

CAPITALISMO DE VIGILÂNCIA: a personalização algorítmica como ferramenta de controle

SURVEILLANCE CAPITALISM: algorithmic personalization as a tool of control

CAPITALISMO DE VIGILANCIA: la personalización algorítmica como herramienta de control

Rafael Gomes Santos

Estudante de Bacharelado em Psicologia pelo Centro Universitário do Rio São Francisco – UniRios

Luciano Domingues Bueno

Psicólogo, mestre em Psicologia (UFAL) e doutorando em Serviço Social (UFAL)

RESUMO

A personalização algorítmica nas plataformas digitais atua como um mecanismo de controle social e psicológico. Este artigo analisa como o capitalismo de vigilância transforma dados em mercadorias, gerando ciclos de engajamento que impactam a saúde mental e a autonomia. A metodologia adotada consistiu em uma revisão sistemática de literatura com abordagem qualitativa, fundamentada na análise crítica de fontes acadêmicas. A busca foi realizada nas bases PubMed e Google Scholar, utilizando os descritores “vigilância digital”, “saúde mental” e “personalização algorítmica”, delimitando-se a artigos revisados por pares publicados entre 2000 e 2023. Dos 29 estudos inicialmente identificados, foram selecionados aqueles com maior aderência teórica aos objetivos da pesquisa. Os resultados revelam que o design algorítmico contribui para o agravamento de quadros de ansiedade e depressão. Conclui-se que a conscientização do usuário e o fortalecimento de regulamentações como a GDPR e a LGPD são essenciais para mitigar esses danos e resgatar a subjetividade do indivíduo no ambiente digital.

Palavras-chave: conscientização; personalização algorítmica; regulamentação. saúde mental; vigilância digital.

ABSTRACT

Algorithmic personalization on digital platforms acts as a mechanism of social and psychological control. This article analyses how surveillance capitalism transforms user data into commodities, generating engagement cycles that impact mental health and autonomy. The methodology consisted of a systematic literature review with a qualitative approach, grounded in the critical analysis of academic sources. The search was conducted in the PubMed and Google Scholar databases using the descriptors “digital surveillance”, “mental health”, and “algorithmic personalization”, focusing on peer-reviewed articles published between 2000 and 2023. From the 29 initially identified studies, those with the highest theoretical alignment with the research objectives were selected. Results reveal that algorithmic design contributes to the worsening of anxiety and depression. It is concluded that user awareness and the strengthening of regulations such as GDPR and LGPD are essential to mitigate these harms and reclaim individual subjectivity in the digital environment.

Keywords: awareness; algorithmic personalization; digital surveillance; mental health; regulation.

RESUMEN

La personalización algorítmica en las plataformas digitales actúa como un mecanismo de control social y psicológico. Este artículo analiza cómo el capitalismo de vigilancia transforma los datos de los usuarios en mercancías, generando ciclos de participación que impactan la salud mental y la autonomía. La metodología consistió en una revisión sistemática de la literatura con un enfoque cualitativo, basada en el análisis crítico de fuentes académicas. La búsqueda se realizó en las bases de datos PubMed y Google Scholar, utilizando los descriptores “vigilancia digital”, “salud mental” y “personalización algorítmica”, limitándose a artículos revisados por pares publicados entre 2000 y 2023. De los 29 estudios identificados inicialmente, se seleccionaron aquellos con mayor adherencia teórica a los objetivos de la investigación. Los resultados revelan que el diseño algorítmico contribuye al agravamiento de cuadros de ansiedad y depresión. Se concluye que la concienciación del usuario y el fortalecimiento de regulaciones como el GDPR y la LGPD son fundamentales para mitigar estos daños y recuperar la subjetividad individual en el entorno digital.

Palabras clave: concienciación; personalización algorítmica; regulación; salud mental; vigilancia digital.

INTRODUÇÃO

O avanço das tecnologias digitais nas últimas décadas transformou radicalmente a maneira como interagimos com a informação e com o mundo ao nosso redor. Em meio a essa revolução, a personalização algorítmica surgiu como uma ferramenta poderosa utilizada por grandes plataformas digitais, como Google, Facebook e YouTube. Embora essa tecnologia tenha inicialmente sido projetada para otimizar a experiência do usuário, ela também deu origem a uma nova forma de controle sobre o comportamento online, configurando o que Shoshana Zuboff (2019) denominou de *capitalismo de vigilância*.

Neste artigo, buscamos explorar as dinâmicas desse capitalismo de vigilância, analisando como as plataformas transformam os dados dos usuários em mercadorias valiosas, moldando padrões de engajamento digital que afetam a autonomia e a saúde mental dos indivíduos. Além disso, investigamos os impactos psicológicos dessa vigilância constante, como a ansiedade, o estresse digital e o sentimento de vigilância, especialmente com relação ao comportamento dos usuários nas redes sociais.

