UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ
GESTÃO PÚBLICA PARA O DESENVOLVIMENTO ECONÔMICO E SOCIAL

VINICIUS MATOS DE ABREU

PRIVACIDADE E ELEIÇÕES NO CONTEXTO DO USO COMERCIAL DE DADOS REGISTRADOS E PRODUZIDOS NA INTERNET

RIO DE JANEIRO
2023

VINICIUS MATOS DE ABREU

PRIVACIDADE E ELEIÇÕES NO CONTEXTO DO USO COMERCIAL DE DADOS REGISTRADOS E PRODUZIDOS NA INTERNET

Trabalho de Conclusão de Curso entregue ao Curso de Bacharelado em Gestão Pública para o Desenvolvimento Econômico e Social do Instituto de Pesquisa e Planejamento Urbano e Regional da Universidade Federal do Rio de Janeiro – UFRJ, como parte dos requisitos necessários à obtenção do título de Bacharel.

Orientador: Prof. Paulo Ricardo da Costa Reis

Rio de Janeiro
2023

CIP - Catalogação na Publicação

A162p

Abreu, Vinicius Matos de
Privacidade e eleições no contexto do uso comercial de dados registrados e produzidos na internet / Vinicius Matos de Abreu. -- Rio de Janeiro, 2023.
40 f.

Orientador: Paulo Ricardo da Costa Reis.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Instituto de Pesquisa e Planejamento Urbano e Regional, Bacharel em Gestão Pública para o Desenvolvimento Econômico e Social, 2023.

1. Comunicação e tecnologia. 2. Internet nas campanhas eleitorais - Legislação (Brasil). 3. Redes sociais. 4. Eleições. 5. Brasil. [Lei geral de proteção de dados pessoais (2018)] . I. Reis, Paulo Ricardo da Costa , orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

VINICIUS MATOS DE ABREU

Privacidade e Eleições no Contexto do Uso Comercial de Dados Registrados e Produzidos na Internet

Trabalho de Conclusão de Curso entregue ao Curso de Bacharelado em Gestão Pública para o Desenvolvimento Econômico e Social do Instituto de Pesquisa e Planejamento Urbano e Regional da Universidade Federal do Rio de Janeiro – UFRJ, como parte dos requisitos necessários à obtenção do título de Bacharel.

Apresentado em: 18/01/2023

BANCA EXAMINADORA

Paulo Ricardo da Costa Reis

Instituto de Pesquisa e Planejamento Urbano e Regional – UFRJ

Alberto de Oliveira

Instituto de Pesquisa e Planejamento Urbano e Regional – UFRJ

Dedico esse trabalho à minha família,
amigos e professores que passaram na minha vida durante a graduação.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais que me deram toda bagagem e educação ao longo da vida e me formaram como profissional e ser humano. Agradeço ao meu irmão que é uma das minhas maiores inspirações na vida. Agradeço a minha namorada Clarisse por todo apoio e dedicação ao longo desses anos, principalmente ao cuidar do nosso filho para que eu escrevesse este artigo. Também agradeço ao restante da minha família, meus amigos e pessoas próximas que são queridas e desejam meu sucesso. Por fim, mas não menos importante, agradeço ao meu orientador que me auxiliou durante esse processo de construção desse artigo, e tive seu apoio e experiência ao meu lado.

RESUMO

Este trabalho visa discutir o dinamismo da produção, extração e comercialização de dados no âmbito das redes sociais a partir das legislações de proteção de dados que buscam regular o uso destes dados no processo eleitoral e as lacunas deixadas pela referente lei. Além de mostrar como as corporações e pessoas influentes têm manipulado a população, usando suas informações de maneira imprudente para conquistarem posições de seus interesses. A metodologia utilizada é baseada no contexto histórico, bibliografias, reportagens e notícias. O texto expõe como as grandes corporações costumam agir para aumentar seu capital e sua influência, além de como os agentes políticos utilizam formas e artifícios ilegais para valorizarem suas imagens e seus discursos. Ao final do trabalho é possível concluir a importância do papel do Estado na regulamentação de leis que protejam o interesse de seus cidadãos, como por exemplo, a Lei Geral de Proteção de Dados, em detrimento de empresas que visam o lucro a qualquer custo.

Palavras-chave: Privacidade; Redes Sociais; Dados Pessoais; Internet; Eleições

ABSTRACT

This work aims to discuss the dynamism of production, extraction and commercialization of data in the context of social networks from the data protection legislation that seeks to regulate the use of this data in the electoral process and the gaps left by the related law. In addition to showing how corporations and influential people have manipulated the population, using their information recklessly to gain positions of their interests. The methodology used is based on the historical context, bibliographies, reports and news. The text exposes how large corporations tend to act to increase their capital and influence, as well as how political agents use illegal forms and devices to enhance their images and speeches. At the end of the work, it is possible to conclude the importance of the role of the State in regulating laws that protect the interests of its citizens, such as the General Data Protection Law, to the detriment of companies that aim for profit at any cost.

Keywords: Privacy; Social networks; Personal data; Internet; Elections

SUMÁRIO

1 INTRODUÇÃO

A era da internet possibilitou mobilidade, conectividade, comunicação e impactou a forma como a sociedade vive, interage, estuda, decide e consome. Esse espaço virtual trouxe algumas comodidades, a comunicação através de aplicativos em tempo real, contas de banco online, compra de produtos em lojas virtuais, dentre outros serviços que facilitam as pessoas a obterem informações e produtos remotamente. Sendo assim, o aumento de pessoas com acesso a internet corroborou para uma rede mais ampla, dado que cerca de 90% dos lares brasileiros já possuem acesso à internet no Brasil, ainda que existam disparidades significativas na qualidade do acesso, segundo a Pesquisa Nacional por Amostra de Domicílios (BRASIL, 2022). Na mesma direção, um estudo do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic) mostra que o volume de compras e transações bancárias online, chamadas de vídeo e podcasts teve um aumento exponencial desde a chegada do coronavírus ao país. Por exemplo, mais de 52 milhões de brasileiros realizaram compras online em 2019, após a pandemia esse número cresceu para mais de 68 milhões. O consumo de podcast cresceu mais de 132% após a pandemia (JANONE, 2022). Para Valter Teixeira, doutor em psicologia pela UFRJ, esses aumentos estão diretamente ligados à pandemia, principalmente durante o lockdown, em que as pessoas eram obrigadas a se relacionar remotamente, usufruindo de ferramentas virtuais para realizar tarefas cotidianas.

No entanto, para participação nestes espaços virtuais, os usuários precisam registrar informações pessoais para o cadastro ser realizado nas plataformas e sites online. A partir destes e outros registros, foram e continuam sendo criadas diversas aplicações capazes de processar bases de dados gigantescas, até mesmo globais, em tempo real ou muito próximo (KOTLER; KARTAJAYA; SETIAWAN, 2017). Fato é que o usuário da rede, de certa forma, ficou mais exposto e deve ficar em alerta ao se deparar com certas situações. Isso porque, tais dados podem ser comercializados pelas próprias empresas proprietárias das redes sociais e páginas da internet em que o usuário registrou as informações a partir de um termo de uso e política de privacidade.

Diante de um ambiente cada vez mais virtual e do volume de dados que são produzidos neste ambiente, é preciso ter certos cuidados, visando a proteção de dados pessoais e de sua confidencialidade. O vazamento de dados que se

caracteriza por expor informações confidenciais de uma pessoa de forma não autorizada, tem ganhado força devido ao mal uso da tecnologia por parte de consumidores e pela exploração abusiva de grandes corporações. Dados como nome, CPF, endereço ou mesmo números de cartão de crédito são os casos mais comuns. É comum que tais dados sejam vazados também por meio de ataques cibernéticos realizados por *hackers*.

Outras ações ligadas ao uso indevido ou até mesmo criminoso dos dados obtidos a partir das interações na internet foram identificadas em grandes eventos da política internacional, como as eleições americanas de 2010, a eleição de Donald Trump em 2016 e o plebiscito de saída do Reino Unido da União Europeia, o Brexit (FGV, 2017). O processamento de dados pessoais sem a devida transparência e controle também parece ter influenciado a última eleição no Brasil, embaralhando as regras da comunicação, com propaganda massiva sem origem clara e praticamente irrastreável (HENNEMANN, 2019). O uso das redes sociais, para além dos dados, tem sido caracterizado pelas Fake news, que, frequentemente, são criadas visando o lucro através da geração de cliques para os conteúdos disseminados via redes sociais. Também podem ser criadas por motivação ideológica, visando influenciar a opinião pública a favor ou contra determinados candidatos em eleições (COSTA; BLANCO, 2018)

Algumas das principais redes sociais estão envolvidas em alguns processos eleitorais pelo mundo. A empresa Facebook teve que responder no tribunal sobre o seu envolvimento na comercialização de dados (BECKER, 2018). Robôs cooperaram na divulgação de mensagens em larga escala nas eleições de 2018 no Brasil pela plataforma do Twitter (ALBUQUERQUE, 2018). E o Whatsapp foi utilizado como ferramenta na disseminação de fake news no período eleitoral (MELLO, 2018).

Diante deste contexto de ampliação do acesso à internet, mais precisamente nas redes sociais, e do uso decorrente deste processo em termos de monitoramento e comercialização de dados dos usuários e disseminação de fake news, o presente trabalho tem como objetivo discutir o empreendimento de produção, extração e comercialização de dados no âmbito das redes a partir das legislações de proteção de dados que buscam regular o uso destes dados no processo eleitoral. Mostrando o papel do Estado na regulamentação de leis que protejam o interesse de seus cidadãos, como por exemplo, a Lei Geral de Proteção

de Dados, diante dos interesses comerciais de empresas que se apropriam destes dados para produção de lucro.

