proteção de dados pessoais, entretanto, tem-se outras normas que podem ser usadas para assegurar o debate virtual como a Lei das Eleições, o Marco Civil da Internet e a Lei de Acesso a Informação. (BRASIL, 1988)

Criada em 2011, a Lei de Acesso a Informação é destinada a assegurar o direito fundamental de acesso à informação, sendo o sigilo uma exceção, surge assim como um mecanismo de fortalecimento da democracia e da participação política. A lei determina que o tratamento de informações pessoais deve ser feito de maneira transparente – proteção do direito fundamental à privacidade. Esta norma não traz nada específico sobre proteção de dados, entretanto, já abarca definições como as de informação, informação pessoal e seu tratamento. (BOFF; FORTES, 2016)

A propaganda eleitoral na internet antes de 2018 era proibida, somente com a reforma eleitoral de 2017 que foi autorizada a propaganda eleitoral paga na internet feita por mecanismos de impulsionamento de conteúdo. Tal mudança repercute de forma a transformar as eleições, agora mais digitais do que nunca. Segundo o artigo 57-C da Lei das Eleições a propaganda eleitoral na internet pode ser feita em alguns casos como no caso de impulsionamento “contratados diretamente com provedor de aplicação de internet com sede e

foro no país”. Outra característica é que o financiamento deverá ser feito apenas por partidos políticos, candidatos e coligações, deste modo pessoas físicas não podem realizar impulsionamento de conteúdo, o que para o TSE significa um mecanismo que potencializa o alcance e divulgação de informações. (CRUZ et al., 2018)

A partir das ferramentas de impulsionar, tornou-se possível micro direcionar publicidade de forma a quase individualizar a mensagem de um candidato ao seu eleitor, tais técnicas como já abordadas anteriormente, são possíveis a partir de consultorias e agências de marketing digital que agregam grande conjuntos de dados pessoais e formam perfis detalhados sobre eles. Os limites gerais do micro direcionamento não estavam bem definidos na lei das eleições já que em razão do artigo 57-E é vedado a candidatos, partidos e coligações se aproveitarem de “cadastros eletrônicos de clientes”. (CRUZ et al., 2018)

Além da Lei das Eleições, já regia no cenário brasileiro o Marco Civil da Internet, este define um conjunto de regras que garante a proteção da privacidade e dos dados pessoais nas redes sociais tendo estas proteções como seus princípios. A lei ainda garante uma série de direitos ao usuário com regras gerais sobre consentimento, finalidade, compartilhamento e transparência de dados pessoais, tudo isso presente no artigo 7º da Lei, especificamente em seus incisos VII, VIII e IX (BRASIL, 2014):

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

Sendo assim, em processos eleitorais devem ser observados esses direitos pelas campanhas em qualquer tratamento de dados que ocorra, como exemplo tem-se a situação de coleta de dados através de formulários, coleta a partir da página em rede social ou site de candidato, uso de dados para envio de propaganda eleitoral seja em rede social ou em aplicativos de mensagens, enfim todas essas ações devem ser precedidas da análise do consentimento, finalidade, transparência e compartilhamento. (MASSARO et al., 2020)

Um dos exemplos acima referidos foi o uso de dados para envio de propaganda eleitoral por rede social ou aplicativo de mensagens, no tópico anterior foi explanado o uso de

diversos envios de spams via *whatsapp*. Sendo assim, resta claro que a técnica de envio de mensagens direcionadas aos eleitores deve observar preceitos fundamentais para serem válidas. O primeiro destes seria o consentimento para obter aquele dado telefônico ou aquela informação disposta na rede social, em seguida é necessária a finalidade do uso desse dado sendo informada ao usuário de forma transparente. Ora, nos casos analisados no tópico anterior é notório que não houve o consentimento das pessoas em receber aquelas mensagens, elas não possuem nem ideia de como o emissor conseguiu seus números de telefone para encaminhar mensagens indesejadas.

Além disso, é importante adentrar ainda mais no aspecto da propaganda eleitoral, esta é um conjunto de técnicas utilizadas para influenciar pessoas quanto a uma compra ou a um voto, acontece que existem artifícios utilizados nas campanhas eleitorais desde muito tempo: os boatos e as mentiras. Mesmo antes da chegada dos computadores, eram espalhados por panfletos ou no “boca a boca” mentiras e boatos sobre determinado candidato, com a internet apenas teve-se a maior disseminação das informações, de todas elas inclusive as mentirosas. As aplicações de internet possibilitaram que qualquer pessoa pudesse publicar informações, sejam elas falsas ou não verificadas, podendo circular em páginas da web como se fossem verdadeiras, estas são as chamadas “*fake news*”. (CRUZ et al., 2018)

O processo de desinformação, então, está presente dentro da corrida eleitoral, onde diversos candidatos precisam se opor uns aos outros para tentar ganhar mais eleitores – jogo eleitoral. O Marco Civil da Internet vai dispor de uma regra em seu artigo 19 sobre a responsabilidade dos provedores de internet por eventual conteúdo ilícito postado por terceiro, ou seja, caso um cidadão publique uma notícia fraudulenta no *facebook*, este só será responsabilizado caso após o recebimento de uma ordem judicial específica não remova o conteúdo. (MONTEIRO, 2020)