Para atingir os objetivos propostos, a presente pesquisa fundamenta-se em uma revisão sistemática de literatura com abordagem qualitativa. O procedimento metodológico consistiu no levantamento e análise crítica de produções acadêmicas indexadas nas bases de dados PubMed e Google Scholar. A busca foi refinada mediante o uso de descritores booleanos

relacionados à 'vigilância digital', 'saúde mental' e 'personalização algorítmica', abrangendo o recorte temporal de 2000 a 2023. Foram aplicados critérios de inclusão rigorosos, selecionando-se apenas artigos submetidos à revisão por pares que apresentassem aderência direta ao fenômeno do capitalismo de vigilância e seus impactos psicossociais. A partir de uma amostra inicial de 29 estudos, foram excluídos artigos duplicados ou fora do escopo. A análise subsequente envolveu a leitura integral dos textos para identificar padrões e lacunas, permitindo uma síntese teórica que integra evidências sobre a erosão da autonomia individual e o controle comportamental no ambiente digital.

1 HISTÓRICO DO CAPITALISMO DE VIGILÂNCIA

O conceito de capitalismo de vigilância emergiu no final do século XX e início do XXI, quando grandes empresas de tecnologia perceberam o imenso valor econômico que os dados dos usuários poderiam gerar. A coleta e análise de informações pessoais e comportamentais não era uma prática centralizada no início da internet. No entanto, com a explosão do uso da web e o surgimento das redes sociais, essa prática se tornou o alicerce do modelo de negócios de diversas empresas.

A transformação começou a se consolidar com o desenvolvimento de tecnologias de rastreamento, como os cookies, introduzidos na década de 1990. Inicialmente, esses pequenos fragmentos de dados eram usados para melhorar a experiência do usuário na navegação, permitindo que websites "lembrassem" informações como preferências de idioma ou itens adicionados a um carrinho de compras. No entanto, com o tempo, essas ferramentas foram adaptadas para coletar informações mais profundas, como padrões de comportamento, preferências e hábitos de consumo, dados que começaram a ser monetizados por empresas como Google e Facebook.

Com o avanço da tecnologia digital no início do século XXI, a quantidade de dados gerados globalmente atingiu níveis sem precedentes. A International Data Corporation (IDC) aponta que o volume de dados passou de 1,2 zettabytes em 2010 para 59 zettabytes em 2020, e estima-se que alcance 175 zettabytes em 2025 (IDC, 2020). Esse aumento expressivo está relacionado ao uso massivo de tecnologias de rastreamento, como cookies e pixels de monitoramento, que permitiram a coleta em larga escala por empresas como Google e Facebook. O lançamento do Google AdSense em 2003 foi um divisor de águas, introduzindo a publicidade segmentada baseada em perfis comportamentais, o que gerou bilhões em receitas publicitárias para a empresa (Smith, 2019). Da mesma forma, em 2004, o Facebook intensificou suas práticas de coleta de dados, o que consolidou o capitalismo de vigilância como o núcleo

de seu modelo de negócios.

Shoshana Zuboff, em seu livro de *The Age of Surveillance Capitalism*, foi uma das principais teóricas a consolidar o conceito de capitalismo de vigilância. Segundo Zuboff (2019), esse modelo econômico se baseia na extração de dados comportamentais das pessoas para prever e moldar seu comportamento, transformando a vida cotidiana em uma fonte de lucro. A Google foi uma das pioneiras nesse campo, ao perceber que as informações geradas pelos usuários de seus produtos poderiam ser processadas para melhorar a precisão de suas ferramentas publicitárias, criando um ciclo de coleta, análise e venda de dados.

A ascensão das redes sociais, como o Facebook, acelerou ainda mais esse processo. Essas plataformas não só coletavam dados de forma ativa, por meio de interações explícitas dos usuários (como curtidas, compartilhamentos e comentários), mas também passivamente, por meio de rastreamento invisível de navegação e uso de cookies de terceiros. Com o tempo, essa vigilância foi integrada em várias camadas da vida digital, ampliando o controle e a capacidade de influência dessas corporações sobre os indivíduos.

O surgimento do capitalismo de vigilância não pode ser dissociado do contexto de globalização e da evolução da cultura digital. A crescente interconexão entre indivíduos e instituições, facilitada pela internet, permitiu que grandes corporações como Google, Facebook e Amazon criassem ecossistemas digitais que vão além das redes sociais. As inovações tecnológicas, como algoritmos de aprendizado de máquina e inteligência artificial, proporcionaram às empresas a capacidade de analisar dados em uma escala sem precedentes, o que intensificou a vigilância e a manipulação do comportamento do usuário (Susskind, 2020).

Vale ressaltar que, o uso generalizado de smartphones alterou profundamente a coleta de dados. Esses dispositivos, que se tornaram essenciais na vida cotidiana, estão equipados com sensores e aplicativos que coletam informações constantemente, incluindo localização, hábitos de consumo e interações sociais. Segundo o estudo Hughes e Brown (2019), aproximadamente 90% dos dados gerados diariamente provêm de dispositivos móveis. Essa nova dimensão do monitoramento digital permite que as empresas acompanhem seus usuários em tempo real, transformando cada interação em um dado valioso que pode ser monetizado.

