

Capitalismo de vigilância e modulação do comportamento humano: o ambiente digital como espaço favorável à manipulação do eleitor?

Recebido: 10 de agosto de 2023 • Aprovado: 9 de novembro de 2024
<https://doi.org/10.22395/ojum.a4542>

José Adércio Leite Sampaio

Pontifícia Universidade Católica de Minas Gerais;
Centro Universitário Dom Helder Câmara, Belo Horizonte, Brasil
joseadercio.contato@gmail.com
<https://orcid.org/0000-0002-9452-4811>

Ana Carolina Marques Tavares Costa

Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, Brasil
anacarolinamtavares@gmail.com
<https://orcid.org/0000-0002-7809-3011>

Resumo

Este artigo busca compreender como os rastros digitais dos usuários do Facebook foram estrategicamente utilizados pela Cambridge Analytica para a modulação da opinião pública na eleição presidencial dos Estados Unidos em 2016. Adota como substrato teórico o capitalismo de vigilância de Shoshana Zuboff, e utiliza o método hipotético-dedutivo, fundado em revisão bibliográfica e estudo de caso, a pesquisa demonstra a influência da inteligência artificial nos processos políticos de uma sociedade hiperconectada. A investigação revela que o perfilamento psicográfico e o microdirecionamento de conteúdo possibilitaram formas sofisticadas de manipulação eleitoral, baseadas na ativação emocional e no controle do comportamento individual à revelia do eleitor. Conclui-se que a ausência de transparência e a opacidade algorítmica representam grave ameaça à autodeterminação informacional e à integridade democrática, demandando formas robustas de regulação jurídica e tecnológica.

Palavras-chave: capitalismo de vigilância; proteção de dados pessoais; psicomетria; eleições digitais; manipulação política; liberdade informacional.

Surveillance capitalism and modulation of human behavior: a digital environment as an enabling space for voter manipulation?

Abstract

This article seeks to understand how Cambridge Analytica strategically used Facebook users' digital footprints to modulate public opinion during the 2016 US presidential election. It adopts Shoshana Zuboff's concept of surveillance capitalism as a theoretical basis, and employs the hypothetico-deductive method, grounded in a literature review and case studies. Research demonstrates Artificial Intelligence's influence on a hyperconnected society's political processes. It reveals that psychographic profiling and content micro-segmentation enabled sophisticated forms of electoral manipulation, based on emotional activation and control of individual behavior behind voters' backs. The study concluded that a lack of transparency and algorithmic opacity represents a serious threat to informational self-determination and democratic integrity, which requires strong forms of legal technological regulation.

Keywords: surveillance capitalism; personal data protection; psychometrics; digital elections; political manipulation; informational freedom.

Capitalismo de vigilancia y modulación del comportamiento humano: ¿el entorno digital como espacio propicio para la manipulación del elector?

Resumen

Este artículo busca comprender cómo las huellas digitales de los usuarios de Facebook fueron estratégicamente utilizadas por Cambridge Analytica para modular la opinión pública durante la elección presidencial de Estados Unidos en 2016. Adopta como base teórica el concepto de capitalismo de vigilancia de Shoshana Zuboff, y emplea el método hipotético-deductivo, fundamentado en revisión bibliográfica y estudio de caso. La investigación demuestra la influencia de la Inteligencia Artificial en los procesos políticos de una sociedad hiperconectada. Revela que el perfilamiento psicográfico y la microsegmentación de contenidos posibilitaron formas sofisticadas de manipulación electoral, basadas en la activación emocional y en el control del comportamiento individual a espaldas del elector. Se concluye que la falta de transparencia y la opacidad algorítmica representan una grave amenaza para la autodeterminación informativa y la integridad democrática, lo que exige formas sólidas de regulación jurídica y tecnológica.

Palabras clave: capitalismo de vigilancia; protección de datos personales; psicometría; elecciones digitales; manipulación política; libertad informativa.

Introdução

Este trabalho resulta das investigações contínuas sobre a fragilização da democracia e do Estado Democrático de Direito diante dos recentes avanços tecnológicos, temática debatida pelos autores em Grupo de Pesquisa vinculado ao Programa de Pós-graduação da PUC MINAS, denominado "Constitucionalismo e Direitos na Era Digital – Algotr.IA". O tema também é objeto de pesquisa em andamento da segunda autora, orientada pelo primeiro autor, intitulada "O capitalismo de vigilância e a modulação do comportamento humano: os espaços digitais como realidades de (de) formação da vontade política", e financiada pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (Código de Financiamento 001).

Todas as positivas promessas que nortearam a Revolução Tecnológica, como a evolução das capacidades humanas e a democratização do conhecimento, acabaram por adormecer as incertezas e as vulnerabilidades da sociedade digital. Se antes, os centros de poder e autoridade concentravam-se em espaços públicos, geralmente nos locais de trabalho, atualmente, esses núcleos foram diluídos e entranhados em espaços privados, no âmbito da particularidade dos cidadãos. O espaço da individualidade foi capturado por projetos obscuros de manipulação subjetiva.