A metodologia utilizada no presente trabalho tem como fundamento o contexto histórico, bibliografias, reportagens e notícias. O que dá a oportunidade de ter como embasamento o estudo realizado por outros autores, tendo uma base de pesquisa adequada e ao mesmo tempo flexível. Além disso, os dados bibliográficos são importantes para relatar fatos históricos. Alguns dos textos que tiverem relevância para o desenvolvimento do presente trabalho, dentre os quais destacam-se: Henneman (2020), que analisou os impactos da Lei Geral de Proteção de Dados nas eleições de 2020; Almeida, T. (2021), que relacionou proteção de dados pessoais e democracia; e Stochero (2020), que analisou o caso da Cambridge Analytica na eleição presidencial dos Estados Unidos em 2016.

Além desta seção introdutória, o trabalho está organizado em mais seis seções. A próxima seção visa apresentar como os dados dos indivíduos são coletados e manipulados, mostrando as principais ferramentas para alimentação dos grandes bancos de dados produzidos pelos usuários da Internet e como esses dados são utilizados pelas grandes corporações. Na sequência, a seção 3 explica o que é privacidade e como se dá a comercialização de dados digitais. A seção 4 busca dar um panorama do contexto político no âmbito das eleições e desmembra como os agentes articulam e manipulam dados virtuais para fins políticos. A seção 5 explica em detalhes o caso das eleições de 2018 no Brasil e no exterior, destacando como se estabeleceu todo o processo de comercialização de dados. A seção 6 destaca a importância da legislação vigente relativa à proteção de dados e a importância da intervenção do Estado na regulamentação dessas leis. Por fim, na sétima seção, são abordadas as considerações finais do trabalho, dando um panorama geral da situação atual.

2 BIG DATA: EXTRAÇÃO, PRODUÇÃO E APROPRIAÇÃO DE DADOS NA INTERNET

De acordo com a IBM, “big data é caracterizado como um termo aplicado a conjuntos de dados cujo tamanho ou tipo está além da capacidade de bancos de dados relacionais tradicionais de capturar, gerenciar e processar os dados com baixa latência”. E possui uma ou mais características a seguir: grande volume, alta velocidade ou imensa variedade. “Podemos condensar o conceito de Big data

como sendo um grande volume de dados estruturados ou não estruturados, de diversas fontes, que devem ser gerenciados e analisados de forma peculiar" (JUNIOR et al., 2016 *apud* SILVA, 2022, p. 10). Para ser criado um big data, é preciso coletar dados. Segundo Erenberg (2003), algumas formas de coletar as informações sobre o consumidor online por parte das empresas passam pelos: Programas espiões, preenchimento de diversos formulários, registros de atividades por parte dos usuários e pela mineração de dados.

Além disso, algumas ferramentas foram criadas especificamente para facilitar a extração de informações dos usuários. As principais ferramentas utilizadas serão abordadas a seguir:

Os cookies são uma ferramenta importante na coleta de dados dos usuários e são caracterizados por serem pequenos arquivos criados por sites visitados e que são salvos no computador do usuário, por meio do navegador. Esses arquivos contêm informações que servem para identificar o visitante, seja para personalizar a página de acordo com o perfil ou para facilitar o transporte de dados entre as páginas de um mesmo site. Cookies são também comumente relacionados a casos de violação de privacidade na web. (ALVES, 2018)

Por mais que a maioria dos sites alertem sobre o uso de cookies e perguntem se o usuário concorda com o uso deles, é difícil saber até que ponto seus dados estão sendo monitorados, daí a importância de estar bem informado, pesquisar em fontes seguras e autorizar o uso apenas em sites confiáveis. É difícil comparar os cookies que melhoram a performance da navegação com os maliciosos que querem coletar informações e espionar o usuário.

O que os cookies geralmente fazem é direcionar o usuário para algum produto ou serviço específicos. Por exemplo, se uma pessoa começa a pesquisar sobre corrida, atletas ou até mesmo tênis de corrida, e essas páginas tiverem cookies, começará a aparecer em diversas páginas anúncios sobre o assunto pesquisado, então podem aparecer propaganda de determinadas marcas de tênis de corrida em lojas que comercializam esse tipo de produto. Portanto, o consumidor deve ter atenção ao aceitar cookies de determinados sites, pois podem significar uma publicidade abusiva e uma manipulação de dados virtuais.

Outro protagonista são os robôs (também conhecidos como bots) são basicamente "softwares que automatizam reações e comportamentos a partir de instruções dadas por seus programadores, passando-se por seres humanos". Certo

é que essa estratégia pode manipular o processo de escolha de representantes políticos e pautas governamentais (CRUZ *et al*., 2018, p.151 *apud* ALMEIDA, T. 2021).

O algoritmo é outra ferramenta criada para manter as pessoas conectadas, então sempre oferece conteúdos que interessam ao leitor para prendê-lo ao aplicativo. A partir destas ferramentas, os usuários são bombardeados por uma publicidade abusiva mesmo contra a sua vontade. Tristan Harris, ex-designer do Google, explica que há três objetivos principais na maior parte dos algoritmos criados por gigantes de tecnologia: “O de engajamento, para aumentar o seu uso e te manter navegando. O de crescimento, para que você sempre convide amigos e os faça convidar outros amigos. E o objetivo da publicidade, para garantir que enquanto tudo acontece, estamos lucrando o máximo possível com anúncios” (COUTINHO, 2020).

A partir de suas performances, os algoritmos se relevam como construtos sociotécnicos que instituem novas lógicas de seleção, hierarquização, recomendação e de controle dos fluxos informacionais (D’ANDREA, 2021, p. 116). Em articulação com as plataformas online, tais algoritmos instauraram regimes de conhecimento e de visibilidade que se apropriam dos dados disponíveis para identificar padrões, tendências e, cada vez com mais frequência, para fazer previsões (BUCHER, 2018; GILLESPIE, 2018 *apud* D’ANDREA, 2021, p. 116).

Os algoritmos estão presentes em diversos locais da Rede, por exemplo, ao assistir um vídeo no Youtube, aparecerão algumas sugestões de outros vídeos que o usuário possa gostar. Ou ao ouvir determinado estilo de música, surgirão opções parecidas com o estilo musical escutado. As redes sociais tem seus algoritmos inteligentes, voltados para apresentar sempre o conteúdo que mais se assemelha com o gosto do usuário. “Ao instaurar regimes de conhecimento e de visibilidade, os algoritmos diversificam as experiências dos usuários, o que coloca em xeque a representatividade atribuída por pesquisadores aos dados obtidos por meio das plataformas”. (D’ANDREA, 2021, p. 106)

Essa variedade de ferramentas permite ao detentor das informações criar um banco de dados bastante significativo. O que é bastante visado pelas grandes corporações, tendo em vista a ampla aplicação comercial que tais dados poderão viabilizar, incluindo as aplicações em processos democráticos, como as eleições.. Por exemplo, a empresa britânica Cambridge Analytica, contratada pela campanha

do atual presidente americano, utilizou dados pessoais de 87 milhões de usuários do Facebook obtidos ilegalmente para entregar propaganda personalizada via correios, TV e redes sociais aos eleitores americanos. (HENNEMANN, 2019). O Street View, do Google, foi restrito em muitos países e continua a enfrentar litígios sobre o que os reclamantes caracterizaram como táticas de coleta de dados 'secretas', 'ilícitas' e 'ilegais' nos EUA, Europa e outros lugares (OFFICE OF THE PRIVACY COMMISSION OF CANADA, 2010; O'BRIEN, 2012; JAMMET, 2014).

Fazendo um paralelo entre Big Data e a apropriação de dados nas redes, para Zuboff (2015), big data está relacionada a maneira como o capitalismo da informação altera o comportamento humano para gerar valor de mercado, deixando de lado as particularidades de cada indivíduo e enfatizando o número de dados coletados, ou seja, a ênfase está nos números. É formado um imenso banco de dados de acordo com as informações produzidas por indivíduos virtualmente, seja por pesquisar alguma coisa em uma página da internet, mandar um email, escutar uma música ou assistir um filme. Esses dados são recorrentemente extraídos, analisados, preparados e vendidos. E esses fluxos de dados foram rotulados pelos tecnólogos como 'exaustão de dados'. “Presumivelmente, uma vez que os dados são redefinidos como resíduos, sua extração e eventual monetização são menos prováveis de serem contestadas” (ZUBOFF, 2015, p. 79).

Uma vez extraídos, os dados são ligados à questão da mercantilização, utilizado como moeda de troca, fazendo valer a lei da oferta e da demanda. “Os capitalistas de vigilância exploraram um atraso na evolução social à medida que o rápido desenvolvimento de suas habilidades para vigiar com fins lucrativos supera a compreensão pública e o eventual desenvolvimento da lei” (ZUBOFF, 2015, p. 83).

A pretensão de transformar tudo em dados armazenáveis e, a partir deles, gerir diversos processos de monitoramento, ranqueamento e predição é uma característica central da datificação. Uma das consequências da adoção generalizada deste modelo científico é um avanço da ideologia do dataísmo, ou seja, de uma “crença generalizada na quantificação objetiva” (VAN DIJCK, 2017, p. 43 *apud* D’ANDREA, p. 107) propiciada pelos dados. Para Solove (2013), o Google aproveita o pouco conhecimento do indivíduo sobre a coleta de dados para utilizar a captação como instrumento de monetização e lucrar com a comercialização. Ou

seja, a ignorância do povo, inclusive com o autogerenciamento de sua privacidade, é utilizada para ganhos de uma minoria.