Esse cenário levanta questões críticas sobre a privacidade e a autonomia dos indivíduos, já que os usuários frequentemente não têm conhecimento pleno das informações que estão sendo coletadas e como essas informações são utilizadas. O capitalismo de vigilância, portanto, se estabelece não apenas como uma estratégia de lucro, mas também como uma nova forma de controle social, onde a vigilância se torna uma parte intrínseca da experiência digital.

A partir dos anos 2000, o modelo de negócios focado na coleta de dados se expandiu

além das gigantes da tecnologia, sendo adotado também por empresas de setores diversos, como Amazon, que utiliza dados para personalizar suas recomendações de produtos, e Microsoft, que explora o uso de seus sistemas operacionais e softwares para coletar insights valiosos sobre seus usuários.

O capitalismo de vigilância, então, não só transformou o mercado digital, mas também moldou o comportamento social, econômico e político, criando um ambiente onde os dados pessoais se tornaram uma commodity essencial para o lucro das corporações e para a manutenção de sua posição dominante no mercado.

2 ESTUDOS DE CASO SOBRE PLATAFORMAS DIGITAIS

O capitalismo de vigilância se manifesta de forma contundente nas práticas de empresas como Google, Facebook e Amazon, que utilizam a coleta massiva de dados para criar perfis comportamentais de seus usuários, transformando essa informação em uma mercadoria altamente rentável. Ao operar dentro de um sistema em que a atenção e os dados dos indivíduos são os principais ativos, essas corporações têm aperfeiçoado técnicas sofisticadas de monitoramento digital, influenciando diretamente o comportamento de seus usuários e criando novos padrões de consumo e interação online.

O Google é um dos principais expoentes desse modelo. A empresa rastreia praticamente todas as atividades online de um indivíduo, utilizando ferramentas como o Google Analytics, cookies de rastreamento e sua vasta rede de anúncios, o Google AdSense. Um estudo de Eslami et al. (2018), revelou que 91% dos usuários não estão cientes do nível de rastreamento que ocorre em suas navegações, evidenciando a falta de transparência nas práticas da empresa. Essas ferramentas permitem que a empresa monitore o comportamento dos usuários em milhões de sites, mesmo aqueles que não possuem contas no Google ou que utilizam navegadores que supostamente protegem a privacidade, como o modo de navegação anônima. Isso ilustra como o controle da infraestrutura digital permite que empresas como o Google coletem informações valiosas sem o consentimento explícito do usuário. Além disso, em 2019, o Google enfrentou uma multa de 5 bilhões de dólares imposta pela Comissão Federal de Comércio dos EUA por práticas de coleta de dados enganosas, demonstrando a seriedade das implicações legais de suas operações.

O Facebook, por sua vez, leva essa vigilância a um nível mais profundo ao coletar dados tanto de usuários logados quanto de não-usuários, utilizando pixels de rastreamento e cookies embutidos em sites de terceiros. Um estudo conduzido por Englehardt e Narayanan (2016) revelou que o Facebook usa tecnologias de rastreamento em mais de 1 milhão de sites,

permitindo que a empresa siga o comportamento online de indivíduos, mesmo fora de sua plataforma. Um caso emblemático foi o escândalo de Cambridge Analytica, que expôs como dados de até 87 milhões de usuários foram coletados sem consentimento para influenciar campanhas eleitorais, levantando questões éticas sobre privacidade e manipulação da opinião pública. Em audiências no Congresso dos Estados Unidos, a plataforma admitiu que monitora as atividades de não-usuários, criando perfis sombra para fins publicitários. Esses perfis, baseados em dados indiretos, como interações com amigos que utilizam a rede ou visitas a sites que integram o sistema de rastreamento do Facebook, geram um nível de vigilância que expande o poder da empresa sobre os fluxos de dados pessoais. Ao mesmo tempo, esses mecanismos influenciam o comportamento dos usuários ao criar bolhas informacionais, reforçando suas opiniões e direcionando-os para conteúdos e anúncios que reafirmam suas preferências, impactando negativamente o discurso público e a formação de opiniões.

A Amazon, embora mais conhecida por seu comércio eletrônico, também utiliza uma vasta rede de coleta de dados, rastreando as preferências de consumo e o comportamento de navegação dos usuários em sua plataforma e em sites afiliados. Em 2020, a empresa foi investigada por práticas anticompetitivas, incluindo o uso de dados de vendedores para desenvolver produtos concorrentes, levando a críticas sobre o uso abusivo de dados de terceiros (Pymnts, 2020). A empresa faz uso de algoritmos de recomendação e inteligência artificial (IA) para moldar o comportamento dos consumidores, incentivando-os a realizar compras frequentes, promovendo assim uma forma de "fetichismo digital", em que os objetos consumidos ganham uma aura quase mágica através da personalização de ofertas e publicidade (Peters, 2021). A cada interação do usuário com a plataforma, seja por meio de uma pesquisa de produto ou ao adicionar itens ao carrinho de compras, a Amazon coleta dados detalhados que vão além das simples preferências de consumo; essas informações incluem o tempo de navegação, padrões de cliques e até mesmo o tempo gasto em diferentes páginas (Bloomberg, 2021). Com esses dados, a empresa não apenas recomenda produtos, mas cria um ambiente digital que estimula o consumo impulsivo e recorrente, muitas vezes apresentando ao usuário itens que ele nem sabia que precisava, mas que, através da hiperpersonalização, parecem indispensáveis.