A pesquisa propõe como questão-problema: "de que forma a tecnologia teria influenciado as eleições ocorridas nos Estados Unidos em 2016?". Para tanto, buscar-se-á compreender como o uso indevido dos dados pessoais de milhões de usuários do Facebook contribuiu, à época, para a manipulação de votos. Adotou-se o raciocínio hipotético-dedutivo, fundado em estudo de caso e levantamento bibliográfico, com base em livros, artigos científicos, trabalhos acadêmicos, notícias e reportagens relacionadas à discussão.

A primeira parte da pesquisa evidenciará como a fórmula de negócios introduzida pelo capitalismo de vigilância remodelou as relações políticas e econômicas, agora fundadas na utilização dos dados como forma de predição comportamental. A utilização desenfreada das redes sociais como principal fonte informacional despertou dilemas cujos impactos não são, ainda, totalmente compreendidos.

As vantagens comerciais obtidas com os rastros digitais apontam a existência de um regime econômico baseado na vigilância, isto é, na coleta, no armazenamento, na mineração, na filtragem e na disseminação de dados pessoais. Sobre a política capitalista de exploração e monetização lucrativa dos dados, Shoshana Zuboff (2021) definiu o capitalismo de vigilância para explicar o *big data* como o componente fundamental de uma lógica de acumulação profundamente intencional. Nessa nova forma de organização do mercado, o valor econômico do dado passa a existir pela possibilidade de alteração das relações sociais, a partir da previsão e da modificação

comportamental em prol de interesses escusos. As consequências para o âmbito político são alarmantes e nada animadoras.

Com foco no escândalo Facebook-Cambridge Analytica, a segunda parte do artigo analisará as técnicas de marketing digital atualmente empregadas para conhecer, previamente (e precisamente), o perfil dos eleitores, e, assim, tornar possível a seleção da propaganda ideologicamente atrativa e persuasiva a cada um deles.

No ano de 2018, veio à tona o vazamento de dados de aproximadamente cinquenta milhões de usuários do Facebook para a Cambridge Analytica, empresa que fazia a modelagem psicométrica para campanhas. Durante a corrida eleitoral americana em 2016, foi feita a segmentação dos eleitores para o disparo de propagandas customizadas aptas a resgatar a atenção e provocar o seu convencimento. A artimanha política também contou com a disseminação de *fake news*. Os traços psicológicos trouxeram as revelações necessárias para a polarização do discurso político – com a exploração dos medos e das vulnerabilidades de cada eleitor, teorias da conspiração ganharam força.

As estratégias comunicativas da Cambridge Analytica de microdirecionamento de conteúdo, com base na curadoria da relevância, e circulação de notícias falsas impactaram, significativamente, os rumos da eleição nos Estados Unidos a favor do candidato Donald Trump. O contexto merece atenção pela facilidade de manipulação do eleitor, cuja vontade política passou a ser moldada por fatores externos, desconhecidos e incontroláveis. Desvendar as técnicas é o caminho inicial para a proposição de formas de regulação das situações de uso indevido dos dados pessoais.

1. A sociedade digital e o capitalismo de vigilância

1.1 Os fundamentos da nova ordem global

O termo capitalismo de vigilância (Zuboff, 2021) amolda-se, em essência, à nova lógica consumerista influenciada pelas facilidades tecnológicas, que abraçaram as predições comportamentais como estratégias eficazes de venda. A disponibilização gratuita da experiência humana transformou a extração de dados a matéria prima essencial e altamente atrativa para a circulação de bens e serviços. O consumo personalizado, fundado na imediata satisfação de interesses e vontades individuais, origina-se do encontro, nada fortuito, entre publicidade e público-alvo. Trata-se de lógica econômica de coleta e acúmulo de dados sem precedentes.

Nos tempos em que as interações e as experiências humanas são edificadas e mantidas nos espaços virtuais, “nunca foi possível reunir tanta informação das pessoas (...) nunca se foi tanto vigiado” (Sampaio, 2022). Os rastros digitais empoderaram o governo e as empresas do Vale do Silício, que, fazendo das vidas humanas verdadeiros livros abertos, criam disparidades ao proteger suas ações de observação por

acordos confidenciais. Sem revelar os mecanismos e interesses comerciais por trás da coleta de dados, esse novo mercado sustenta-se em práticas negociais dotadas de opacidade, como fenômeno semelhante à operação de uma caixa preta (Pasquale, 2015).