Isso porque o MCI preza pela proteção do direito à liberdade de expressão, o qual tem posição de destaque quando confrontado com outros direitos fundamentais, não podendo atuar de maneira preventiva quanto a postagem de conteúdo ilegal nas redes. A proibição de algo preventivo existe por conta da vedação à censura, não poderia o legislador deixar a margem dos provedores de internet a decisão de remover ou não um conteúdo, assim este só pode ser excluído após decisão judicial. (MONTEIRO, 2020)

Certo é que, o Marco Civil da Internet não é culpado pelo crescimento exponencial da utilização da internet, é natural que quanto mais a utilização das ferramentas online maior a decorrência direta do meio digital na vida cotidiana e a legislação veio regular justamente isso. No cenário atual, a propaganda eleitoral encontra ambiente para propagação em massa,

conteúdos com finalidades eleitorais podem em questão de horas influenciar o resultado de uma eleição e assim transformar totalmente o ambiente físico. (VIANA; FILHO, 2020)

Outro protagonista nas eleições brasileiras de 2018 foram os robôs, também conhecidos como *bots* que são basicamente “softwares que automatizam reações e comportamentos a partir de instruções dadas por seus programadores, passando-se por seres humanos”. Elas são aquelas contas que podem até mesmo interagir com humanos se perceberem o contexto que foram instruídos a funcionar, sendo capazes de imitar o comportamento humano e até mesmo de intervir em alguma postagem. Certo é que essa estratégia pode manipular o processo de escolha de representantes políticos e pautas governamentais. (CRUZ et al., 2018, p.151)

A legislação eleitoral prevê dois dispositivos que restringem condutas que podem envolver *bots*, estabelece no §2º do art. 57-B e no artigo 57-H da Lei nº 9.504/97 que “não é admitida a veiculação de conteúdos de cunho eleitoral mediante cadastro de usuário de aplicação de internet com intenção de falsear identidade” e que “será punido com multa de R\$ 5.000 (cinco mil reais) a R\$ 30.000,00 (trinta mil reais) quem realizar propaganda eleitoral na internet atribuindo indevidamente sua autoria a terceiro, inclusive candidato, partido ou coligação”. Sendo assim, existem contornos jurídicos que precisam ser respeitados. (CRUZ et al., 2018)

Deste modo, constata-se que as normas vigentes quando a realização das eleições brasileiras de 2018 não tratavam de forma específica sobre as diversas manipulações com dados, porém já traziam normas paradigmas como a questão do consentimento e da finalidade para uma operação com dados, sendo assim, mesmo sem aplicação da LGPD seria possível afirmar que houve uso indevido de dados nas eleições de 2018 sendo violadas regras do Marco Civil da Internet e da legislação eleitoral.

4.3 A Lei Geral de Proteção de Dados e o futuro da democracia na era da informação

Verificou-se que diversos candidatos e partidos políticos contratam empresas de marketing digital para gerenciar suas ações na internet, fazendo com que ocorra o impulsionamento de conteúdo partidário dispondo de perfis dos usuários com dados pessoais coletados e tratados a partir de uso da técnica do big data. Certo é que, na maior parte dos casos os usuários não sabem que seus dados pessoais – sua privacidade – estão sendo tratados para

tal finalidade, sendo assim, observou-se anteriormente dispositivos normativos que tratam sobre o tema e que estavam sendo aplicados durante as eleições de 2018, para agora se dispor sobre a criada em 2018, Lei Geral de Proteção de Dados. (VIANA; FILHO, 2020)

A Lei Geral de Proteção de Dados (Lei 13.709/2018) consolida um regime de proteção de dados pessoais, uniformizando conceitos e estabelecendo regras, deveres e direitos. Essa lei estabelece um regime geral que passa a conviver e interagir com outras regras como o Marco Civil da Internet e a legislação eleitoral. A LGPD teve influência direta do Regulamento Geral de Proteção de Dados Europeu (GDPR), este definiu que sites e empresas mesmo fora da Europa deveriam seguir suas regras se fossem contratadas por usuários europeus, e mesmo impondo diretrizes isso não retirou a liberdade de cada país definir sua própria legislação. Dessa forma, a GDPR impulsionou a criação da LGPD que se aprofundou em conceitos, regras e sanções alinhados com os padrões internacionais. (FARIAS, 2020)

A função da legislação brasileira de proteção de dados é proteger o sujeito titular da informação, o qual se encontra em uma posição de vulnerabilidade ao ceder seus dados em troca de bens ou serviços, abrangendo assim todos os tipos de dados pessoais. (FARIAS, 2020)

Dado pessoal é aquele que diz respeito a toda pessoa identificada ou identificável, como já exposto anteriormente, certo é que a análise da relação entre informação e um indivíduo deve ser feita observando o contexto. A LGPD em harmonia com o Marco Civil da Internet adota um conceito expansionista de dado pessoal, ou seja, aquela informação cruzada com um banco de dados, por exemplo, pode vir a identificar um indivíduo. Essa informação não precisa ser necessariamente um fato, podendo ser uma suposição ou uma informação errada, todo tipo pode ser considerado dado pessoal. (MASSARO et al.,2020)

Ademais, importante lembrar sobre dados pessoais sensíveis que são aqueles sobre raça, credo, orientação sexual, saúde, além de claro dados biométricos e genéticos. Estes, segundo a LGPD, só podem ser tratados mediante consentimento específico.