Esses estudos de caso demonstram como essas plataformas moldam o comportamento dos usuários, extraindo valor econômico por meio do monitoramento constante de suas atividades e promovendo o fenômeno da alienação digital. Esse processo de alienação ocorre quando os usuários se tornam produtos de suas interações digitais, muitas vezes sem plena consciência do processo (Zuboff, 2019). A constante vigilância e a coleta de dados, assim como

a influência sobre o comportamento dos indivíduos, levantam questões mais amplas sobre privacidade, liberdade de escolha e o controle exercido por essas empresas sobre a vida digital. Esse cenário desafia as regulações existentes e evidencia a necessidade de políticas mais transparentes e robustas para proteger os direitos dos indivíduos frente ao crescente poder das corporações digitais (Bloom, 2021).

De maneira semelhante ao que ocorre no monitoramento constante e no impacto sobre o comportamento digital, a verdadeira transformação dos dados coletados por essas plataformas ocorre na maneira como essas informações são monetizadas. Esses dados se tornam ativos valiosos principalmente através da personalização de anúncios, um dos principais modelos de monetização no capitalismo de vigilância. Plataformas como Google e Facebook utilizam perfis comportamentais de usuários para oferecer anúncios direcionados, aumentando a chance de conversão e, assim, atraindo anunciantes dispostos a pagar mais por esse tipo de segmentação. Conforme descreve Zuboff (2019), esses perfis permitem que as empresas prevejam e até mesmo modifiquem comportamentos futuros dos usuários, vendendo esses 'futuros comportamentais' aos anunciantes, que competem em leilões de anúncios em tempo real. Por outro lado, a Amazon utiliza dados de consumo e navegação para promover recomendações personalizadas, o que estimula o aumento das vendas e reforça o ciclo de coleta de dados e lucro (Acquisti ; Taylor ; Wagman, 2016).

3 ASPECTOS LEGAIS E REGULATÓRIOS

Com o crescimento do capitalismo de vigilância, surgem também desafios legais e éticos que demandam a criação de marcos regulatórios para proteger a privacidade e a autonomia dos indivíduos. A General Data Protection Regulation (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil são exemplos significativos de legislações que visam regular a coleta e o uso de dados pessoais, estabelecendo direitos e obrigações para as corporações.

A GDPR, implementada em 2018, é considerada uma das legislações mais rigorosas em matéria de proteção de dados. Ela estabelece princípios fundamentais, como a necessidade de consentimento explícito para o tratamento de dados, o direito de acesso e a portabilidade dos dados, e o direito ao esquecimento. Segundo o artigo 5º da GDPR, os dados devem ser "processados de forma lícita, leal e transparente em relação ao titular dos dados" (European parliament, 2016). Isso reflete uma tentativa de restabelecer o equilíbrio entre a autonomia individual e o controle das corporações sobre as informações pessoais.

No Brasil, a LGPD, sancionada em 2018 e em vigor desde setembro de 2020, tem como objetivo proteger os direitos fundamentais de liberdade e privacidade dos indivíduos. A lei é

inspirada na GDPR e estabelece normas sobre a coleta, uso, tratamento e armazenamento de dados pessoais. O artigo 6º da LGPD reforça a importância do consentimento e define as bases legais para o tratamento de dados, como a execução de contratos e o cumprimento de obrigações legais (Brasil, 2018).

A implementação dessas leis é fundamental para mitigar os riscos associados ao capitalismo de vigilância, pois proporcionam maior transparência e controle aos usuários sobre suas informações pessoais. Além disso, as legislações incentivam as empresas a adotarem práticas éticas no tratamento de dados, promovendo uma cultura de responsabilidade e respeito à privacidade. Contudo, a efetividade dessas legislações ainda enfrenta desafios, como a necessidade de conscientização e educação dos usuários sobre seus direitos, bem como a capacidade das autoridades reguladoras em fiscalizar e punir as violações (Bloom, 2021).