A vigilância não é exclusiva das sociedades contemporâneas, mas foi, certamente, aprofundada pela tecnologia, dada a expansão e potência inimagináveis dos bancos de dados. A complexidade do processo de influência comportamental relembra os alertas de Foucault sobre a assimetria de olhares do panóptico de Jeremy Bentham. No cenário de hipervigilância ou data vigilância, com a comoditização dos dados pessoais, estruturou-se uma forma assimétrica de distribuição de poder. Somente alguns (poucos) monopolizam as ferramentas de coleta, agregação e inserção do *big data* em algoritmos aptos a torná-lo inteligível ou a ele atribuir sentido. A previsão do comportamento humano ocorre "sob a ordem de grandeza do *big data* e da velocidade da gestão dos algoritmos" quando "os difusos processos de monitoramento digital buscam conhecer, classificar e reconhecer padrões de ação individuais" (Bentes, 2021, p. 23).

O termo *big data*, central no capitalismo de vigilância, refere-se ao grande volume de dados —organizados ou não—, utilizado para orientar decisões. Ou seja, *big data* compõe o conjunto de ferramentas destinadas à análise de um grande volume de dados essenciais à geração de resultados importantes. Esses dados são coletados e analisados a partir da teoria dos 3Vs (volume, velocidade e variedade), que demonstra que, (i) é capturado, inicialmente, um grande volume de dados oriundos de fontes diversas; (ii) os dados são transmitidos e tratados com rapidez; e, ao fim, (iii) são tratados para que sejam transformados em informações relevantes, que tenham utilidade para a empresa. A ação do *big data*, portanto, é traduzida ao método de análise de dados, mapeamento e monitoramento de padrão comportamental, para a tomada de decisão (Santos & Inácio, 2018) (Simão Filho & Schwartz, 2015).

A acuidade preditiva dos algoritmos é alimentada pela mobilização e direcionamento da atenção dos usuários. Daí, a perenidade da conexão e a ubiquidade da internet. Quanto maior o tempo de navegação, mais dados são armazenados – a agregação de valor à mercantilização de dados é consequência da eterna, e aparentemente consentida, alimentação do sistema de predição comportamental. A atenção dos cidadãos, enganchados e engajados por meio de estratégias persuasivas de captura, torna-se um hábito ou um comportamento automático necessário à "economia que se nutre dessa necessidade existencial de ver e ser visto" (Bentes, 2021, p. 31).

O valor dos rastros digitais é mensurado por sua capacidade de se converterem ações humanas, tornando possível o direcionamento de propagandas e conteúdo. Os lucros desse novo capitalismo são resultado da exitosa combinação entre dois elementos fundamentais: vigilância unilateral e modificação do comportamento. O capitalismo de dados seria adequado para expressar a transição de um modelo de

comércio eletrônico, baseado na venda de mercadorias online, para um modelo de publicidade baseado na venda de audiências, ou melhor, na monetização de predições (West, 2019).

Nessa nova ordem econômica do século XXI, constituem, como pilares básicos, a assimetria de poder e a assimetria informacional. Dos usuários, sabe-se tudo; das operações e mecanismos utilizados para tamanha invasão, pouco ou nada é conhecido. A extração unilateral, gratuita e frequentemente inconsciente da experiência humana estrutura uma nova ordem social, baseada na destituição da soberania dos indivíduos como forma de condução das ações humanas e geração de lucros às grandes empresas (Zuboff, 2021).

A vigilância, como instrumento de poder, envolve a observação de indivíduos e populações, a produção de conhecimento sobre os vigiados, e, como consequência, a intervenção (a nível social, manifestada na indução ações humanas) (Bentes, 2021). Uma técnica que, antes, restringia-se ao aparato estatal securitário, foi, então, apropriada pelo mercado, que se aproveita do "volume de dados coligidos e tratados (...) continuamente e, em altíssima velocidade (...) em que se negocia uma gigantesca base de dados coligida da internet e de fontes secundárias, com ou sem o consentimento dos usuários" (Sampaio & Assis, 2021).

O capitalismo de vigilância apoia-se em discursos promissores para mascarar os controles sociais e políticos. As ameaças são negligenciadas em nome da liberdade de expressão, da transparência e da ampliação do poder de consumo pelo universo personalizado. O cego culto ao novo facilita a distribuição desigual de poder que fundamenta o atual momento (West, 2019).

1.2 Compreendendo a vigilância

Nos estágios iniciais do Google, quando a empresa ainda se consolidava como motor de busca, havia a percepção de um certo equilíbrio de poder. Todo o subproduto comportamental decorrente da busca do Google, também denominado *data exhaust* – por exemplo, o padrão de busca, a ortografia, o tempo de leitura da página, os cliques, o tempo de visualização – era utilizado para o aprimoramento o próprio produto ou serviço.