Isso porque, parte significativa de campanhas de marketing podem trazer o uso de dados pessoais sensíveis, um exemplo são as listas de filiados em determinado partido já que revelam a posição política dos sujeitos. Ademais, não são apenas estes que a LGPD submete a esse regime mais restritivo, qualquer tratamento de dados pessoais inclusive os triviais que revele dados pessoais sensíveis e possa vir a causar dano ao titular (art.11 §1º), como por exemplo, uma lista de seguidores em uma página de perfil político: pode eventualmente revelar um dado sensível (opinião política) já que o usuário segue a página e curte seus posts. (MASSARO et al.,2020)

Os dados possuem forte poder de influenciar no processo decisório de alguém, já

que eles trazem informações pessoais e sensíveis, basta observar o caso da *Cambridge Analytica*. Portanto, a LGPD em seu artigo 6º resolveu elencar princípios que devem ser observados quando da atividade de tratamento de dados de acordo com a boa fé e a: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. (NETO; NEVES, 2020)

Deste princípios, guarda importância detalhar alguns. O primeiro princípio é o da finalidade, este busca garantir o propósito pelo qual o tratamento de dados é efetuado para assim evitar a reutilização de dados para diferente propósito. Sendo assim, deve-se assegurar a finalidade para qual aquele dado está sendo tratado e se está é legítima e específica – não pode ser vedada por lei e nem ampla ou genérica. Como exemplifica Heloisa Massaro et al. (2020, p.15):

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

Além disso, outro caso em que é necessário atentar ao princípio da finalidade é no caso de dados públicos como cadastros de eleitores ou informações publicadas pelos próprios indivíduos em suas redes sociais, não é porque aquela informação é pública que ela pode ser utilizada para qualquer coisa.

Massaro et al. (2020) lecionam que a coleta, reutilização ou tratamento desses dados por campanhas políticas seja para criação de bancos de dados ou para envio de propaganda configuram tratamento de dados pessoais em violação ao princípio da finalidade.

Quanto ao princípio da adequação e da necessidade, este primeiro diz respeito ao tratamento adequado aquela finalidade informada ao titular e em relação a necessidade tem-se que o tratamento de dados deve ser limitado ao mínimo possível. Um exemplo de afronta ao princípio da necessidade é justamente a coleta de dados para exame psicométrico de eleitores para micro direcionamento de mensagens, como ocorreu no caso da *Cambridge Analytica*, clássico caso de tratamento excessivo de dados. (MASSARO et al., 2020)

O prévio consentimento do usuário para fins políticos também veio assegurado na LGPD, mesmo já sendo previsto em outras normas anteriormente, destaca-se que não se trata de simples anuência mas de um consentimento qualificado, ato inequívoco e livre. Outro princípio trazido pela legislação foi o da transparência, garantindo informações claras, precisas

e facilmente acessíveis, este princípio traz consigo o ideal de reduzir a assimetria entre poder e informação, tonando a informação clara e utilizável pelo usuário. (VIANA; FILHO, 2020)

Além desses princípios listados no artigo 6º, o artigo 7º da LGPD traz que o tratamento de dados pessoais somente pode ser realizado nas hipóteses do consentimento, para o cumprimento de obrigação legal, para realização de estudos, quando necessário para execução de contrato, entre outras situações. Entre elas encontra-se a hipótese do legítimo interesse do controlador ou de terceiros, esse acontece porque a LGPD busca também um livre fluxo de dados para dar ensejo ao desenvolvimento econômico, dessa forma surge o direito de manipular dados pessoais. Para que se possa considerar o legítimo interesse ainda se faz necessária a leitura do artigo 10º da lei, o qual dispõe sobre o que seria esse legítimo interesse, que depende de diversos deveres para ser alcançado. (BIONI; KITAYAMA; RIELLI, 2021)

Lê-se o artigo 10º da LGPD (BRASIL,2018):

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

Primeiramente, vale realizar uma leitura sistemática e teleológica do artigo, o qual também alcança a figura do terceiro, isso porque o controlador pode realizar um tratamento de dados que não seja do seu próprio interesse mas de terceiros ou da sociedade. O objetivo central do artigo 10 é criar parâmetros que norteiem a aplicação do legítimo interesse, sendo assim, chega-se à conclusão que os incisos seriam cumulativos. . (BIONI; KITAYAMA; RIELLI, 2021, p.28)

Em segundo lugar, importante ressaltar a “barreira de modulação ao voto de confiança dado ao agente de tratamento de dados, que é quem terá discricionariedade para avaliar se o seu interesse é legítimo”, ou seja, os princípios dispostos no artigo 6º. Para aplicabilidade do artigo 10º é criado um ônus argumentativo referindo-se aos princípios da finalidade, necessidade e transparência – os quais possuem incidência horizontal. (BIONI; KITAYAMA; RIELLI, 2021, p.28)

Diante disso, importante observar os princípios que regem à proteção de dados pessoais quando do controle de dados pessoais, ou seja, é necessário que haja o respeito a finalidade, a necessidade, a transparência, boa-fé e todos os outros princípios listados na Lei.