A aplicação prática da GDPR nos últimos anos tem gerado uma série de penalidades significativas contra grandes corporações, evidenciando seu impacto na proteção dos dados pessoais. Um caso notório foi a multa de €50 milhões imposta ao Google pela Comissão Nacional de Informática e Liberdades (CNIL) da França, em 2019. O motivo da penalidade foi a falta de transparência nas políticas de privacidade da empresa e a forma como ela obtinha consentimento para a personalização de anúncios (CNIL, 2019). De acordo com a GDPR, os usuários devem ser informados de forma clara e explícita sobre como seus dados são coletados e utilizados, e o Google não cumpriu essas exigências. Outro caso marcante ocorreu em 2021, quando a Amazon foi multada em €746 milhões por violações à GDPR em Luxemburgo. A empresa foi acusada de processar dados pessoais de forma inadequada, sem o consentimento explícito dos usuários, demonstrando que mesmo gigantes da tecnologia podem enfrentar sérias repercussões por desrespeitar a privacidade dos consumidores (Bloomberg, 2021).

No Brasil, a aplicação da LGPD também já resultou em penalidades para empresas. Em 2022, o Banco C6 foi multado em R\$ 11 milhões pela Autoridade Nacional de Proteção de Dados (ANPD) por falhas no tratamento de dados pessoais de clientes. O banco foi acusado de não implementar medidas de segurança adequadas para proteger os dados sensíveis de seus clientes, expondo-os a riscos de vazamentos e fraudes (ANPD, 2022). Outro exemplo significativo foi a multa de R\$ 5 milhões aplicada à empresa Telefônica/Vivo, por práticas inadequadas no uso de dados para marketing direto, sem o devido consentimento dos usuários (Valente, 2022). Esses casos destacam a crescente importância das legislações de proteção de dados na promoção de práticas mais transparentes e seguras.

Essas iniciativas legislativas, portanto, representam um passo importante na busca por um equilíbrio entre os interesses das corporações e os direitos dos indivíduos, ajudando a

moldar um ambiente digital mais seguro e ético.

4 A PERSONALIZAÇÃO COMO FERRAMENTA DE CONTROLE

A personalização algorítmica nas redes sociais pode ser entendida como uma faca de dois gumes. De um lado, oferece uma experiência adaptada, supostamente simplificando o acesso a conteúdos de interesse para os usuários. De outro, serve como uma ferramenta de controle que maximiza o engajamento, visando aumentar o tempo gasto nas plataformas e, consequentemente, os lucros dessas empresas. Essa lógica cria uma dependência comportamental e emocional, capturando os usuários em um ciclo de recompensas e estímulos (Vaid, 2023). O que parecia ser uma “personalização” benéfica revela-se uma forma de manipulação projetada para reter a atenção do usuário a qualquer custo.

A personalização algorítmica é baseada em técnicas de aprendizado de máquina que analisam os comportamentos passados dos usuários para prever e influenciar suas futuras interações. Isso é feito através da coleta massiva de dados, que incluem desde cliques e curtidas até o tempo gasto em cada postagem. Esses dados são então usados para criar perfis detalhados dos usuários, permitindo que os algoritmos apresentem conteúdos que são mais prováveis de gerar engajamento. Essa prática não apenas aumenta o tempo que os usuários passam nas plataformas, mas também pode levar a uma forma de dependência digital, onde os indivíduos se sentem compelidos a retornar constantemente às redes sociais para obter novas recompensas e estímulos (Zuboff, 2019).

Além disso, a personalização algorítmica pode ter efeitos profundos na formação da identidade e nas relações sociais dos usuários. Ao serem constantemente expostos a conteúdos que reforçam suas preferências e crenças, os indivíduos podem desenvolver uma visão distorcida da realidade, onde suas opiniões são constantemente validadas e raramente desafiadas. Isso pode levar a uma forma de isolamento social, onde os usuários se tornam menos propensos a interagir com pessoas que têm pontos de vista diferentes, exacerbando a polarização social e política (Sunstein, 2017).

Um exemplo claro desse fenômeno é o experimento de 2012 conduzido pelo Facebook, onde a plataforma manipulou o conteúdo exibido nos feeds de seus usuários para estudar o impacto na alteração de seu humor. O estudo, conhecido como “Experimental evidence of massive-scale emotional contagion through social networks”, envolveu a alteração do conteúdo emocional das postagens vistas por cerca de 689.000 usuários sem o seu conhecimento. Os resultados indicaram que era possível influenciar o estado emocional das pessoas através de pequenos ajustes no conteúdo algorítmico (Kramer et al., 2014). Especificamente, os usuários

que foram expostos a conteúdos mais positivos tendiam a postar mensagens mais positivas, enquanto aqueles expostos a conteúdos mais negativos faziam postagens mais negativas.

Esse experimento levanta preocupações éticas significativas sobre o poder das empresas de tecnologia em moldar o comportamento humano sem o consentimento explícito dos indivíduos. A manipulação emocional sem o conhecimento dos usuários não apenas viola princípios de consentimento informado, mas também questiona a responsabilidade ética das plataformas em relação ao bem-estar psicológico de seus usuários. Além disso, a falta de transparência sobre tais práticas impede que os usuários compreendam plenamente como suas emoções e comportamentos estão sendo influenciados, o que pode ter implicações de longo prazo para a confiança nas plataformas digitais (Flick, 2016).