3 PRIVACIDADE, MANIPULAÇÃO E COMERCIALIZAÇÃO DE DADOS

Considerando o uso crescente de dados, com as aplicações comerciais destes dados por capitalistas da informação ou capitalistas de vigilância (ZUBOFF, 2015), muito se tem discutido acerca das políticas de uso e privacidade dos dados produzidos e extraídos na Internet. Tais discussões enfatizam a necessidade de proteger a privacidade dos indivíduos e todas as informações coletadas sobre eles na Internet. Não obstante, as legislações para proteção de dados serão discutidas na seção 6. Nesta seção discutiremos mais especificamente o conceito de privacidade e as práticas mais comuns de manipulação de comercialização de dados.

Segundo Reis (2020, p. 52), “privacidade, em essência, é a capacidade de o indivíduo controlar a circulação de informações a seu respeito”. Também pode ser definida como o direito que o indivíduo tem de manter seus dados e informações sob sigilo. Além de administrar a disseminação de notícias relacionadas à vida privada e à intimidade da pessoa (GODOY, 2021).

A captação de dados feita pelas grandes empresas consegue analisar também dados mais aprofundados sobre cada um, inclusive do que a pessoa tem tendência em gostar, perfil das pessoas que ela segue, posicionamento político, lugares frequentados, etc. “Com o uso de dados, a tomada de decisão é mais assertiva, graças à possibilidade de visualizar históricos e padrões de comportamento que seriam impossíveis de se observar através de uma análise limitada” (MAYER-SCHÖNBERGER; CUKIER, 2013 *apud* STOCHERO, 2020, p. 14).

> Ocorre que, muitas vezes, os cidadãos e especialmente os usuários das novas ferramentas tecnológicas como a internet, têm sua privacidade e intimidade violadas por pessoas físicas ou jurídicas que buscam obter suas informações a todo o custo. Além disso, uma vez armazenada a informação, ela é repassada a terceiros sem o consentimento – ou, pior, sem o conhecimento – dos titulares dos dados. Configura-se, daí uma verdadeira violação ao direito à privacidade dos indivíduos, que ficam à mercê de quem detém o conhecimento técnico, sem poder ter controle das informações sobre si mesmo, as quais são bens privados de cada um e merecem a devida proteção e respeito. Porém, no que diz respeito ao titular desses dados, muitas vezes a apropriação de tais informações por

> terceiros gera constrangimento e/ou revolta, por se tratar de dados privados. (MENDONÇA, 2014, p. 2).

Os principais meios pelos quais ocorrem violações de dados, segundo Miriam Fernandes (2021) são: Os ciberataques, responsáveis por grande parte das violações de dados na internet. Roubos ou perdas de equipamentos, permitindo o uso dos aparelhos por pessoas não autorizadas. Divulgação não intencional, ocorre quando há um uso não permitido através de erros no sistema. E vazamento de dados em empresas, condicionando o vazamento de dados de colaboradores pelas redes.

Quando o usuário aceita os termos de utilização de determinados sites, dá a eles a autorização de fazer o que bem entender com suas informações, inclusive comercializá-las. A empresa proprietária do site deveria ser transparente com o usuário, alertando-os e informando-os as maneiras como os dados serão utilizados, se serão vendidos, arquivados ou até mesmo excluídos.

Geralmente esses termos são aceitos sem o usuário ler integralmente o documento, dando direito a esses sites de usarem suas informações, muitas vezes de maneira ilícita (ATHENIENSE, 2010). A desinformação torna esses documentos cada vez mais desprezados, o que é perigoso devido ao teor de seu conteúdo. A pessoa pode se comprometer sem nem mesmo saber do que se trata. Além de não ser do interesse dos sites informar os usuários das implicações de armazenamento e análise cruzadas de grandes quantidades de dados confidenciais.

Os termos de privacidade do Whatsapp, por exemplo, estão disponíveis no site da plataforma e trazem algumas informações importantes que são debatidas neste presente trabalho. Algumas informações que são coletadas por eles: Dados da conta; Mensagens; Contatos; Dados de status; Dados de transações e pagamentos; Além de alguns dados que são coletados automaticamente: Dados de uso e de registro; Dados sobre conexões e dispositivos; Dados de localização; Cookies. A plataforma diz que precisa receber ou coletar algumas informações para operar, fornecer, melhorar, entender, personalizar e comercializar seus serviços e oferecer suporte para eles, incluindo quando você os instala, acessa ou usa. Inclusive compartilha informações dos usuários à medida que utilizam seus serviços e se comunicam por meio deles para ajudar a operar, fornecer, aprimorar, entender, personalizar e comercializar seus serviços (WHATSAPP, 2021).

Na política de dados do Facebook e do Instagram, como são plataformas da mesma empresa (Meta), possuem a mesma política de dados. São apresentadas a seguir algumas informações sobre os dados e privacidade do usuário de acordo com termos disponíveis no site das plataformas: As informações que eles coletam e tratam sobre o usuário dependem do uso dos produtos. Por exemplo, coletam informações diferentes se você vende móveis no Marketplace ou publica um vídeo no Reels no Instagram. Usam as informações coletadas para lhe proporcionar uma experiência personalizada, incluindo anúncios, junto com as outras finalidade, além de oferecerem produtos. Em certos casos, para usarem menos informações relacionadas a usuários individuais, desidentificam ou agregam as informações para que elas não sejam identificadas. Também exigem que parceiros e terceiros sigam regras sobre como usar e divulgar as informações fornecidas.

Esse novo formato de coleta de dados permite às plataformas a terem um banco de dados extenso, com informações privilegiadas das pessoas. Empresas de marketing e publicidade têm explorado cada vez mais esse mercado, tendo em vista a efetividade de obter informações em grande escala, exigindo menos tempo. O problema, no entanto, se dá na forma como as empresas utilizam esse material, o uso e armazenamento das informações pessoais em banco de dados para serem utilizadas quando bem entenderem gera abuso de privacidade (ATHENIENSE, 2010).

Empresas publicitárias estão cada vez mais inseridas nos ambientes virtuais. Propagandas no Facebook, por exemplo, dependendo do valor ofertado pelas empresas, elas têm acesso a diversas possibilidades de personalização, a plataforma dá acesso a definição do público alvo, alcance de usuários e perfil dos clientes. Enquanto as pessoas são bombardeadas de conteúdo publicitário abusivo, as empresas têm acesso a diferentes dados dos consumidores.

Essas propagandas se dão através do perfil de cada consumidor. É criado um parâmetro de consumo e de opinião de cada indivíduo, com projeções sobre escolhas pessoais, diversas áreas da vida particular do usuário são utilizadas para formar um banco de dados (STOCHERO, 2020). Então, o tipo de conteúdo que a pessoa consome, o que ela curte, as pessoas que ela segue, formam uma “bolha” agradável de se viver, criando uma ilusão de que a grande maioria das pessoas próximas possuem as mesmas opiniões. Mas, na verdade, somos induzidos e selecionados a convivermos em determinados grupos onde nos é mais conveniente

e interessante. A tendência das redes sociais é induzir a criação de laços com pessoas mais parecidas conosco e fortalecermos esse laço, criando um senso de comunidade e amparo social no meio virtual.

Por fim, é importante ressaltar que na medida em que tem aumentado a crítica quanto ao uso que as empresas fazem dos dados pessoais ao comercializá-los, também existe a perspectiva de que o próprio indivíduo possa comercializar seus dados. Ou seja, você próprio pode regular o mercado de dados, mas ele continuará como uma engrenagem do capitalismo de vigilância. Cada vez que os dados de algum indivíduo forem comercializados na internet, a pessoa poderá sem recompensada financeiramente. Nesse novo período da história, os dados são a nova matéria prima fundamental no mercado, e, neste momento, os usuários estão no centro dessa economia (CAPPRA, 2020).

4 INTERFERÊNCIA NO CENÁRIO POLÍTICO ELEITORAL

As manipulações e violações de dados produzidos e comercializados a partir da Internet não têm sido orientadas apenas para geração de lucros. Na última década, foram observados diversos casos de apropriação dos dados produzidos na internet para influenciar processos de tomada de decisão no campo político, mais especificamente em processo eleitorais. Nesta seção, serão apresentados os seguintes usos: Robôs, algoritmos e as fake news.

Um artifício que começou a ser muito utilizado a partir das eleições de 2014 são os robôs. Se caracterizam por serem contas controladas por software que geram artificialmente conteúdo e estabelecem interações com não robôs. “Os robôs sociais se distinguem de outros, como robôs autodeclarados ou de spams, pela capacidade de conseguir imitar o comportamento de um usuário real e se passar por seres humanos a partir do uso de inteligência artificial” (DOURADO, 2020), conseguindo interferir em debates e discussões nas redes.

No ambiente político, os robôs têm sido usados por quase todos os políticos não apenas para conquistar seguidores, mas também para atingir opositores e forjar discussões. Esses robôs são programados para criarem notícias falsas e manipularem debates políticos para influenciarem a opinião pública enviando mensagens em larga escala (FGV, 2017). A eleição de 2018 no Brasil foi marcada por robôs programados para dispararem fake news para usuários pelas redes sociais. As mensagens continham conteúdos duvidosos e notícias infundadas,

disseminando notícias falsas e dados alterados sobre outros candidatos à presidência.

Os algoritmos também ganharam muita notoriedade nos últimos anos, programas de inteligência artificial moldaram essa ferramenta para entregar melhores resultados. Por exemplo, algoritmos mais atuais conseguem identificar perfis famosos e segui-los, identificam um assunto na rede e geram um pequeno texto por meio de programas específicos, gerando mais interação (FGV, 2017). Ou seja, é uma ferramenta que reúne uma grande gama de informações dos usuários. Tristan Harris, ex-designer do Google, afirma que tudo o que já fizemos, todos os cliques, os vídeos que assistimos, as curtidas, tudo isso ajuda a moldar um modelo de dados cada vez mais fiel. Assim que esse modelo é criado, é possível prever um padrão de comportamento (COUTINHO, 2020).