Outrossim, a Lei obriga que qualquer pessoa que faça o tratamento obtenha o consentimento dos seus titulares, sendo ainda possível a revogação da autorização a qualquer

momento. Além disso, os dados não podem ser utilizados para fins ilícitos ou abusivos, com o objetivo de discriminar algum sujeito, portanto, o controlador deve adotar medidas capazes de comprovar o cumprimento das normas de proteção de dados. (SOUSA; GOREZEVSKI, 2020)

Muito foi dito até aqui sobre o disparo de mensagens em aplicativos, entretanto, o que foi dito não se aplica ao tratamento de dados pessoais realizado para fins particulares e não econômicos, quando um eleitor envia mensagem à um familiar, este não está sujeito a LGPD. Na legislação eleitoral, a mesma coisa, esta entende que manifestação espontânea na internet não é considerada propaganda eleitoral, assim dispôs a Resolução nº 23.610/2019.

Massaro et al.(2020) encontram problemas quanto a essa definição já que a delimitação de “pessoas naturais” e “consensualmente” ou “fins não econômicos” são de difícil definição. Sendo assim, os autores concluem que a definição de “pessoas naturais” não abrange indivíduos que trabalham para campanhas, da mesma forma que “para fins particulares e não econômicos” envolve a não relação com a prática de campanhas, portanto, na ausência da espontaneidade a mensagem pode vir a ser considerada propaganda eleitoral e sujeita-se à LGPD.

A Resolução nº 23.610/19, ainda, vedou o disparo em massa de conteúdo, o artigo 34 veda a realização de propaganda por disparo de mensagem sem concordância do destinatário, fazendo-nos entender que é preciso da anuência do usuário. Entretanto, nem com a concordância seria legítimo já que o artigo 28, inciso IV da Resolução veda de forma ampla qualquer contratação de disparo em massa para realização de propaganda por aplicativo de mensagens. (MASSARO et al., 2020)

Com isso, tem-se clarividente que os ataques em massa por meio do *whatsapp* realizados nas eleições brasileiras de 2018 afrontam a legislação de proteção de dados pessoais e a legislação eleitoral vigentes já no ano de 2021. A LGPD traz por meio de seus princípios e normas diversos regramentos importantes e que sustentam a proteção de dados pessoais, entretanto estes não são por si só suficientes.

Somente a Lei Geral de Proteção de Dados não é capaz de garantir o pleno desenvolvimento democrático na internet, para Bruna Bastos, Luiza Berger von Ende e Rafael Santos de Oliveira (2020) a LGPD vai ter um impacto positivo para coibir violações algorítmicas e abuso de dados, entretanto, ela não é capaz de concretizar sanções a grandes empresas estadunidenses (como o *whatsapp*) pela falta de norma respectiva nos Estados Unidos, então seria necessária uma atuação internacional para regulamentar as plataformas.

Certo é que, a LGPD de fato só veio a entrar em vigor em setembro de 2020, não sendo aplicada às eleições do mesmo ano, Monteiro, A. P. L., Tavares, C, Borges, E., Brito

Cruz, F. e Massaro, H. (2021) afirmam ser muito cedo para entender como essas regras vão impactar nas estratégias das campanhas digitais, tendo que se esperar às próximas eleições em 2022 com a atuação da Autoridade Nacional de Proteção de Dados para guiar os caminhos encabeçados pela LGPD. Assim, o futuro da democracia na era da informação permanece incerto porém, inegável a afirmação de que uma lei geral de proteção de dados faz diferença já que orientada com princípios essenciais para o regular tratamento de dados.

5 CONCLUSÃO

Na monografia em questão, foi objetivado conhecer os instrumentos que concretizaram a sociedade de informação, analisar sua repercussão em múltiplos ambientes, assim como compreender o direito à privacidade que é a base para o que tem-se hodiernamente como um direito à proteção de dados pessoais. Para assim, estudar de que forma o tratamento de dados impacta na democracia, de acordo com as eleições brasileiras de 2018. Tendo como hipótese que a mineração de dados realizada para fins de atuação em um processo eleitoral infringe o direito à liberdade e autonomia dos eleitores, afetando o processo democrático.

Ao longo dessa dissertação, foi analisado diversos conceitos referentes ao direito digital. Inicialmente, foi apresentada como a tecnologia alterou o modo como se vive em sociedade, conduzindo-se assim até o que diversos autores conceituam como sendo novo a esta sociedade, alguns afirmar ser as tecnologias, outros dizem ser a informação que agora é constante ou até mesmo que está-se diante de uma quarta revolução industrial. Destarte, o que conclui-se é que não importa a nomenclatura adotada, a sociedade opera de acordo com as Tecnologias de Informação e Comunicação (TICs).