Soma-se a isso, o conceito de “bolhas de filtro”, popularizado por Eli Pariser, mostrando como a personalização pode restringir o acesso a informações diversas. Os algoritmos tendem a reforçar opiniões já existentes, expondo os usuários quase exclusivamente a conteúdos que confirmam suas crenças prévias. Esse processo, longe de ser neutro, agrava a polarização política e social, dificultando o contato com diferentes perspectivas e promovendo uma visão limitada e fragmentada da realidade (Pariser, 2011). Por exemplo, um usuário que frequentemente interage com conteúdos de uma determinada orientação política verá cada vez mais conteúdos alinhados com essa orientação, enquanto conteúdos de perspectivas opostas serão filtrados. Isso cria um ambiente onde as opiniões divergentes são raramente vistas, reforçando a crença de que a visão de mundo do usuário é a única correta.

Estudos demonstram que essa polarização impacta a saúde mental dos usuários, intensificando sentimentos de ansiedade e depressão (Boulianne, 2019). A exposição constante a conteúdos polarizados pode criar um ambiente de estresse e conflito, onde os usuários se sentem constantemente pressionados a defender suas opiniões e atacar as dos outros. Além disso, a falta de exposição a perspectivas diversas pode levar a uma visão de mundo mais estreita e menos empática, dificultando a capacidade dos indivíduos de compreender e se conectar com aqueles que têm experiências e opiniões diferentes (Iyengar ; Westwood, 2015).

A pesquisa de Tufekci (2015) sobre o papel das redes sociais em eventos políticos sugere que essa dinâmica pode ter influenciado resultados eleitorais, evidenciando ainda mais a relevância da manipulação algorítmica no cenário atual. Tufekci argumenta que as redes sociais não apenas facilitam a organização de movimentos sociais, mas também amplificam a visibilidade de determinados discursos, potencialmente influenciando a opinião pública e os resultados eleitorais. Por exemplo, durante a Primavera Árabe, as redes sociais foram cruciais para a mobilização de protestos, mas também foram usadas por regimes autoritários para

monitorar e reprimir dissidentes (Tufekci, 2015).

A manipulação algorítmica também tem implicações significativas para a democracia. A capacidade de direcionar informações específicas para diferentes grupos de eleitores pode manipular suas opiniões e votos, comprometendo a integridade dos processos democráticos. A falta de transparência sobre como os algoritmos funcionam é uma grande preocupação. As empresas de tecnologia precisam ser mais transparentes e responsáveis pelo impacto de seus algoritmos. A educação digital é crucial para capacitar os usuários a entenderem como os algoritmos funcionam e como podem proteger sua privacidade e autonomia online. Além disso, a regulamentação mais rigorosa é necessária para proteger os usuários contra a manipulação algorítmica. Exemplos de legislações recentes, como o GDPR na Europa, podem ser mencionados como passos importantes nessa direção.

5 IMPACTOS PSICOLÓGICOS DA VIGILÂNCIA ALGORÍTMICA

A vigilância algorítmica, impulsionada por práticas de coleta de dados massiva e personalização, gera uma série de consequências psicológicas significativas para os usuários. A pressão constante para "performar" nas redes sociais, onde a autoimagem é frequentemente moldada pela validação externa por meio de curtidas e comentários, pode impactar negativamente a autoestima. Os indivíduos podem sentir que suas vidas estão sendo avaliadas com base em critérios que não correspondem à sua realidade, levando a comparações sociais prejudiciais (Hogan, 2020).

Além disso, o ambiente digital, onde a performance é muitas vezes medida em tempo real, pode contribuir para um estado contínuo de estresse e ansiedade. De acordo com um estudo realizado por Barlow e Durand (2020), a percepção de que os usuários estão sempre sob vigilância pode levar a um aumento da pressão psicológica, resultando em comportamentos de autoavaliação compulsiva. A busca por aceitação e validação online pode levar a uma ansiedade generalizada, especialmente entre jovens e adolescentes, que estão mais suscetíveis às influências das redes sociais.

Outro aspecto relevante é o fenômeno do "estresse digital", que se refere à ansiedade e à sobrecarga emocional resultantes do uso excessivo de tecnologia e da exposição constante a informações. O estresse digital pode manifestar-se de diversas maneiras, incluindo dificuldade de concentração, irritabilidade e fadiga mental (Susskind, 2020). A necessidade de estar sempre conectado e disponível pode criar um ciclo vicioso, onde os indivíduos se sentem pressionados a monitorar suas redes sociais constantemente, exacerbando sua ansiedade em relação à privacidade e ao controle sobre suas informações pessoais.