Havia um ciclo de revestimento do valor comportamental, na medida em que os dados adicionais produzidos pelos usuários eram exauridos no aperfeiçoamento do próprio sistema de busca e na melhoria da experiência. O que não integra o ciclo de reinvestimento é denominado superávit comportamental, este matéria-prima do capitalismo de vigilância a ser convertida em produtos de predição. Assim, ao invés de trabalho, a nova ordem econômica se apropria da experiência humana. Os produtos de predição são comercializados/negociados em mercados de comportamento humano que

se formam por empresas que dele dependem para alavancar suas vendas de produtos e serviços (Zuboff, 2021).

Sobre a vigilância como dispositivo das sociedades contemporâneas, Bruno (2013), sem pretender esgotar a complexidade que envolve o tema, enumera algumas de suas principais características. Em primeiro lugar, trata-se de uma vigilância cada vez mais onipresente, como uma verdadeira extensão das práticas cotidianas. Essa vigilância é descentralizada em variados dispositivos, serviços e ambientes, que operam de formas distintas e captam os dados pessoais para finalidades variadas. Os objetos e alvos de vigilância não são anteriormente definidos (todos são vigias e vigiados em potencial). Além disso, a vigilância não assume, necessariamente, a função principal de alguns dispositivos e serviços; pode ser resultado colateral, como os aplicativos voltados à sociabilidade e ao entretenimento, como Instagram.

Zuboff acrescenta que a vigilância é resultado de um trabalho híbrido, de uma articulação dos elementos humanos e não humanos, com o encurtamento de distâncias, custos e tempo de resposta. A questão mostra-se sensível quando as atuais práticas de vigilância "não estão restritas aos circuitos de controle, segurança e normalização, mas estão intensamente presentes em circuitos de (...) prazer" (Zuboff, 2021, p. 34), instigando, assim, a diversão e o desejo por meio de modelos colaborativos que convivem, simultaneamente, com os hierarquizados e centralizados típicos da sociedade moderna.

O discurso que enaltece a tecnologia, sustentado pela aposta de universalização do conhecimento, precisa ser contestado (Pariser, 2012). Não se nega o comodismo em torno da possibilidade do encontro do produto "correto" à busca pessoal, dispensando-se esforços adicionais. Sob essa crença inicial, contudo, eventuais ilegalidades ou abusos praticados pelas empresas para o mapeamento do perfil e dos interesses dos titulares são deliberadamente ignorados. A hipervigilância parece se normalizar. Afinal, a falta de transparência passa a ser responsabilidade do internauta, a quem compete a escolha (ou o ônus) de recusar totalmente o serviço ou concordar com os termos de uso autorizativos da coleta de dados.

A internet parece, então, apropriar-se de algo essencial: as subjetividades que diferenciam e autodeterminam cada vida humana. A ideia de que "se você tem algo a esconder, não deveria estar usando a internet" naturaliza a exposição virtual, como se a experiência humana só fosse válida se irrestritamente conhecida por todos. O poder das Big Techs (Google, Apple, Meta, Amazon e Microsoft) não decorre de conquistas envolvendo corpos ou inimigos, mas de um processo muito sutil, que conta com a concessão irrefletida por parte da própria sociedade (Intrínseca, 2021). É ilusório e ingênuo, nesse novo cenário, acreditar em uma efetiva liberdade de escolha, quando, na realidade, as regras do mercado são pretensiosamente articuladas para moldar o padrão de consumo (Sunstein, 2007).

O capitalismo de vigilância, porém, não se limita às predições econômicas.

Apesar de todo o conforto cognitivo, os dados contribuem, hoje, de forma valiosa, para a satisfação de um apetite insaciável das agências de tecnologia em vigiar e modelar a comunicação global. A lógica de concentração de conhecimento beneficia intenções políticas, a exemplo do que fora feito pela Cambridge Analytica nas eleições de 2016 nos Estados Unidos, evidenciando "o perigo do mau uso das novas tecnologias para a democracia (...) no ponto em que servem para a debilitação da liberdade e do diálogo que permite a formação do pensamento livre (...)" (Bolzan de Moraes & Lobo, 2020).

2. O escândalo Facebook-Cambridge Analytica

A Cambridge Analytica, subsidiária da empresa britânica de inteligência privada SCL Group, atuava para além de uma simples agência de publicidade, destinava-se a realizar comunicações psicologicamente assertivas (BBC News Brazil, 2018) por meio de serviços de análise do eleitorado a partir de dados obtidos na internet.

As atividades avançadas de consultoria política ganharam a atenção global quando foram revelados, em 2018, os escândalos de privacidade e manipulação dos eleitores na campanha presidencial de 2016 nos Estados Unidos e no referendo do Brexit.

O documentário *Privacidade Hackeada* (2019) revelou os relatos de dois ex-funcionários da empresa, Brittany Kaiser e Cristopher Wylle, responsáveis por denunciar as práticas antiéticas e abusivas da empresa, consistentes, basicamente, no uso indevido de dados de milhões de usuários do Facebook sem o prévio consentimento (Amer & Noujaim, 2019). Os trabalhos empregavam a metodologia psicográfica ou o *microtargeting comportamental*, cujo preceito básico se resumiria no seguinte conceito "para fazer as pessoas agirem, você devia criar as condições sob as quais será maior a probabilidade de elas fazerem o que você quer que façam". A chave do êxito das campanhas políticas conduzidas pela empresa residia, portanto, na própria audiência, ou seja, na capacidade de influenciar e modular o comportamento dos eleitores (Kaiser, 2020, p. 54).