Hodiernamente, a sociedade opera com a informação como elemento central, é introduzida a ideia de que os bits desmaterializaram a informação, já que com a linguagem binária (dígitos 1 – 0) pode-se guardar grande quantidade de informações e separa-las em pastas. Assim, identificada uma mudança quantitativa e qualitativa no processo de armazenamento de dados, tem-se a atenção como elemento fulcral no ambiente econômico já que está-se diante de um trade-off (troca). Rodotà vai chamar isso de sociedade da classificação, o indivíduo troca suas informações pelo acesso àquele serviço, o pagamento não é mais feito por dinheiro mas, por uma cessão de informações. Finalizando com os modelos de negócio, explicados por Bruno Bioni, conclui-se que o usuário paga pelo acesso a determinado site ou aplicativo.

Além disso, foi introduzida ainda a ideia do capitalismo de vigilância, já que a internet se tornou essencial e ela está cheia de anúncios, o comércio em prol da divulgação de propaganda está subordinada a vigilância no sistema de informação. Para tanto, é preciso que se utilize de dados dos usuários. Sendo assim, clara a relação dos dados com o comércio, todavia, no momento que houve essa mudança também houve a mudança no espaço público, a democracia também está dependente das TICs.

Logo após esse momento, foi dissertado sobre a origem do direito à privacidade, desde a ideia do direito de ser deixado só até a compreensão de que a privacidade é muito mais que isso. A privacidade é o ato de controlar as informações em qualquer momento e em qualquer

lugar, dessa forma nasce o direito à auto determinação informativa: cada indivíduo pode decidir sobre a divulgação e utilização de seus dados. Foi abordado também problemas referentes ao fim da privacidade, o qual estaria acontecendo com toda essa invasão nas tecnologias, tecnologias essas que crescem a cada dia que passa, informatizando diversos aparelhos.

Além disso, foi estudado acerca do nascedouro da democracia, como ela funcionava e como teve que se adaptar ao longo do tempo, se caracterizando atualmente como algo muito maior que a lógica da soberania popular. A democracia se tornou digital, com a mudança da sociedade de informação também transformou-se o modo como se elegem candidatos. Sendo assim, tem-se que uma democracia na era da informação precisa observar certos parâmetros como o devido tratamento de dados pessoais, sob o risco de estar infringindo o direito à liberdade de escolha dos eleitores.

Adentrando no segundo capítulo, foi discutido um direito fundamental à proteção de dados, direito este implícito na constituição brasileira, já que não disposto na Constituição Federal, porém, conjugado com outros direitos pode ser reconhecido como materialmente constitucional. Reconhecida a fundamentalidade do direito, foi introduzida a ideia de Big Data e como funciona o tratamento de dados pessoais, para então poder falar das possibilidades e limites existentes quando se trata de dados pessoais e democracia, assim se observa o caso da *Cambridge Analytica* que repercutiu como sendo operado pelo big data, os dados de milhões de usuários foram coletados para servir ao direcionamento de conteúdo eleitoral.

Já no terceiro capítulo, é pincelado sobre como o uso das redes em campanhas políticas iniciou durante a campanha de Obama em 2008 e em seguida isso já repercutiu no Brasil em 2014, com o uso massivo de robôs durante a corrida eleitoral. É realizada então uma breve digressão histórica do ambiente em que encontrava-se o Brasil durante as eleições de 2018 as quais elegeram um extremista de direita. Estudando as eleições de 2018, é possível perceber a presença de um aplicativo significativo: o *whatsapp*. Este é utilizado para troca de mensagens pela grande maioria dos brasileiros e, durante as eleições presidenciais, foi espaço para disparo de mensagens com teor político.

Inegável afirmar que as eleições brasileiras de 2018 tiveram repercussões provenientes de instrumentos do Big Data, o certo é que o direcionamento de mensagens ocorreu, mesmo que de forma diferente do que aconteceu nos Estados Unidos. Enquanto nos EUA, foi utilizado o aplicativo *facebook* para direcionar mensagens aos eleitores, no Brasil o aplicativo utilizado em massa foi o *whatsapp* – aplicativo de troca de mensagens, o qual diferente do utilizado pela *Cambridge Analytica* não possui espaço de propaganda já que se trata de um meio de troca direta entre os interlocutores.

Sendo assim, resta claro o modo como o tratamento de dados pessoais impacta na democracia, ao haver o direcionamento publicitário a partir da análise de dados durante o processo eleitoral, as empresas que adquirirem esses dados possuem poder de fazer o que quiserem com eles, podendo manipular o eleitor e aponta-lo na direção que desejam.

Explica-se, o acesso à banco de dados que informam número de telefone, e-mail, nome e até mesmo status de relacionamento ou posicionamento político dá abertura para classificação dessas pessoas em grupos, quando classificadas é possível emitir mensagens direcionadas influenciando o usuário em sentido x ou y, interferindo assim na liberdade de escolha do eleitor, o qual terá uma visão específica do candidato já que a mensagem foi direcionada à ele – tudo isso sem que haja o consentimento do usuário em dispor de suas informações para tal finalidade.