Estudos psicológicos recentes revelam que o uso excessivo de redes sociais pode ter efeitos prejudiciais à saúde mental em diversas faixas etárias, com impactos diferenciados em cada grupo. Uma pesquisa conduzida por Twenge et al. (2020) demonstrou que adolescentes, especialmente meninas, são mais vulneráveis ao desenvolvimento de sintomas de depressão e ansiedade relacionados ao uso intensivo de redes sociais, devido à exposição constante a comparações sociais e validação externa. Contribuindo para esse debate, um estudo de Chopra e Sharma (2021) mostrou que adultos jovens, na faixa dos 20 aos 30 anos, tendem a experimentar uma maior pressão para manter uma "identidade digital" de sucesso, levando a sentimentos de esgotamento mental e estresse crônico. Já entre os idosos, conforme apontado por Lowe e Robards (2019), a vigilância nas redes sociais pode contribuir para o isolamento social e a sensação de inadequação, especialmente em relação à capacidade de adaptação às tecnologias digitais. Esses estudos evidenciam que o impacto das redes sociais na saúde mental varia conforme a faixa etária, mas todos indicam um aumento significativo no nível de estresse e na deterioração do bem-estar psicológico.

A ansiedade ligada à privacidade é uma preocupação crescente na era do capitalismo de vigilância. Muitos usuários expressam insegurança sobre como seus dados estão sendo utilizados e quem tem acesso a eles. Essa falta de transparência pode gerar um sentimento de vulnerabilidade, contribuindo para o aumento da desconfiança em relação às plataformas digitais e às empresas que as administram (Sushchick, 2021). Os indivíduos podem se sentir como se estivessem sendo observados constantemente, levando a um estado de vigilância interna que impacta suas interações sociais e sua saúde mental.

Portanto, as consequências psicológicas da vigilância algorítmica não podem ser ignoradas. A interseção entre monitoramento digital, autoimagem e saúde mental destaca a necessidade urgente de considerar o impacto das práticas de vigilância nas vidas dos indivíduos. Esse cenário exige uma reflexão crítica sobre a forma como a tecnologia é utilizada e como os usuários podem se proteger em um ambiente cada vez mais vigiado.

6 RECOMENDAÇÕES PARA MITIGAÇÃO DOS EFEITOS DA VIGILÂNCIA ALGORÍTMICA

Para mitigar os impactos negativos da vigilância algorítmica na saúde mental e na privacidade, é essencial adotar uma abordagem multifacetada que envolva tanto os usuários quanto as plataformas digitais. A educação e conscientização sobre o funcionamento dos algoritmos e a coleta de dados são essenciais para mitigar os impactos negativos da vigilância algorítmica. Conforme apontado por Freire (1970) e desenvolvido na literatura da Psicologia

Social Comunitária, o conceito de conscientização envolve um processo de reflexão crítica que permite aos indivíduos entenderem as estruturas de poder que moldam suas experiências digitais e sociais (Pinto; Paiva, 2021). Aplicado ao cenário da vigilância algorítmica, esse processo é fundamental para que os usuários recuperem a autonomia sobre suas vidas digitais e exijam políticas de privacidade mais justas e transparentes. As plataformas digitais podem desenvolver campanhas que esclareçam aos usuários como seus dados são coletados e utilizados. A criação de ferramentas que ajudem os usuários a monitorar seu tempo de uso, como alertas e notificações que incentivem pausas regulares, pode ser uma maneira eficaz de promover um uso mais saudável e consciente das redes sociais (Jackson et al., 2021). Um bom exemplo comparativo são os efeitos das políticas públicas de regulamentação, proibição de publicidade e conscientização da população sobre os efeitos do cigarro que conseguiu ter impactos no consumo de cigarros pela população e, consequentemente, de seus malefícios.

Vale ressaltar que, a transparência nas políticas de privacidade é crucial para que os usuários possam tomar decisões mais informadas sobre o compartilhamento de suas informações pessoais. Muitas vezes, as políticas de privacidade são complexas e de difícil compreensão, o que impede uma leitura atenta por parte dos usuários. Por isso, as empresas devem adotar uma linguagem simplificada, destacando de forma clara as práticas de coleta e uso de dados. Segundo Goldstein (2020), a implementação de uma política de "privacidade por padrão", onde as configurações mais restritivas de privacidade são aplicadas automaticamente, seria um avanço significativo no empoderamento dos indivíduos sobre suas informações pessoais.

Outra medida importante envolve a promoção do bem-estar digital por meio de práticas que incentivem a desconexão periódica e a redução da exposição constante às redes sociais. A pressão para estar sempre conectado e disponível pode gerar esgotamento mental e emocional, conforme apontado por Smith e Taylor (2019). Ferramentas como modos de "foco" e "não perturbe" podem ser oferecidas pelas plataformas, permitindo que os usuários se concentrem em atividades fora do ambiente digital sem interrupções constantes, promovendo assim um equilíbrio saudável entre o mundo online e offline.