Para alcançar os resultados do marketing político proposto, a empresa utilizou dados dos usuários do Facebook obtidos a partir de diferentes testes de personalidade, entre eles o "*This is your digital life*" – baixado por cerca de 270.000 (duzentos e setenta mil) pessoas, que reuniu informações não só daqueles que o instalaram, mas dos respectivos amigos, totalizando dados de aproximadamente 87 (oitenta e sete) milhões de usuários (Revell, 2018).

A combinação da precisão e da velocidade das tecnologias de informação e do modelo Big Five Personality Traits (ou o modelo dos cinco fatores globais de personalidade) foi decisiva para a descoberta das campanhas eleitorais mais personalizadas da história. A empresa teve forte influência na corrida eleitoral de 2016, quando

auxiliou o candidato Donald Trump (Halpern, 2018). Os testes de personalidade aplicados aos eleitores forneciam predições políticas surpreendentes, de resultados mais exatos comparados aos testes humanos (Hinds & Joinson, 2019).

Os eleitores, especialmente os indecisos, foram, à época, classificados pelos psicólogos da empresa conforme o nível de (i) abertura a novas experiências, (ii) conscienciosidade (ou cuidado e responsabilidade), (iii) extroversão, (iv) neuroticismo (ou instabilidade emocional) e (v) amabilidade ou agradabilidade.

Definidos os perfis psicológicos a partir dos dados coletados pelo Facebook (aproximadamente 50 milhões de usuários tiveram o seu nome, nascimento, local de residência, preferências políticas e outras informações vazadas), foram criados os perfis psicológicos necessários ao disparo direcionado de anúncios políticos (Bakir, 2020). A mobilização do medo, das vulnerabilidades e das emoções humanas era o segredo da efetividade da curadoria informacional (Silva, 2022). A lógica do capitalismo de vigilância viabilizou, assim, a entrega da propaganda política ajustada ao perfil de cada internauta, de modo a influenciar o seu comportamento como eleitor.

A título de exemplo, a depender do perfil psicológico, diferentes anúncios eram transmitidos sobre uma mesma bandeira defendida por Donald Trump durante a sua campanha. Em relação ao porte de arma, as pessoas mais propensas a novas experiências receberam anúncios sugerindo a importância das armas para a defesa da liberdade; pessoas com maior nível de cuidado foram submetidas a propagandas que alertavam a importância de proteção à família e ao futuro (Pato, 2018). O perfilamento psicográfico permitiu a identificação da melhor publicidade para cada visão particular de mundo, objetivando o voto do eleitor no candidato apoiado pela empresa (Furbino & Bocchino, 2023).

A Cambridge Analytica também recorreu à desinformação em larga escala. Explorando os preconceitos e as inclinações pessoais, a empresa conseguiu rastrear os indivíduos mais suscetíveis às *fake news* e ao consequente compartilhamento, de modo a maximizar a rapidez de disseminação.

Teorias da conspiração incitavam o medo e ganhavam notória repercussão, como ocorreu com a ligação de Hillary Clinton à suposta rede de prostituição e exploração sexual de crianças na pizzeria Comet Ping Pong na cidade de Washington (Canossa, 2018). A vantagem de Trump também foi resultado da publicação pelo site *Political Insider* de uma notícia que anunciava a confirmação pelo *WikiLeaks* do envolvimento de Hilary Clinton com o fornecimento de armas para grupos terroristas como os jihadistas islâmicos (Silverman, 2016). Seguidores de Trump e sites de extrema direita utilizaram da linguagem sensacionalista e do efeito cascata para reforçar opiniões que maculavam a imagem da candidata.

No contexto de personalização e de disparo de *fake news*, diferentes opiniões políticas foram radicalizadas “simplesmente porque não era possível que duas pessoas discutissem calmamente os pontos positivos e negativos”, afinal, a Cambridge Analytica encarregou-se de mostrar “conteúdos dramaticamente diferentes para pessoas diferentes, destruindo a experiência comum” (Véliz, 2021, p. 64). O conteúdo cada vez mais individualizado reforçou crenças e visões pré-existentes sobre determinada matéria.

As técnicas da Cambridge Analytica obstruíram e censuraram qualquer diálogo entre opiniões divergentes, abafando a diversidade e o pluralismo tão essenciais à democracia, em um processo de desativação da esfera pública (Magrani, 2014).