Para além dos modelos de previsão de comportamento a partir do monitoramento do usuário na Internet, o uso de fake news também tem se destacado como uma ferramenta para influenciar o comportamento político. Fake news pode ser conceituada como notícias falsas geradas e divulgadas intencionalmente para manipular as concepções dos cidadãos e fomentar ideologias nocivas à democracia (JARDELINO; CAVALCANTI; TONIOLO, 2020). “Ao explorar a dimensão da personalidade que mais afeta cada pessoa, a empresa aumenta a chance de que o eleitor vote em determinado candidato” (FLORES, 2017 *apud* HANNEMANN, 2019, p. 10), facilitando a união de votos de pessoas com visões distintas.

Além destas ferramentas, há outras técnicas que são utilizadas nas campanhas políticas e serão afirmadas na definição dos Grupos de Estudos em Proteção de Dados e Eleições (2021, p. 02):

> As campanhas políticas se apropriaram das novas ferramentas e técnicas de marketing comercial baseadas no tratamento de dados pessoais, tais como: (i) o micro direcionamento (microtargeting) e o impulsionamento de notícias, propagandas e anúncios pagos, (ii) a segmentação de audiência-alvo de acordo com perfis específicos e amostras selecionadas, bem como (iii) o envio automatizado de mensagens em massa.

4.1 CASOS EXTERNOS

Para além das fronteiras brasileiras, o filme Privacidade Hackeada (NETFLIX, 2019) retrata o uso de dados pessoais e privados de assinantes do Facebook com o intuito de manipular e influenciar eleitores nos EUA e Inglaterra, contribuindo para a eleição de Donald Trump e na interferência da votação do Brexit, o que ocasionou na saída da Inglaterra da União Europeia. Este destaca ainda os testes realizados pela Cambridge Analytica em pequenos países, antes da sua aplicação nos EUA e Inglaterra no qual os dados pessoais e o perfil das pessoas no Facebook eram analisados, e através destes era possível determinar os indecisos.

A empresa era propriedade do bilionário do mercado financeiro Robert Mercer, ex-especialista de dados da IBM (FORBES, 2017), e era presidida, à época, por Steve Bannon, então principal assessor de Trump.

> A Cambridge Analytica, foi criada “para resolver o vácuo no mercado político republicano dos EUA”, que se tornou evidente quando Mitt Romney foi derrotado nas eleições presidenciais de 2012. Os democratas estavam aparentemente liderando a revolução tecnológica, e a análise de dados e o engajamento digital eram áreas onde os republicanos não conseguiram alcançá-los. Vimos isso como uma oportunidade (ALEXANDER NIX, 2016).

Christopher Wylie (BBC, 2018 *apud* STOCHERO, 2020), um ex-funcionário da empresa, confirmou que a CA coletava dados de mais de 50 milhões de usuários do Facebook, para serem usados em estratégias na eleição presidencial dos EUA. O banco de dados é formado através de um teste de personalidade realizado pelos usuários, além de ter informações do próprio usuário, conseguiam de seus amigos também.

A Cambridge Analytica conseguiu criar um Big Data extremamente extenso, conseguindo implantar e manipular diversos casos na área política. “A CA percebeu que poderia integrar informações de seu estudo a uma gama de dados de plataformas, cookies, compras online e resultados de votação para criar mais de 5.000 pontos de dados em 230 milhões de adultos nos EUA” (ISAAK; HANNA, 2018 *apud* STOCHERO, 2020, p. 31). Segundo Educiber (2019), para Brittany Kaiser, que gerenciou todas as campanhas políticas da CA durante anos —

incluindo a do Brexit e a de Trump —, a ferramenta que a empresa tinha em mãos não era apenas um facilitador de marketing em massa, mas uma verdadeira arma de manipulação de mentes, que pode ser usada para mudar os rumos de uma nação manipulando cada um de seus cidadãos a partir do medo, e continuar manipulando-os para que continuem acreditando no que quer que devem acreditar.

As primeiras revelações sobre os escândalos políticos vieram a público ainda em dezembro de 2015 e alertavam para o uso de dados obtidos mediante “testes psicológicos” pela campanha do senador estadunidense Ted Cruz à vaga do Partido Republicano para as eleições presidenciais do ano seguinte (DAVIES, 2015).

A eclosão definitiva se deu em maio de 2018, quando revelações feitas pelo jornal inglês The Guardian (CARDWALLARD; GRAHAM-HARRISON, 2018 *apud* HENNEMANN, 2019) e outras publicações apontaram que dados de dezenas de milhões de usuários do Facebook teriam sido coletados pela CA. Ou seja, a política de compartilhamento de dados com terceiros adotada pelo Facebook permitiu não apenas que milhões de cidadãos fossem expostos a anúncios e outras ações hiperpersonalizadas, mas ainda escancarou, para um público mais amplo, como as práticas de colaboração entre usuários da comunidade global presidida por Mark Zuckerberg eram fortemente orientadas para uma otimização do uso comercial da datificação.

O então executivo chefe da empresa, Alexander Nix (FORBES, 2018), explicou em três fatores como a Cambridge Analytica agia no processo eleitoral:

> a) teorias de ciências comportamentais são utilizadas para se estabelecer elementos genéricos de personalidades humanas que sejam do interesse do estrategista de campanha para a categorização de eleitores; b) uma infinidade de dados pessoais é analisada pela metodologia de big data dentro de um modelo informático capaz de fazer um enquadramento de pessoas reais em diferentes categorias de personalidade, deduzindo assim as inclinações políticas dos indivíduos; c) as mensagens de propaganda são desenvolvidas de forma segmentada e entregues com um alto grau de aderência a cada eleitor.

Segundo (STACEY, 2019 *apud* HENNEMANN, 2019), Trump se envolveu em outro escândalo envolvendo o Facebook. Criou-se uma ferramenta desenvolvida por um professor da Universidade de Cambridge que coletou dados de 270 mil pessoas para fins científicos, mas estes dados foram transferidos posteriormente sem autorização para uma empresa que participou da campanha do então

candidato à presidência dos EUA. De acordo com a matéria apresentada pelo G1, em 2018, as informações dos usuários do Facebook foram coletadas por um aplicativo chamado this is your digital life (essa é sua vida digital, em português), que pagou a centenas de milhares de usuários pequenas quantias para que eles fizessem um teste de personalidade e concordassem em ter seus dados coletados para uso acadêmico. Após o episódio, o Facebook fechou um acordo de 5 bilhões de dólares com as autoridades norte-americanas para o encerramento do processo, alegando vulnerabilidade em sua política de privacidade.

Além disso, de acordo com a pesquisa Semantikos (2017), a equipe de Trump criou uma rede de sites exclusivamente para direcionar as campanhas de anúncios para mensagens falsas, muito partidárias ou unilaterais sobre seus oponentes. Sites que podem ser vinculados uns aos outros por meio de endereços IP, administradores e servidores.

4.2 ELEIÇÕES NO BRASIL

Com as manifestações de 2013, o cenário político passou por mudanças e deu início a uma nova era. Destacam-se três pontos primordiais para compreender o panorama atual: Primeiro, o início da Operação Lava Jato. Segundo, o impeachment da então presidente Dilma Rousseff. Terceiro, a eleição de 2018 que foi marcada pela polarização e pelo aumento de ferramentas virtuais que permitiram um maior alcance de eleitores, mas ao mesmo tempo, abriu espaço para temas como fake news e robôs automatizados na política (BRITES; PORCELLO, 2018 *apud* JARDELINO; CAVALCANTI; TONIOLO, 2020).

Durante este cenário, mais precisamente em 2017, a reforma eleitoral foi promulgada e a propaganda eleitoral realizada por mecanismos de impulsionamento de conteúdo na internet foi autorizada. Tal mudança repercutiu de forma a transformar as eleições, agora mais digitais do que nunca (ALMEIDA, T. 2021). Com isso, “abriu-se a possibilidade das campanhas utilizarem ferramentas de micro direcionamento oferecidas na internet, sobretudo no Facebook, em que é possível escolher um público-alvo, dentro de determinada região, por faixa etária ou gênero” (CRUZ, 2018, p. 172, *apud* HENNEMANN, 2019, p.11). Permitindo as campanhas a direcionarem o estilo de eleitor que elas visam alcançar.

Além disso, o que corroborou para a ascensão do conteúdo digital nas mídias sociais foi a vedação das doações para partidos e candidatos vindos de pessoas físicas (HENNEMANN, 2019). Tal medida teve impacto direto nas campanhas eleitorais que buscaram novas formas de financiamento. A partir disso, cresceu o uso de ferramentas tecnológicas para captar eleitores, tendo como ênfase a procura de investimentos em softwares e em equipes especializadas de marketing digital.

Por exemplo, a disseminação de notícias falsas por robôs em redes sociais teve um impacto significativo no resultado das eleições de 2018. O Gerente de Políticas Públicas e Eleições Globais do WhatsApp, Ben Supple, admitiu publicamente que constatou na eleição brasileira de 2018, “atuação de empresas fornecedoras de envios maciços de mensagens que violaram os termos de uso do aplicativo para atingir um grande número de pessoas” (MELLO, 2019 *apud* HANNEMANN, 2019, p. 13). Esse envio maciço de mensagens só é possível porque essas empresas detêm um enorme banco de dados com as características dos usuários.

Segundo reportagem exibida pela Folha de São Paulo (2018), as empresas encaminhavam mensagens em massa utilizarando dados de terceiros, obtidos de forma ilegal – tendo como base a falta de autorização das pessoas e o seu desconhecimento sobre a prática –, para, mediante falseamento de identidade, realizar o cadastro junto às empresas de telefonia. Por meio destes cadastros, conseguiam os devidos registros de chips de celulares e concretizavam os disparos em massa das mensagens de cunho eleitoral.