Após tal conclusão, foi estudado o marco normativo vigente durante as eleições de 2018 sobre o tratamento de dados e o disparo de mensagens ocorrido, concluindo-se que mesmo sem uma lei de proteção de dados em vigor existiam outras legislações, como a eleitoral e o marco civil da internet, que já caracterizavam o uso indevido de dados durante a corrida eleitoral de 2018.

Por fim, foi apresentada a Lei Geral de Proteção de Dados e seus princípios estruturantes, como a finalidade, consentimento, adequação, necessidade, entre outros que devem ser observados em qualquer tratamento de dados. Deste modo, concluiu-se que por mais que tenha-se uma legislação própria sobre proteção de dados, ainda é muito cedo para saber como essas regras vão impactar as campanhas digitais.

A LGPD entrou em vigor somente em setembro de 2020 e ainda não foi aplicada em nenhum processo eleitoral, sendo assim, somente com as eleições de 2022 e com a devida atuação de uma Autoridade Nacional de Proteção de Dados que se terá uma amostra do futuro da democracia na era da informação, enquanto isso permanece a incerteza, porém sabendo-se que de acordo com os princípios e regras trazidos com a LGPD, o regular tratamento de dados deve ser observado.

Imperioso ressaltar que as eleições brasileiras de 2018 tiveram interferência por conta do direcionamento de mensagens conflituosas, notícias fraudulentas assim como vídeos e imagens adulteradas, que influenciaram na liberdade de escolha do eleitor. Os grandes bancos de dados fazem parte da estrutura de marketing brasileiro e dispõem de informações gerais sobre grande parte dos cidadãos, caso estes sejam utilizados para direcionar conteúdo eleitoral tem-se uma violação ao princípio da finalidade.

Desde às eleições de 2014, o Brasil passa por momento de entrelaçamento entre o

digital e o real, tendo o uso de robôs representado grande fluxo durante a corrida eleitoral e posterior impeachment da presidente eleita. Sendo assim, já em 2018 tem-se várias corretoras de dados trabalhando com o intuito de melhorar o marketing de empresas, todavia, essas mesmas podem ser manuseadas também em eleições. Com o escândalo da *Cambridge Analytica*, as corretoras brasileiras ficaram tímidas, entretanto, inegável que o esquema de spams realizado por meio do aplicativo *whatsapp* foi resultado das técnicas do big data e alterou, de certa forma, o resultado das eleições de 2018.

Conclui-se, portanto, que o *whatsapp* e as redes sociais em geral tiveram papel decisivo no processo eleitoral, sendo assim, o tratamento de dados realizado para direcionar mensagens infringiu o direito à liberdade e autonomia do eleitor, o que por conseguinte demonstra que o tratamento de dados acaba por impactar de algum modo na democracia.

REFERÊNCIAS

- ANTONIALLI, Dennys; CRUZ, Francisco Brito. **Privacidade e internet: desafios para a democracia brasileira**. Coleção ensaios democracia digital, texto n. 1: março, 2017.
- ARRUDA, Vinicius Cervantes Gorgone. **Big data, dados pessoais e propriedade intelectual: limites e tutela jurídica das bases de dados**. Dissertação (Mestrado em Direito Político e Econômico): Universidade presbiteriana Mackenzie, São Paulo, 2018.
- AVELINO, Daniel Pitangueira de; POMPEU, João Cláudio; FONSECA, Igor Ferraz da. **Democracia digital: mapeamento de experiências em dados abertos, governo digital e ouvidorias públicas**. Instituto de Pesquisa Econômica Aplicada – Brasília: 2021.
- AYRES PINTO, Danielle Jacon; MORAES, Isabela. **As mídias digitais como ferramenta de manipulação de processos eleitorais democráticos: uma análise do caso BREXIT**. Revista de Estudios Sociales 74: 71-82, 2020.
- BASTOS, Bruna; VON ENDE, Luiza Berger; OLIVEIRA, Rafael Santos. **Abusos algorítmicos e a possível proteção da democracia pela lei geral de proteção de dados brasileira**. Anais do Congresso Internacional de Direito do Vetor Norte, Belo Horizonte: FAMINAS, 2020.
- BECK, Ulrich. **A metamorfose do mundo: novos conceitos para uma nova realidade**. Tradução Maria Luiza X. De A. Borges; Revisão técnica Maria Claudia Coelho. – 1.ed. – Rio de Janeiro: Zahar, 2018.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.
- BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021.
- BOBBIO, Norberto. **O positivismo jurídico: lições de filosofia do direito**. São Paulo: Ícone, 1995.
- BOFF, Salete Oro; FORTES, Vinicius Borges. **Internet e proteção de dados pessoais: uma análise das normas jurídicas brasileiras a partir das repercussões do caso NSA VS. Edward Snowden**. Caderno do programa de Pós Graduação em Direito UFRGS: Volume XI, n.1, p. 340-370, Porto Alegre, 2016.
- BRASIL, Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29.mai.2021.
- BRASIL, LGPD (2018). **Lei Geral de Proteção de Dados Pessoais**. Brasília, 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 29.mai.2021.

BRASIL. **Proposta de Emenda à Constituição nº 17, de 2019**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 29.mai.2021.