3 A manipulação eleitoral

Sobre a distinção entre a manipulação do mercado (ou manipulação estática da TV e das revistas) e a manipulação online, Calo (2014) explica: enquanto a primeira viola a privacidade dos consumidores para que consumam um produto ou uma marca que não precisariam ou que não pensariam – o que representaria, ao fim, um custo marginal –, a manipulação online é escalável e atinge todos os aspectos da existência humana, não só o poder de consumo. A manipulação de mercado era relativamente estática, limitada por barreiras físicas e pela falta informações detalhadas sobre a personalidade dos consumidores, a depender da exposição por eles concedida. A manipulação virtual explora as fragilidades pessoais.

A Cambridge Analytica adotou uma técnica psicológica sutil de motivação comportamental, voltada a provocar determinada conduta por meio da recomendação de conteúdo e utilização do apelo sensacionalista para a captura de atenção. Nesse cenário, a liberdade de escolha estaria sendo limitada pelo direcionamento de notícias que interferem na formação da identidade humana (Bani, 2021).

Várias campanhas presidenciais dos Estados Unidos usaram de manipulação simbólica do eleitorado. A questão é que, com a tecnologia, a estratégia ficou mais fácil e invasiva, apresentando-se, portanto, mais perigosa para a democracia e para a autodeterminação informacional (Zuboff, 2021). A manipulação online ocorre da influência intencional sobre alguém que a desconhece, fazendo uso de suas fraquezas a partir dos dados pessoais.

O microdirecionamento político feito pela Cambridge Analytica modulou as emoções humanas como forma de influência na decisão política. O objetivo era expor os usuários a anúncios políticos baseados na Teoria da Inteligência Afetiva, sob a qual o medo e o entusiasmo têm papel central. A depender do traço de personalidade, cada anúncio despertava um tipo de reação emocional, exatamente como pretendia a empresa. Quando um anúncio político afetivo (positivo ou negativo) corresponde ao perfil psicológico do receptor, ocorrerá um aumento na mensagem elaborada, que,

por sua vez, tem um impacto positivo na persuasão política (ou seja, na atitude e na intenção de voto) (Zarouali et al, 2022). O ambiente de conturbação e enviesamento é propício para as notícias falsas.

Percebendo que a personalidade dita o comportamento e o comportamento dita a ação (Amer & Noujaim, 2019), a Cambridge Analytica inovou na forma de persuasão em massa, que faz uso de características psicológicas para a definição da vontade em larga escala. A indução do comportamento em benefício de determinado grupo político ou candidato revela a face perversa do mau uso das tecnologias (Matz et. al, 2017), ao furtar do eleitor a oportunidade de uma escolha independente e conscientizada. A escolha não recai sobre o que é melhor para o eleitor ou para o bem comum; é sobre o candidato detentor do poder de vigilância exercido pelos aprimorados algoritmos preditivos da Cambridge Analytica.

Vendeu-se, para a campanha de Trump, a predição de comportamento (ou seja, o produto do capitalismo de vigilância ou a análise obtida dos dados). A técnica de mapeamento do perfil psicográfico ficou também sendo conhecida como "software de leitura de mente" e "máquina de Inteligência Artificial de propaganda armada".

A ilegalidade das condutas da empresa decorre da própria excepcionalidade técnica: (i) a autonomia de escolha do eleitor é afetada quando o seu comportamento é distorcido ou contaminado por propagandas microdirecionadas em relação às quais não houve consentimento; (ii) a escalabilidade da manipulação online representa ameaça à democracia (há manipulação da intenção de voto de um grupo significativo); (iii) a manipulação digital é personalizada e sistematizada (os algoritmos possuem um nível de precisão científica jamais alcançado pela mente humana); (iv) facilita-se o fenômeno do "digital gerrymandering", a significar o efeito cascata que decorreu do mecanismo desenvolvido pelo Facebook de incentivos de votos a partir da transmissão de mensagens de amigos que votaram (Kilovaty, 2019); (v) as interações em mídias sociais são capazes de orientar os estados emocionais dos usuários, definindo sentimentos como ansiedade, raiva, racismo, sexismo, e culpa; (vi) o microdirecionamento é mais agressivo e ilimitado tendo em vista o rico volume de dados produzidos na era digital (Kilovaty, 2019).

Com o escândalo Facebook-Cambridge Analytica, compreende-se quão inconsciente, intrusiva e silenciosa é a manipulação do eleitor. O objetivo, aqui, foi evidenciar, levantando as problemáticas em torno da matéria, como os novos tempos demandam novas respostas. Quando os mecanismos tradicionais legais de proteção parecem incapazes de enfrentar a alta sofisticação e a engenhosidade das empresas de tecnologia (Kilovaty, 2019), é necessário o desenvolvimento de um olhar crítico sobre as técnicas por elas atualmente empregadas. Conhecer o método é o ponto de partida para desvelar a obscuridade legitimadora dessa irracional influência.