Por meio da Ação de Investigação Judicial Eleitoral de 2021, descobriu-se que uma rede de empresas recorreu ao uso fraudulento de nomes e CPF de idosos para registrar chips de celular e garantir o disparo de lotes de mensagens em benefício de políticos. Havia uma relação de dez mil nomes de pessoas nascidas entre 1932 e 1953 enviada por Hans River do Rio Nascimento, ex-funcionário da empresa Kiplix, à reportagem, o que representa a prova real das alegações. Isso porque, nessa faixa etária, seria facilitada a utilização das informações pessoais por terceiros sem o conhecimento dos interessados. Considerou, ainda, que este grupo de agências (Yacows e Kiplix) teria sido subcontratado pela empresa AM4, maior fornecedora da campanha do candidato da Coligação “Brasil Acima de Tudo, Deus Acima de Todos” (TSE, 2021). Por fim,

a Ação de Investigação Judicial Eleitoral de 2021 identificou que mensagens foram enviadas para contatos registrados pela campanha dos candidatos, além dos contatos que foram vendidos pela empresa contratada. Perfis falsos foram utilizados durante a campanha, além de compra de cadastros de usuários irregulares, formando a ilegalidade. (TSE, 2021).

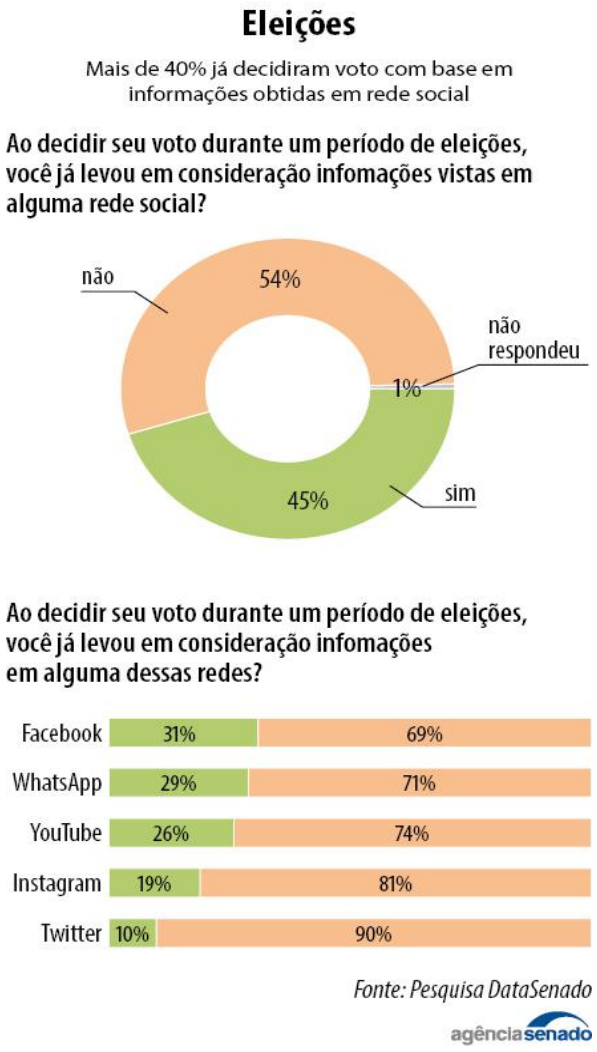
Seguindo a mesma linha, de acordo com reportagem realizada pela Folha de São Paulo (2019), empresários apoiadores de Bolsonaro contrataram diretamente os serviços das agências de marketing digital Yacows, Quick Mobile e CrocServices, e também adquiriram 40 licenças de um software de disparos em massa da empresa espanhola EnviaWhatsApp, o que possibilitou o encaminhamento de até 20 mil mensagens por hora, aumentando o poder de alcance do candidato. Contudo, é proibido o uso de ferramentas de automatização, como os softwares de disparo em massa. Em outubro de 2018, uma outra reportagem da Folha de São Paulo, 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. Ou seja, determinadas empresas que estavam sendo financiadas, identificavam os perfis dos eleitores sensíveis a temas específicos, e, a partir disso, tentavam influenciar o voto desses eleitores com informações seletivas.

Essa influência cresceu com a utilização de ferramentas ainda mais aprimoradas para automação e interpretação de mensagens enviadas por meio de grupos no Whatsapp, segundo reportagem do site de notícias The Intercept. As novas tecnologias possibilitaram a criação de filtros complexos de checagem das preferências dos usuários, de modo a permitir o direcionamento de conteúdo personalizado a cada contato presente nos bancos de dados dos sistemas (REIS, 2021).

Os episódios relatados indicam a violação de inúmeros dispositivos da legislação eleitoral. Existem evidências que indicam o uso destas aplicações de dados na eleição, o que pode ter influenciado o resultado da eleição. Além da provável violação também do art. 57-B, III, que autoriza o envio de mensagens eletrônicas apenas para “endereços cadastrados gratuitamente pelo candidato, partido ou coligação” (CRUZ; MASSARO; BORGES, 2018, p. 26).

Uma pesquisa realizada pelo instituto DataSenado, também assinalou a influência das plataformas digitais nas eleições brasileiras, ao constatar que 45% dos participantes afirmaram terem sido influenciados por informações vistas em redes sociais. Facebook e Whatsapp foram os aplicativos que tiveram maior impacto nas eleições (AGÊNCIA SENADO, 2019).

Tabela 3: Influência crescente das redes sociais como fonte de informação para o eleitor



Fonte: Agência Senado

Neste contexto de proliferação de informações divulgadas nas redes, as estratégias de campanha eleitoral começaram a ter como foco a credibilidade e caráter de seus oponentes, minando a imagem e a honra dessas pessoas através da proliferação de notícias falsas veiculadas midiaticamente. Como as redes

sociais são o principal instrumento de comunicação de alguns candidatos, eles conseguem manipular os debates públicos mais amplamente, já que o contato pelas redes sociais é direto com os seguidores. O candidato pode abordar qualquer tipo de discussão sem restrição (exceto assuntos que ultrapassem o limite dado pela respectiva rede social e pela legislação vigente).

Constata-se que as normas vigentes durante a realização das eleições brasileiras de 2018 não tratavam de forma específica sobre as diversas manipulações com dados, porém, já traziam elementos 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 (ALMEIDA, T. 2021).

5 LEGISLAÇÃO E PROTEÇÃO DE DADOS DOS USUÁRIOS

O conteúdo apresentado nas seções anteriores contextualizou e descreveu o problema público que envolve o uso de dados produzidos e registrados na Internet e as violações de privacidade destes dados para fins econômicos e políticos.

A preocupação com a proteção de dados antecede o desenvolvimento da Internet e das aplicações de Big Data. A primeira lei de proteção de dados, inclusive, foi uma lei criada em Hesse, na Alemanha, em 1970. A referida lei visava proteger todos os dados digitalizados contra vazamentos, modificação ou exclusão por funcionários públicos (RULE; GREENLEAF, 2010 *apud* STOCHERO, 2020). No entanto, após a criação da internet e os sucessivos escândalos envolvendo dados produzidos e capturados na rede, para reduzir as incertezas quanto à proteção de dados, mais precisamente em 25 de maio de 2018, entrou em vigor o Regulamento Geral de Proteção de Dados (GDPR) que avançou para além das fronteiras europeias, inspirando iniciativas nacionais na busca da proteção de dados pessoais, tanto na esfera pública como na esfera privada, passíveis de identificação no ciberespaço (SANTOS, C.; FERNANDES, 2021). Permitindo que cada nação tivesse a liberdade para definir sua própria legislação, já que é difícil delimitar fronteiras quando se trata de Internet.

No âmbito nacional, o Marco Civil da Internet, através da Lei n° 12.965 de 2014, criou a norma legal que disciplina o uso da Internet no Brasil por meio da

previsão de princípios, garantias, direitos e deveres para quem faz uso da rede, bem como da determinação de diretrizes para a atuação do Estado. A Lei Geral de Proteção de Dados Pessoais (LGPD), por sua vez, foi criada logo após, em 2018, pela lei nº 13.709, sendo um marco regulatório para o tratamento da proteção de dados no Brasil, visando garantir os princípios da privacidade e transparência dos cidadãos alinhados com padrões internacionais.

De forma complementar, a Lei n. 13.853, de 08 de julho de 2019, prevê a criação da Autoridade Nacional de Proteção de Dados (ANPD), que é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Além de regulamentar o tratamento de dados pessoais e aplicar as penalidades previstas em casos de descumprimento da lei, a ANPD tem como função informar a população sobre a política de proteção de dados e os direitos sobre os seus próprios dados. A ANPD é uma autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal, de acordo com a lei nº 13.709. É um órgão independente e parte do Poder Executivo do Governo Federal criada com atribuições de fiscalizar e divulgar como toda a informação pessoal e dados pessoais que circulam e são utilizados pelas empresas devem ser tratados, ou seja, fazer cumprir a LGPD. Ou seja, a ANPD é o órgão público chave para compreender as respostas públicas que são dadas por meio da legislação, traduzindo a forma como a gestão pública atua na proteção de dados pessoais, buscando concretizar os objetivos contidos na legislação.

Quanto aos objetivos da LGPD, de acordo com o MPF (2022), a referida lei visa garantir os direitos fundamentais da privacidade e liberdade. A função da legislação brasileira 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), além de resguardar o cidadão juridicamente criando um padrão regulatório para proteger os dados pessoais baseado em exemplos internacionais.

A LGPD em seu artigo 6º elencou 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 *apud* ALMEIDA, T. 2021). De acordo

com a LGPD, o cidadão tem o direito de acessar, retificar e apagar seus dados, além de autorizar o tratamento deles e solicitar sua portabilidade. A lei garante que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Se há o processamento de informações sobre pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser observada. Além de autorizar também o compartilhamento de dados pessoais com organismos internacionais e com outros países, desde que observados os requisitos nela estabelecidos.