BRASIL. **Resolução nº 23.610/2019**. Disponível em: <<https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>>. Acesso em: 29.mai.2021

CANOTILHO, José Joaquim Gomes. **Direito constitucional**. 6ª edição – Livraria Almedina. Coimbra, 1993.

CASTELLS, Manuel (org.); CARDOSO, Gustavo (org.). **A sociedade em rede: do conhecimento à ação política**. Debates Presidência da República. Conferência promovida pelo Presidente da República, 4 e 5 de março de 2005 – Centro Cultural de Belém.

CESARINO, Letícia. **Como vencer uma eleição sem sair de casa: a ascensão do populismo digital no Brasil**. *Internet&Sociedade*, n.1, v.1, p. 91-120, 2020.

CODIND RIGHTS. **DADOS E ELEIÇÕES 2018: uma pesquisa realizada pela coding rights e publicada como relatório brasileiro para o projeto internacional ‘dados pessoais e influência política’, desenvolvido pela tactical technology collective para a plataforma “our data, our selves”**. Publicação: Rio de Janeiro, Outubro 2018. Disponível em:<https://www.codingrights.org/wpcontent/uploads/2018/11/Report_DataElectons_PT_EN.pdf>. Acesso em: set.2020

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. **Os direitos de personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais**. *Revista brasileira de direito civil em perspectiva*. V. 5, N.2, p.22-41, Belém: 2019.

CRUZ, Francisco Brito (coord.); MASSARO, Heloisa. OLIVA, Thiago; BORGES, Ester. **Internet e eleições no Brasil: diagnósticos e recomendações**. InternetLab: São Paulo, 2019.

CRUZ, Francisco Brito... [et al.]. **Direito eleitoral na era digital**. Belo Horizonte (MG): Letramento: Casa do Direito, 2018.

CRUZ, Francisco Brito; MASSARO, Heloisa; BORGES, Ester. **‘Santinhos’, memes e correntes: um estudo exploratório sobre spams recebidos por WhatsApp durante as eleições**. InternetLab: São Paulo, 2019.

DAHL, Robert A. **A democracia e seus críticos**. Tradução Patrícia de Freitas Ribeiro; revisão da tradução Aníbal Mari. – São Paulo: Editora WMF Martins Fontes, 2012.

DAHL, Robert A. **Sobre a democracia**. Tradução de Beatriz Sidou – Brasília: Editora Universidade de Brasília, 2001.

- DATAPRIVACY. **DADOCRACIA – EP.10 – Decisão histórica do STF estabelece proteção de dados pessoais como direito fundamental.** Entrevistados: Bruno Bioni e Mariana Rielli. Entrevistador: João Paulo Vicente. 19.mai.2020, Dadocracia podcast by DataPrivacyBR. Disponível em: <<https://open.spotify.com/episode/1GOHCkafFG9GFRXpZHopmm?si=NoMMO8JISbKDIvOxkQh1wg>>. Acesso em: 26.mai.2021
- DONEDA, Danilo. **A proteção de dados pessoais como um direito fundamental.** Joaçaba, v.12, n.2, p.91-108, jul/dez. 2011.
- DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.
- EMPOLI, Giuliano da. **Os engenheiros do caos.** Tradução Arnaldo Bloch – 1.ed. – São Paulo: Vestígio, 2019.
- FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional.** 9.ed.rev, ampl. e atual – Salvador: JusPODIVM, 2017.
- FORNASIER, Mateus de Oliveira; Beck, Cesar. **Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia.** Revista do Departamento de Ciências Jurídicas e Sociais da Unijuí – Ano XXIX – n. 53 – jan/jun, 2020.
- FUNDAÇÃO GETÚLIO VARGAS. **Robôs, redes sociais e política no Brasil.** FGV/DAPP – Diretoria de Análise de Políticas Públicas, 2018. Disponível em: <<http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web/>>. Acesso em: 29.mai.2021
- GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 4.ed. – São Paulo: Atlas, 2002.
- GOMES, Wilson. **A democracia digital e o problema da participação civil na decisão política.** Revista Fronteiras – estudos midiáticos. VII (3): 214-222, set/dez, 2005.
- GOMES, Wilson. **A democracia no mundo digital: história, problemas e temas.** São Paulo: Edições Sesc São Paulo, 2018.
- KAISER, Brittany. **Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque.** Tradução: Roberta Clapp, Bruno Fiuza. – 1.ed. – Rio de Janeiro: Harper Collins, 2020.
- KAKUTANI, Michiko. **A morte da verdade.** Tradução André Czarnobai, Marcela Duarte. – 1.ed. – Rio de Janeiro: Intrínseca, 2018.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. **Private traits and attributes are predictable from digital records of human behavior**. University of California, Berkeley, CA, 2013.

LAKATOS, Eva Maria. **Fundamentos de metodologia científica** / Marina de Andrade Marconi, Eva Maria Lakatos. – 5.ed. – São Paulo: Atlas, 2003.

LEVY, Pierre. **Cibercultura**/Pierre Levy: tradução de Carlos Irineu da Costa. – São Paulo: Ed.34, 1999.