Conclusões

O capitalismo de vigilância anunciou o grande potencial preditivo dos rastros digitais. Constatou-se que os algoritmos depreenderiam, de forma eficaz, as características psicológicas e as vulnerabilidades necessárias ao direcionamento de conteúdo adaptado às preferências subjetivas. O entusiasmo em torno dos serviços gratuitos da internet passou a ser questionado diante da máxima: 'se você não está pagando por um produto, então você é o produto'. Afinal, na economia de dados, o produto comercializado não mais diz respeito a um indivíduo específico, mas aos padrões comportamentais extraídos de seus dados pessoais.

O fenômeno do *big data* revela a importância central dos algoritmos, seja pelo processo de captura de dados em larga escala, seja pela capacidade de cruzar e analisar informações para a extração de previsões. O atual modelo de negócios sustenta-se na ideia de personalização do serviço para a melhoria da experiência do usuário, que, por consequência lógica, passa mais tempo no ambiente virtual gerando mais dados. Inaugura-se, assim, uma ordem econômica de influência nos processos de tomada de decisão.

As campanhas políticas descobriram no mercado de predição comportamental, até então utilizado como estratégia de incentivo ao consumo, uma maneira de (de) formar a vontade do eleitor. Agora, os imensos bancos de dados não se destinam apenas aos ganhos financeiros (como têm sido há aproximadamente duas décadas com o capitalismo de vigilância), mas abrangem a produção de perfis políticos.

A otimização do impacto emocional de uma mensagem política, de acordo com a segmentação do público-alvo, foi a principal estratégia utilizada pela Cambridge Analytica nas eleições presidenciais ocorridas em 2016 nos Estados Unidos.

Lançando mão da curadoria informacional resultante de operações psicológicas, a empresa desenvolveu uma técnica única de indução de comportamentos e escolhas eleitorais. O perfilamento psicográfico, com base na teoria dos Cinco Grandes Traços de Personalidade, propiciou a pretendida persuasão dos eleitores. Com base nas fraquezas pessoais, informações e desinformações impactaram as atitudes políticas e intenções de voto. O processo ficou conhecido como *microtargeting* político.

A manipulação contemporânea é sem precedentes: dispensa consentimento prévio e opera em escala global. A sistematização é o fundamento do efeito cascata e da polarização dos discursos políticos, facilitando a propagação de *fake news*.

O microdirecionamento e a desinformação constituem formas sofisticadas de manipulação da opinião pública pela mobilização dos medos e pela ingerência intencional no processo de formação da vontade individual, sem que isso seja revelado ao eleitor. Nesse cenário, a tendência de personalização das campanhas eleitorais representa uma ameaça real à democracia, sugerindo a necessidade de formas legais de proteção

cibernética e de preservação da autodeterminação informacional dos eleitores. É preciso pensar em regulações eficazes à delimitação dos riscos da segmentação social.

Referências

- Amer, K. & Noujaim, J. (2019). *The Great Hack* [documentário]. Netflix.
- Bakir, V. (2020). Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting. *Frontiers in Communication*, 5, 1-16. <https://doi.org/10.3389/fcomm.2020.00067>
- Bani, Z. (2021). *The Threat of Filter Bubbles on Democratic Values* [tese de bacharelado, Utrecht University]. Repositório. <https://studenttheses.uu.nl/handle/20.500.12932/40275>
- BBC News Brasil. (2018, 20 de março). *Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades*. <https://www.bbc.com/portuguese/internacional-43461751>
- Bentes, A. C. F. (2021). *Quase um tique: economia da atenção, vigilância e espetáculo em uma rede social*. Editora UFRJ. <https://pantheon.ufrj.br/handle/11422/16510>
- Bolzan de Moraes, J. L. & Lobo, E. (2020). A democracia corrompida pela surveillance ou uma fake democracia distópica. In: J. L. Bolzan de Moraes (org.), *A Democracia Sequestrada* (pp. 27-42). Tirant lo Blanch.
- Bruno, F. (2013). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Editora Sulina.
- Calo, R. (2014). Digital Market Manipulation. *George Washington Law Review*, 82(4), 995-1051. <https://doi.org/10.2139/ssrn.2309703>
- Canossa, C. (2018, 13 de abril). *Pizzagate: o escândalo de fake news que abalou a campanha de Hillary*. Super INTERESSANTE. <https://super.abril.com.br/mundo-estranho/pizzagate-o-escandalo-de-fake-news-que-abalou-a-campanha-de-hillary>
- Furbino, M. & Bocchino, L. A. (2023). Democracia e legitimidade: Do processo eleitoral: novos desafios frente a atuação das fake news. In: J. A. L. Sampaio (org.), M. Furbino, L. A. Bocchino & M. J. N. Lima (orgs.), *A inteligência artificial: a (des)serviço do estado de direito* (pp. 257-277). CAPES; PUC Minas; Editora RTM. [https://www.pucminas.br/pos/direito/Documentos%20Gerais/Ebook%20-%20A%20INTELIG%20C%80%20ANCIA%20ARTIFICIAL%20A%20\(DE\)SERVI%20C%80%20DO%20ESTADO%20DE%20DIREITO.pdf](https://www.pucminas.br/pos/direito/Documentos%20Gerais/Ebook%20-%20A%20INTELIG%20C%80%20ANCIA%20ARTIFICIAL%20A%20(DE)SERVI%20C%80%20DO%20ESTADO%20DE%20DIREITO.pdf)
- Halpern, S. (2018, 21 de março). *Cambridge Analytica, Facebook, and the Revelations of Open Secrets*. The New Yorker. <https://www.newyorker.com/news/news-desk/cambridge-analytica-facebook-and-the-revelations-of-open-secrets>
- Hinds, J. & Joinson, A. (2019). Human and Computer Personality Prediction From Digital Footprints. *Current Directions in Psychological Science*, 28(2), 204-211. <https://doi.org/10.1177/0963721419827849>
- Intrínseca (2021, 9 de dezembro). *Capitalismo de Vigilância e Democracia, com Shoshana Zuboff* [vídeo]. Youtube. <https://www.youtube.com/watch?v=fG2tB6tdmpg>
- Kaiser, B. (2019). *Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque*. HaperCollins.
- Kilovaty, I. (2019). Legally Cognizable Manipulation. *Berkeley Technology Journal*, 34(2), 449-502. <https://doi.org/10.2139/ssrn.3224952>