Em que pese a relevância da criação de uma instituição como a ANPD, Serpro (2022) ressalta que há um problema na falta de autonomia administrativa do órgão diante da fiscalização de dados realizada pelo próprio governo. Além disso, dispor de uma autoridade nacional para regulamentar a lei faz com que o Brasil esteja dentro do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, credenciando o país a enviar informações e dados para o bloco. O papel da ANPD é fiscalizar se a LGPD está sendo cumprida e penalizar caso o contrário. Regulando e orientando preventivamente sobre as aplicações da lei para uma melhor colaboração de cidadãos e organizações (SERPRO, 2022).

Fazendo uma conexão entre a legislação vigente e o cenário político, pode-se observar que a lei tem combatido alguns tipos de abusos através da exigência de responsabilidade pelo vazamento de dados, pois cada vez mais tem sido frequente a ocorrência de incidentes de uso indevido.

Não obstante, a legislação é apenas um dos elementos capazes de contribuir para o controle dos abusos e violações a partir de dados produzidos na rede. Isso porque, um ambiente com menos interferência de conteúdos falsos e difamatórios nas eleições também depende da combinação de metodologias e tecnologias, bem como de atores, reunindo: Veículos da imprensa, agências de checagem de dados, pesquisadores, especialistas em comunicação digital e empresas detentoras das plataformas sociais. (ALMEIDA, R. 2018).

Pode-se dizer que a aplicação da LGPD ocorre em duas vertentes distintas: Uma admite a vulnerabilidade do titular de dados, exigindo condições básicas para o consentimento, levando em consideração o abismo informacional diante das grandes tecnologias. Por outro lado, externaliza o papel da autonomia privada tratando o usuário como um contratante, tendo a responsabilidade de gerir as suas próprias informações pessoais. Os dados pessoais, quando passam a ser

regulados por uma lei, são, portanto, uma mercadoria universalizada, disponível a todos no mercado, cuja troca é agora legitimada. O progresso do capitalismo de vigilância, termo dado por Zuboff (2019), está diretamente ligado a conversão das vivências humanas em dados, e, posteriormente, a reintegração disso na existência, através de investimentos, ganhos e novos negócios (FORNASIER; KNEBEL, 2020).

O Big Data trabalha com a reutilização de dados para diferentes finalidades que não são estabelecidas anteriormente. O que acarreta no prejuízo da autonomia do usuário, que é um dos problemas apresentados, já que a LGPD garante que o usuário tenha conhecimento da finalidade específica determinada para os seus dados. O mesmo carece de condições materiais para a execução da ampla liberdade sobre seus dados pessoais. Além disso, a referida lei regulamenta a criação de um mercado de dados no Brasil, que se assegura através desse consentimento do usuário, regulando e legitimando a exploração de dados como uma contratação (FORNASIER; KNEBEL, 2020)

> O problema das databases não é que os coletores falham em pagar o valor adequado das informações pessoais. O problema é a falta de controle, falta de conhecimento sobre como esses dados serão usados no futuro e falta de participação das pessoas no processo. Não é suficiente permitir que as pessoas vendam suas informações, relegar a elas toda a titularidade sobre e permitir que companhias as usem esses dados como lhes for apropriado. Isso proporciona às pessoas uma troca do tipo “tudo ou nada” na qual provavelmente elas se submeterão quando desconhecerem como essa informação poderá ser usada no futuro [...] Privacidade é uma questão que afeta a estrutura da sociedade e envolve nossa relação com a burocracia pública e privada (SOLOVE, 2004, p. 90).

É preciso enxergar o ambiente dos dados de forma macro, uma vez que um dado isolado de uma pessoa não faz tanta diferença, porém, um conjunto de dados recolhidos de várias pessoas pode ser revelador e pode dar uma informação valiosa para o detentor. O mesmo raciocínio é válido para uma informação comportamental dada por uma pessoa, uma informação em específico pode não trazer muitas revelações, mas um conjunto de informações da mesma pessoa é uma ameaça à privacidade da própria, uma vez que não se sabe as potenciais utilidades que podem ser destinadas a esses dados (SOLOVE, 2013).

Segundo Fuchs (2019, p. 58-59) “o poder algorítmico do capitalismo de vigilância pode resultar em um mundo que seja um grande shopping center, com humanos colonizados pela lógica comercial, no âmbito do seu comportamento”. A

população acaba vivendo à mercê dos agentes do mercado e de grandes empresas, como se a remuneração conquistada pela vigilância fosse uma forma de compensação, independente se os lucros são maiores que os prejuízos ou não (MOROZOV, 2018).

Além do debate sobre a verdadeira aptidão do usuário para entender e estimar os possíveis prejuízos e perdas, ainda mais com uso de termos enormes e difíceis por parte do mercado de dados, é necessário refletir sobre o desequilíbrio de poderes que estão relacionados no tratamento do mesmo (Morellato; Santos, B. 2021). Em uma sociedade capitalista informacional, a maioria das relações se dão através do consumo. Reflexo disso é que no capitalismo de vigilância é criado um mercado mediante a digitalização da vida (BELLER, 2013 *apud* Morellato; Santos, B. 2021).

6 CONSIDERAÇÕES FINAIS

O presente trabalho tratou dos principais temas em torno da comercialização de dados virtuais, como os agentes exploradores costumam agir, o papel do usuário nesse contexto, como a legislação vigente pretende proteger os direitos dos cidadãos e as brechas deixadas pelas próprias leis.

Somos bombardeados por propagandas excessivas, marketings abusivos, spams na caixa de e-mail, monitoramento de atividades durante o uso da internet e temos nossos dados expostos sem permissão. É crucial entender a importância da privacidade e impedir que dados pessoais sejam usados como moeda de troca em transações exuberantes entre grandes corporações que detém um enorme banco de dados.

A LGPD regulamentou a comercialização de dados desde que o usuário permitisse através do seu consentimento. A questão principal não está no consentimento em si, mas na desigualdade estrutural atribuída a tecnologia, pois os usuários enquanto sociedade apenas contribuem fornecendo os seus dados, enquanto as empresas realizam a tradução desses dados diante do avanço tecnológico e de inteligências artificiais. Os usuários que são os produtores da matéria prima, proprietários dos seus dados, são manipulados por um panorama sem nenhum tipo de controle social e acabam não tendo acesso ao que seria o resultado de suas próprias experiências. Há um abismo informacional entre a população e as empresas detentoras de máquinas cada vez mais avançadas

tecnologicamente (FORNASIER; KNEBEL, 2021). A exploração econômica dos dados foi viável através das condições materiais e pelos padrões de vigilância impostos pela sociedade. Abrindo margem para novas desigualdades sociais e amplificando novos padrões de exploração na internet (FUCHS, 2019).

O controle político se tornou mero detalhe, atualmente, com atualizações tecnológicas cada vez mais complicadas e de difícil acesso, faz com que os usuários cedam informações pessoais comportamentais em troca de melhores condições de serviços que serão cada vez mais necessários no cotidiano. Um dos principais tipos de controle deixará de ser imposto fisicamente e passará a ser virtual, tornando o usuário refém de seus próprios dados (FORNASIER; KNEBEL, 2021). Como afirma Zuboff (2019, p. 309): Conhecimento, autoridade e poder estão do lado do capital de vigilância, enquanto as pessoas são, somente, “matéria prima humana”. Nesse modelo de economia, os indivíduos não são obrigados a fornecerem seus dados ou informações, mas acabam fornecendo-os pela falta de conhecimento e de alternativa diante do cenário atual.

Logo, o jogo de interesses presente no mercado de dados representa um risco real à democracia, dada a influência das empresas e agentes públicos perante a sociedade. A partir daí temos a necessidade de uma legislação eficiente, em que as instituições e os direitos dos cidadãos sejam respeitados. O fortalecimento destas instituições de controle, como por exemplo a ANDP, é um dos caminhos de resistência e de fortalecimento da democracia.

Ainda que o trabalho tenha buscado discutir o empreendimento de produção, extração e comercialização de dados no âmbito das redes a partir das legislações de proteção de dados que buscam regular o uso destes dados no processo eleitoral, por meio de levantamento ou pesquisa bibliográfica, é preciso registrar algumas limitações, bem como indicações de pesquisas futuras. Em termos de limitações, cabe uma melhor distinção entre as discussões de “fake news” e “big data”, destacando o embasamento legal e o contexto político de cada um separadamente. Em termos de pesquisas futuras, vale aprofundar a questão da privacidade além do contexto eleitoral, explorando as desigualdades geradas pelo capitalismo. Além de um aprofundamento dos limites dos instrumentos legais no Brasil e no exterior para coibir a influência de grupos econômicos influentes.

REFERÊNCIAS

ALBUQUERQUE, Filipe. Exército de robôs segue presidenciáveis no Twitter – e isso ameaça influenciar a eleição. **Gazeta do povo**, 04 de jul. 2018. Debate Político. Disponível em: https://www.gazetadopovo.com.br/politica/republica/eleicoes-2018/exercito-de-robos-segue-presidenciaveis-no-twitter--e-isso-ameaca-influenciar-a-eleicao-duzlzrw4pln32icfsj73htjx8/. Acesso em: 20 de dez. 2022.

ALMEIDA, Raquel de Q. **Fake news**: arma potente na batalha de narrativas das eleições 2018. Ciência e cultura, v. 70, nº 2, São Paulo, 2018. Disponível em: http://dx.doi.org/10.21800/2317-66602018000200004. Acesso em: 27 de out. 2022.