LIMA, Manuela Ithamar; COSTA, Sebastião P. Mendes. **Direito, inovação e ciência: possibilidades e desafios da sociedade do conhecimento**. Arquivo jurídico, v.6, n.1 – p.173-199. Teresina-PI, 2019.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV editora, 2018.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2.ed. Porto Alegre: Arquipélago Editorial, 2019.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. **Proteção de dados pessoais e democracia: fake News, manipulação do eleitor e o caso da Cambridge Analytica**. REDES: revista eletrônica direito e sociedade. Canoas, v.7, n.3, p. 135-148, out. 2019.

MASSARO, Heloisa; SANTOS, Bruna; BIONI, Bruno; BRITO CRUZ, Francisco; RIELLI, Mariana; VIEIRA, Rafael. **Proteção de dados nas eleições: democracia e privacidade**. Grupo de estudos em proteção de dados e eleições, 2020.

MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia. **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015.

MELLO, Patrícia Campos. **Empresários bancam campanha contra o PT pelo whatsapp**. Disponível em: < <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml>>. Acesso em: 29.mai.2021.

MONTEIRO, A. P. L.; TAVARES, C; BORGES, E; BRITO CRUZ, F; MASSARO, H. **Missing bridges: a comparative analysis of legal frameworks governing personal data in political campaigning in Latin America**. São Paulo: InternetLab, 2021.

MONTEIRO, Celso de Faria. **Redes sociais, marco civil da internet e democracia**. Revista Eletrônica de Direito Eleitoral e Sistema Político. V.4, N.1: São Paulo, 2020.

NETO, José Mauricio Linhares Barreto; NEVES, Fernando Henrique Cardoso. **Compliance eleitoral para partidos – conformidade para a democracia?** Revista Justiça Eleitoral em debate, v.10, n.1, 2020.

ORWELL, George. **1984**/George Orwell; tradução Alexandre Hubner, Heloisa jahn; posfácio Erich Fromm, Ben Pimlott, Thomas Pynchon. – São Paulo: Companhia das letras, 2009.

PRIVACIDADE HACKEADA. Direção: Karim Amer; Jehane Noujaim. Produção: Karim Amer; Jehane Noujaim; Pedro Kos; Geralyn Dreufous; Judy Korin. Estados Unidos. Netflix. 2019.

RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. **Cuál derecho para el nuevo mundo?** Revista de Derecho Privado, núm. 9, julio-diciembre, 2005 pp.5-20. Universidad Externado de Colombia. Bogotá, Colombia.

RUARO, Regina Linden; MAÑAS, José Luis Piñar Molinaro, Carlos Alberto (Orgs.). **Privacidade e proteção de dados pessoais na sociedade digital.** Porto Alegre, RS: Editora Fi, 2017.

RUARO, Regina Linden; RODRIGUEZ, Daniel Pineiro, Brunize Finger (Org.). **O direito à proteção de dados pessoais e a privacidade.** Revista da Faculdade de Direito - UFPR, Curitiba, n.47, p.29-64, 2008

SARLET, Ingo Wolfgang. **Curso de Direito Constitucional/** Ingo Wolfgang Sarlet, Luiz Guilherme Marinoni e Daniel Mitidiero. – 8.ed. – São Paulo: Saraiva Educação, 2019.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal de 1988: contributo para a construção de uma dogmática constitucionalmente adequada.** Direitos Fundamentais & Justiça, Belo Horizonte, ano 14, n. 42, p.179-218, jan/jun, 2020.

SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. **Sociedade da informação: inquietudes e desafios.** Revista de Estudos e Pesquisas Avançadas do Terceiro Setor, Brasília, v.4, n.1, p. 440-480, Jan-Jun, 2017.

SCHWAB, Klaus. **A quarta revolução industrial.** Tradução: Daniel Moreira Miranda – São Paulo: Edipro, 2016.

SHAFFER, Kris. **Data versus democracy: how big data algorithms shape opinions and after the course of history.** Colorado, USA: Apress, 2019.

SILVEIRA, Sergio Amadeu da. **Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas.** São Paulo: Edições Sesc, 2019.

SOUPIZET, Jean-françois. **Cidades inteligentes: desafios para as sociedades democráticas.** Coleção: Ensaio democracia digital. Texto n.2, Edição fundação FHC/Centro Edelstein, 2017.

SOUSA, Devilson da Rocha; GOREZEVSKI, Clóvis. **A manipulação das informações e o perigo à democracia: a ameaça oferecida pelo acesso irrestrito a dados pessoais.** Revista de Direito brasileira v.26, n.10, p.410-426 – Florianópolis, 2020.

VIANA, Daniel Augusto Sabec; SIMÃO FILHO, Adalberto. **Democracia, propaganda eleitoral e proteção de dados.** Anais do Congresso Brasileiro de Processo Coletivo e

Cidadania, n.8, p. 156-173, out/2020.

WARREN, Samuel D; BRANDEIS, Louis D. **The right to privacy**. Harvard Law Review, Vol. 4, N.5, pp.193-220, 1890.

ZUBOFF, Shoshana. **Big Other: surveillance capitalism and the prospects of an information civilization**. Journal of information technology, p.75-89, 2015.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. New York: PublicAffairs, 2018.