- Magrani, E. (2014). *Democracia conectada: a internet como ferramenta de engajamento político-democrático*. Juruá Editora.
- Matz, S. C., Kosinski, M., Nave, G. & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the United States of America*, 114(48), 12714-12719. <https://doi.org/10.1073/pnas.1710966114>
- Pariser, E. (2012). *O filtro invisível: o que a internet está escondendo de você* (D. Alfaro, trad.). Zahar.
- Pasquale, F. (2015). *The black box society. The secret algorithms that control money and information*. Harvard University Press.
- Pato, G. (2018, 5 de abril). O ESCÂNDALO DO FACEBOOK: Cambridge Analytica, Privacidade e mais... - Futuro Agora [vídeo]. YouTube. <https://www.youtube.com/watch?v=nXvm4JZ6WSU&t=468s>
- Revell, T. (2018, 16 de abril). How Facebook let a friend pass my data to Cambridge Analytica. NewScientist. <https://www.newscientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica>
- Sampaio, J. A. L. (2022). Datificação e vigilância: o judiciário é guardião dos direitos fundamentais na sociedade digital?. *Revista Brasileira de Direitos Fundamentais & Justiça*, 16(46), 155-175. <https://doi.org/10.30899/dfj.v16i46.1059>
- Sampaio, J. A. L. & Assis, C. C. (2021). Estado de vigilância. *Cadernos de Direito Actual*, (16), 178-200.
- Santos, G. N. C. & Inácio, J. B. (2018). Observatório do turismo e big data: a importância da informação e da tecnologia no desenvolvimento de destinos turísticos inteligentes e sustentáveis. *Caminhos de Geografia*, 19(65), 286-299. <https://seer.ufu.br/index.php/caminhosdegeografia/article/view/38865>
- Simão Filho, A. & Schwartz, G. A. D. (2016). Big Data Big Problema! Paradoxo Entre O Direito À Privacidade E O Crescimento Sustentável. *Conpedi Law Review*, 2(3), 311-331. https://doi.org/10.26668/2448-3931_conpedilawreview/2016.v2i3.3644
- Silva, C. R. C. (2022). *De adversários a inimigos: riscos à autenticidade dos processos eleitorais e à integridade democrática pelo agir estratégico da comunicação política nas mídias digitais* [dissertação de mestrado, pontifícia Universidade Católica de Minas Gerais]. Pergamum. <https://bib.pucminas.br/acervo/546834>
- Silverman, C. (2016, 16 de novembro). *This analysis shows how viral fake election news stories outperformed real news on facebook*. BuzzFeed.News. <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>
- Sunstein, C. R. (2007). *Republic.com 2.0*. Princeton University Press.
- Véliz, C (2021). *Privacidade é poder. Por que e como você deveria retomar o controle dos seus dados* (S. Oliveira, trad.). Editora Contracorrente.
- West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, 58(1), 20-41. <https://doi.org/10.1177/0007650317718185>
- Zarouali, B., Dobber, T., De Pauw, G. & de Vreese, C. (2022). Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media. *Communication Research*, 49(8), 1066-1091. <https://doi.org/10.1177/0093650220961965>
- Zuboff, S. (2021). *A Era do Capitalismo de Vigilância: uma luta por um futuro humano na nova fronteira do poder* (G. Schlesinger, trad.). Editora Intrínseca.