ALMEIDA, Thiago Martins. **Proteção de dados pessoais e democracia**: Os impactos do tratamento de dados nas eleições brasileiras de 2018. São Luís, 2021. Monografia (Graduação em Direito) - Curso de Direito – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2021, f. 72. CDU 342.8:004.738.5. Disponível em: http://repositorio.undb.edu.br/bitstream/areas/554/1/THIAGO%20MARTINS%20ALMEIDA.pdf. Acesso em: 07 de dez. 2022.

ALVES, Paulo. **O que são cookies?** Entenda os dados que os sites guardam sobre você. Techtudo, 04 de out. 2018. Internet. Disponível em: https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml. Acesso em: 14 de out. 2022.

ATHENIENSE, Alexandre. **Empresas vendem dados pessoais do consumidor na internet**. Jusbrasil, 2010. Disponível em: https://alexandre-atheniense.jusbrasil.com.br/noticias/2556744/empresas-vendem-dados-pessoais-do-consumidor-na-internet. Acesso em: 16 de ago. 2022.

AUDI, Amanda; Dias, Tatiana. Seu número de telefone vale 9 centavos no zap dos políticos. **The Intercept**, 22 out. 2018. Social. Disponível em: https://theintercept.com/2018/10/22/whatsapp-politicos/. Acesso em: 07 de dez. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ações e Programas. **Gov.**, 2021. https://www.gov.br/anpd/pt-br/acesso-a-informacao/programas-projetos-e-acoes. Acesso em: 03 de jan. 2022.

BAPTISTA, Rodrigo. **Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado**. Senado Notícias, 12 de dez. 2019. Institucional. Disponível em:

https://www12.senado.leg.br/noticias/materias/2019/12/12/redes-sociais-influenciam-voto-de-45-da-populacao-indica-pesquisa-do-datasenado. Acesso em: 02 de out. 2022.

BATISTELLA, Carla. **O que é a venda de dados e quais os impactos da LGPD?** Certifiquei, 01 de mar. 2021. Segurança da Informação. Disponível em: https://www.certifiquei.com.br/venda-dados/. Acesso em: 16 de ago. 2022.

BECKER, Fernanda. Facebook: a máquina de fazer dinheiro agora se prepara para se enquadrar à lei. **El País**, São Paulo, 17 abr. 2018. Tecnologia. Disponível em: https://brasil.elpais.com/brasil/2018/04/13/tecnologia/1523575337_496030.html. Acesso em: 20 de dez. 2022.

BIONI, Bruno; MONTEIRO, Renato Leite. **Proteção de Dados Pessoais Como Elemento de Inovação e Fomento à Economia**: O impacto econômico de uma lei geral de dados. In: REIA, Jhessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo. Horizonte presente tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito; FGV, p. 232-248, 2019. Disponível em: http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27448/Horizonte%20presente%20-%20tecnologia%20e%20sociedade%20em%20debate.pdf?sequence=1&isAllowed=y. Acesso em: 13 de jan. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidente da República, [2014]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03 de jan. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidente da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 de jan. 2022.

BRASIL. **Lei nº. 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 04 de jan. 2022.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº. 23.610, de 18 de dezembro de 2019**. Relatoria Min. Luís Roberto Barroso. Publicado no DJE-TSE, nº 249, de 27.12.2019, p. 156-184. Disponível em:

https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 28 de out. 2022.

CAPPRA, Ricardo. **O mercado dos dados pessoais**. Mit Technology Review, 2020. Negócios e Economia. Disponível em: https://mittechreview.com.br/o-mercado-dos-dados-pessoais/. Acesso em: 03 de jan. 2023.

COSTA, Cristina; Blanco, Patrícia. **Liberdade de expressão e campanhas eleitorais - Brasil 2018**. São Paulo: ECA-USP, 2019, 273 p. DOI: 10.11606/9788572052320. Acesso em: 02 de out. 2022.

COUTINHO, Dimítria. **O dilema das redes**: O que aprendemos com o filme que expõe o pior da tecnologia. 2020. Tecnologia. Disponível em: https://tecnologia.ig.com.br/2020-09-19/o-dilema-das-redes-o-que-aprendemos-com-o-filme-que-expoe-o-pior-da-tecnologia.html. Acesso em: 07 de jan. 2022.

D'ANDRÉA, C. (2021). **Para além dos dados coletados**: políticas das APIs nas plataformas de mídias digitais. MATRIZes, 15(1), 103-122. https://doi.org/10.11606/issn.1982-8160.v15i1p103-122. Acesso em: 14 de out. 2022.

DOURADO, Tatiana Maria Silva Galvão. **Fake news na eleição presidencial de 2018 no Brasil**. 308 f. Tese (Doutorado) – Programa de Pós-Graduação em Comunicação e Culturas Contemporâneas, Universidade Federal da Bahia, Salvador, 2020. Disponível em: https://repositorio.ufba.br/bitstream/ri/31967/1/Tese_Tatiana%20Dourado.pdf. Acesso em: 28 de set. 2022.

G1. Criminosos vendem dados pessoais pela internet utilizando cadastros de órgãos oficiais. 04 de dez. 2021. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2021/12/04/criminosos-vendem-dados-pessoais-pela-internet-utilizando-cadastros-de-orgaos-oficiais.ghtml. Acesso em: 21 de ago. 2022.

G1. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. 20 de mar. 2018. Tecnologia. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 09 de out. 2022.

ERENBERG, Jean Jacques. **Publicidade patológica na internet à luz da legislação brasileira**. São Paulo: Juarez de Oliveira, 2003. 128 p.

FACEBOOK, Política de privacidade do Facebook, 2023. Disponível em: https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0. Acesso em: 21 de dez. 2022.

FERNANDES, Dinalva. **Compra online é preferência de 74% dos consumidores brasileiros**. E-commerce Brasil, 15 de mar. 2019. Mercado. Disponível em: https://www.ecommercebrasil.com.br/noticias/compra-online-preferencia-de-consumidores-brasileiros. Acesso em: 19 de dez. 2022.

FERNANDES, Mirian. **Privacidade online**: desvende os riscos e saiba como se proteger. Starti, 2021. Disponível em: https://blog.starti.com.br/privacidade-na-internet/. Acesso em: 10 de out. 2022.

FERREIRA, Inaiara de Lima; Alcantara, Naiara Sandi de Almeida. **Eleições 2018**: A relação entre fake news e os candidatos Jair Bolsonaro e Fernando Haddad. CPOP, Paraná, 01 de mai. 2020. Comunicação Política. Disponível em: https://cpop.ufpr.br/eleicoes-2018-a-relacao-entre-fake-news-e-os-candidatos-jair-bolsonaro-e-fernando-haddad/. Acesso em: 24 de out. 2022.

FOLHA DE SÃO PAULO. Empresa que ajudou Trump roubou dados de 50 milhões de usuários do Facebook. São Paulo, 17 de mar. 2018. Mundo. Disponível em: https://www1.folha.uol.com.br/mundo/2018/03/empresa-que-ajudou-trump-roubou-dados-de-50-milhoes-de-usuarios-do-facebook.shtml. Acesso em: 12 de dez. 2022.

FOLHA DE SÃO PAULO. Empresas contrataram disparos pró-Bolsonaro no WhatsApp. Espanha, 18 de jun. 2019. Política. Disponível em: https://www1.folha.uol.com.br/poder/2019/06/empresas-contrataram-disparos-pro-bolsonaro-no-whatsapp-diz-espanhol.shtml. Acesso em: 09 de out. 2022.

FORBES. Robert Mercer, (s.d.). Disponível em: https://www.forbes.com/profile/robert-mercer/?sh=4cf3b05e7f9b. Acesso em: 26 de dez. 2022.

FORNASIER, Mateus de Oliveira; Knebel, Norberto Milton Paiva. **O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados**. Revista Direito e Práxis, vol. 12, núm. 2, p. 1002-1033, 2021. Programa de Pós-Graduação em Direito, Universidade

do Estado do Rio de Janeiro. Disponível em: DOI: https://doi.org/10.1590/2179-8966/2020/46944. Acesso em: 17 de dez. 2022.

FUCHS, Christian. **Karl Marx in the age of big data capitalism**. In: CHANDLER, D.; FUCHS, C. (orgs.). Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data, p. 53-71, Londres: University of Westminster Press, 2019. Disponível em: https://www.uwestminsterpress.co.uk/site/chapters/10.16997/book29.d/download/2301/. Acesso em: 13 de jan. 2023.

GAMA, Sophia. **Guerra de desinformação**: As fake news nas eleições de 2018. Câmara Municipal de Curitiba, 15 de jul. 2022. Disponível em: https://www.curitiba.pr.leg.br/informacao/noticias/guerra-de-desinformacao-as-fake-news-nas-eleicoes-de-2018. Acesso em: 28 de set. 2022.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. - São Paulo: Editora Atlas S.A., 2002. Bibliografia. ISBN 85-224-3169-82002. Disponível em: https://files.cercomp.ufg.br/weby/up/150/o/Anexo_C1_como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf. Acesso em: 27 de dez. 2022.

GODOY, Claudio Luiz Bueno de. **Privacidade**. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Civil. Rogério Donnini, Adriano Ferriani e Erik Gramstrup (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/474/edicao-1/privacidade. Acesso em: 13 de jan. 2023.

GOLDZWEIG, Rafael Schmuziger. Por que devemos nos preocupar com a influência das redes sociais nas eleições 2018? **El País**, 22 de set. 2018. Eleições. Disponível em: https://brasil.elpais.com/brasil/2018/09/21/opinion/1537557693_143615.html. Acesso em: 05 de set. 2022.

HENNEMANN, Gustavo Hermes. **Impactos da Lei Geral de Proteção de Dados nas eleições de 2020**. Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie, São Paulo, 2018, p. 7-27. Disponível em: https://dspace.mackenzie.br/bitstream/handle/10899/29756/GUSTAVO%20HERMES%20HENNEMANN.pdf?sequence=1&isAllowed=y. Acesso em: 27 de out. 2022.

IBM. Análise de Big Data. Estados Unidos. (s.d.). Disponível em: https://www.ibm.com/analytics/big-data-analytics. Acesso em: 20 de dez. 2022.

IGNACIO, Bruno. **Governo federal usa LGPD como pretexto para esconder dados, alertam especialistas**. Tecnoblog, 2021. Legislação. Disponível em: https://tecnoblog.net/especiais/governo-federal-esta-usando-lgpd-como-pretexto-para-esconder-dados/. Acesso em: 20 de ago. 2022.

INSTAGRAM, Política de privacidade do Instagram, 2023. Disponível em: https://privacycenter.instagram.com/policy. Acesso em: 21 de dez. 2022.

JANONE, Lucas. Compras online e consumo de podcast têm boom durante a pandemia, diz pesquisa. **CNN Brasil**, Rio de Janeiro, 21 jun. 2022. Tecnologia. Disponível em: https://www.cnnbrasil.com.br/business/compras-online-e-consumo-de-podcast-tem-boom-durante-a-pandemia-diz-pesquisa/. Acesso em: 20 de dez. 2022.

JARDELINO, Fábio; Cavalcanti, Davi Barboza; Toniol, Bianca Persici. «**A proliferação das fake news nas eleições brasileiras de 2018**», Comunicação Pública [Online], Vol.15, nº 28, 2020. Disponível em: https://doi.org/10.4000/cp.7438. Acesso em: 24 de out. 2022.

KOTLER, P.; Kartajaya, H.; Setiawan, I. **Marketing 4.0**. Edição traduzida. Rio de Janeiro: Sextante, 2017.

MAGENTA, Matheus; Gragnani, Juliana; Souza, Felipe. Eleições 2018: Como telefones de usuários do Facebook foram usados por campanhas em 'disparos em massa' no WhatsApp. **BBC News**, São Paulo, 20 de out. 2018. Eleições. Disponível em: https://www.bbc.com/portuguese/brasil-45910249. Acesso em: 02 de out. 2022.

MELLO, Patrícia Campos. Empresários bancam campanha contra o PT pelo WhatsApp. **Folha de S. Paulo**, v. 18, n. 10, p. 2018, 2018. Disponível em: https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml. Acesso em: 07 de dez. 2022.

MENDONÇA, Fernanda Graebin. **O direito à autodeterminação informativa**: A (des)necessidade de criação de um novo direito fundamental para a proteção de dados pessoais no Brasil. Mestranda em Direito pela Universidade Federal de Santa Maria (UFSM), 2014. Disponível em: https://online.unisc.br/acadnet/anais/index.php/sidspp/article/viewFile/11702/1571. Acesso em: 07 de jan. 2023.

MOROZOV, Evgeny. Big Tech: A ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018. [e-book].

OLSON, Parmy. **Cara a cara com o esquivo Alexander Nix da Cambridge Analytica**. Forbes, inovação, 2018. Disponível em: https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/?sh=710cfd6e535f. Acesso em: 26 de dez. 2022.

O DILEMA DAS REDES. Direção: Jeff Orlowski. Estados Unidos: Netflix, 2020. Documentário: O Dilema das Redes. Disponível em: https://www.netflix.com/br/title/81254224. Acesso em: 07 de dez. 2022.

PASQUINI, Patrícia. 90% dos eleitores de Bolsonaro acreditam em fake news. **Folha de São Paulo**, São Paulo, 02 de nov. 2018. Política. Disponível em: https://www1.folha.uol.com.br/poder/2018/11/90-dos-eleitores-de-bolsonaro-acreditaram-em-fake-news-diz-estudo.shtml. Acesso em: 10 de set. 2022.

PORTO, Cristiane de Magalhães; Oliveira, Kaio Eduardo de Jesus; Chagas, Alexandre Meneses. **EDUCIBER**: dilemas e práticas contemporâneas / organização [de] Cristiane Porto, Kaio Eduardo de Jesus Oliveira, Alexandre Meneses Chagas Aracaju: EDUNIT, 2019. Volume 2 - E-book 2º Edição, 244 p. ISBN - 978-85-68102-51-0. Disponível em: http://dx.doi.org/10.17564/2019.68102.51.0. Acesso em: 13 de jan. 2023.

PRIVACIDADE HACKEADA. Direção: Karim Amer; Jehane Noujaim. Produção: Karim Amer; Jehane Noujaim; Pedro Kos; Geralyn Dreufous; Judy Korin. Estados Unidos. Netflix. 2019. Disponível em: https://www.netflix.com/watch/80117542?trackId=13752289&tctx=0%2C0%2C6808c261-468b-49ae-82b6-75a4a4bdeca3-58929296%2C%2C. Acesso em: 06 de dez. 2022.

REIS FILHO, Cláudio Luiz Martins. **Redes sociais digitais e democracia**: Proteção de dados e a desinformação nas eleições de 2018. Dissertação (mestrado) - Universidade Federal Fluminense, Niterói, 2020, f. 160. Disponível em: doi: http://dx.doi.org/10.22409/PPGDC.2020.m.09612844712. https://app.uff.br/riuff/bitstream/handle/1/25398/REDES%20SOCIAIS%20DIGITAIS%20E%20DEMOCRACIA%20claudio%20luiz.pdf?sequence=1. Acesso em: 15 de dez. 2022.

RODRIGUES, Arthur; Mello, Patrícia Campos. Fraude com CPF viabilizou disparo de mensagens de WhatsApp na eleição. **Folha de São Paulo**, São Paulo, 2 dez. 2018. Disponível em:

https://www1.folha.uol.com.br/poder/2018/12/fraude-com-cpf-viabilizou-disparo-dem ensagens-de-whatsapp-na-eleicao.shtml Acesso em: 26 de dez. 2022.

RUEDIGER, Marco Aurélio. **Robôs, redes sociais e política no Brasil**: estudo sobre interferências ilegítimas no debate público na web, riscos à democracia e processo eleitoral de 2018. Rio de Janeiro: FGV, DAPP, 2017. ISBN: 978-85-68823-41-5. Disponível em: https://bibliotecadigital.fgv.br/dspace;/bitstream/handle/10438/18695/Robos-redes-s ociais-politica-fgv-dapp.pdf?sequence=1&isAllowed=y. Acesso em: 26 de out. 2022.

SALOMÃO, Luis Felipe. **Ação de investigação judicial eleitoral**. 2021, p. 1-58 Disponível em: https://static.poder360.com.br/2021/10/AIJE-1968-80-1.pdf. Acesso em: 07 de out. 2022.

SANTOS, Bruna et al. **Proteção de Dados Pessoais e Eleições** - Relatório de Recomendações para o quadro brasileiro atual, InternetLab - Law and Technology Research Center, São Paulo, 2021. Disponível em: https://www.econstor.eu/bitstream/10419/242251/1/Full-text-report-Santos-et-al-Prot ecao-de-dados.pdf. Acesso em: 19 de out. 2022.

SANTOS, Caroline Coradassi Almeida; Fernandes, Ana Claudia de Batista. **O enfrentamento das fake news no processo eleitoral a partir das leis de proteção de dados**. Universidade Positivo, 2021, p. 1-12. Disponível em: http://www.enajus.org.br/anais/assets/papers/2021/sessao-20/3-o-enfrentamento-d as-fake-news-no-processo-eleitoral-a-partir-das-leis-de-protecao-de-dados.pdf. Acesso em: 07 de dez. 2022.

SERPRO. **O que muda com a LGPD?** Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 10 de jan. 2023.

SOLOVE, Daniel J. **Digital person**: technology and privacy in the information age. New York: New York University Press, 2004.

SOLOVE, Daniel J. (2013). **Introdução**: Autogestão da privacidade e o dilema do consentimento, Harvard Law Review 126(7): 1880–1904.

SOUZA, João Carlos. **A Mediatização da Política na Era das Redes Sociais**. Análise Social, liv (3.º), 2019 (n.º 232), pp. 649-653 Disponível em: https://doi.org/10.31447/as00032573.2019232.15 issn online 2182-2999. Acesso em: 26 de out. 2022.

STOCHERO, Daniel. **Privacidade de dados no marketing**: Estudo de caso da Cambridge Analytica na eleição presidencial dos Estados Unidos em 2016. Caxias do Sul, 2020, UCS, p. 8-54. Disponível em: https://repositorio.ucs.br/xmlui/bitstream/handle/11338/8976/TCC%20Daniel%20Stochero%20de%20Aguiar.pdf?sequence=1&isAllowed=y. Acesso em: 01 de nov. 2022.

TEIXEIRA, Alvaro. **O que é ANPD?** [Autoridade Nacional de Proteção de Dados]. Tecnoblog, Brasil, 2020. Disponível em: https://tecnoblog.net/responde/o-que-e-anpd-autoridade-nacional-de-protecao-de-dados/. Acesso em: 03 de jan. 2022.

VAN DIJCK, J. (2013). **The culture of connectivity**: A critical history of social media. Oxford University Press.

Vazamento e venda de dados pessoais. **E.Veritas**, (s.d). Disponível em: https://www.emailveritas.com/pt/blog/vazamento-e-venda-de-dados-pessoais. Acesso em: 17 de ago. 2022.

WHATSAPP, Política de privacidade do Whatsapp, 2023. Disponível em: https://www.whatsapp.com/legal/privacy-policy. Acesso em: 21 de dez. 2022.

ZUBOFF, Shoshana, **Big Other**: Surveillance Capitalism and the Prospects of an Information Civilization (April 4, 2015). Journal of Information Technology (2015) 30, 75–89. Disponível em: doi:10.1057/jit.2015.5. Acesso em: 14 de out. 2022.

90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa. **Gov**, 19 de set. 2022. Conectividade. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa. Acesso em: 19 de dez. 2022.