Por fim, é essencial que as plataformas digitais sejam pressionadas a assumir um papel de maior responsabilidade social. No entanto, não se pode esperar que essas corporações ajustem seus algoritmos voluntariamente, uma vez que o atual modelo de negócios capitalista incentiva práticas que promovem o engajamento a qualquer custo, incluindo o agravamento de problemas de saúde mental (Zuboff, 2019). Estudos indicam que o aumento de sentimentos negativos, como ódio e indignação, gera mais interações do que sentimentos positivos, tornando

essas dinâmicas lucrativas para as plataformas (Tufekci, 2018). Dessa forma, é necessário que o Estado e órgãos reguladores intervenham, impondo regras claras sobre o uso de algoritmos e limitando o poder das corporações de manipular o comportamento dos usuários em detrimento de sua saúde mental. Além disso, a conscientização crítica dos usuários e a pressão por parte da sociedade civil são essenciais para criar um ambiente digital mais justo e equilibrado. Estudos mostram que a amplificação de conteúdo baseado em métricas de popularidade, como curtidas e compartilhamentos, pode aumentar a pressão social e os sentimentos de inadequação (Johnson, 2020). Ao ajustar os algoritmos para priorizar conteúdo positivo e informativo, e reduzir o foco em métricas de validação social, as plataformas podem contribuir para uma experiência digital mais saudável e menos orientada pela competitividade social.

Essas recomendações, quando aplicadas, têm o potencial de reduzir significativamente os impactos negativos da vigilância digital, promovendo um ambiente online mais saudável e equilibrado. A combinação de práticas de conscientização, políticas de privacidade mais claras e a promoção de um uso mais moderado das redes sociais pode ajudar tanto os usuários quanto as plataformas a criar um ecossistema digital mais sustentável e ético.

7 O CAPITALISMO DE VIGILÂNCIA E O FETICHISMO DIGITAL: UMA ANÁLISE DO TRABALHO OCULTO

O conceito de fetichismo da mercadoria, conforme Karl Marx delineia em *O Capital*, refere-se à forma como as relações sociais de produção são ocultadas e distorcidas pelo valor atribuído às mercadorias. No capitalismo, as relações entre as pessoas passam a ser mediadas por objetos, criando uma ilusão de que os produtos possuem valor intrínseco, independente do trabalho humano que os produziu. Esse processo mascara as condições de exploração e alienação do trabalhador, que se vê distanciado do valor real que ele cria (Marx, 2013).

Ao fetichizar as mercadorias, o capitalismo obscurece a verdadeira fonte de valor, que é o trabalho humano. Para Marx (2013), o fetichismo da mercadoria cria uma inversão na percepção das relações sociais: em vez de ver as mercadorias como resultado das interações humanas e do trabalho, as pessoas começam a perceber as relações sociais como relações entre coisas. As mercadorias parecem ter vida própria, como se possuíssem valor intrínseco e pudessem circular no mercado sem a intervenção humana. Esse "encantamento" das mercadorias esconde a exploração do trabalho e as condições de produção, apresentando os produtos como autônomos e separados de seu processo criativo. Dessa forma, o fetichismo não apenas distorce a realidade econômica, mas também contribui para a alienação do trabalhador, que perde a conexão com o produto de seu trabalho e, conseqüentemente, com sua própria

atividade produtiva.

Essa alienação é reforçada pela divisão do trabalho no capitalismo, onde o trabalhador se especializa em tarefas fragmentadas e desconexas. O resultado final do trabalho coletivo se materializa em produtos que parecem independentes das relações sociais que os criaram. O trabalhador, portanto, não reconhece a si mesmo na mercadoria, perdendo o controle sobre o processo de produção e sobre o valor que seu trabalho gera. Esse distanciamento contribui para uma forma de alienação mais ampla, na qual o indivíduo não apenas se desconecta do fruto de seu trabalho, mas também das relações sociais que estruturam a sociedade capitalista (Marx, 2013).

No capitalismo de vigilância, descrito por Zuboff (2019), essa lógica de fetichismo é exacerbada no ambiente digital. O capitalismo de vigilância é caracterizado pela coleta massiva de dados dos comportamentos dos usuários, que são transformados em commodities digitais, muitas vezes sem o conhecimento ou consentimento explícito daqueles que fornecem essas informações. Esses dados, extraídos de forma sistemática e invisível, tornam-se mercadorias com valor de troca, transformando as interações humanas cotidianas em uma forma de capital. Para Zuboff, a coleta de excedente comportamental – um termo que ela cunha para descrever os dados excedentes não necessários para o aprimoramento dos serviços oferecidos, mas sim destinados à criação de novos mercados – torna-se a base da acumulação de riqueza no capitalismo digital.

Assim como o fetichismo da mercadoria esconde as relações de exploração no capitalismo industrial, o fetichismo digital oculta a extração de valor dos dados gerados pelos usuários. O usuário, ao interagir com plataformas digitais, fornece informações que se tornam matéria-prima para a criação de produtos preditivos vendidos no mercado de comportamentos futuros (Zuboff, 2019). Empresas como Google, Facebook e Amazon monetizam a previsão e modulação do comportamento humano, sem que os usuários tenham plena consciência de como seus dados estão sendo coletados, analisados e comercializados (Tufekci, 2018). Esse processo estabelece uma relação assimétrica de poder, onde as corporações tecnológicas controlam a informação e as condições de sua utilização, enquanto os indivíduos se tornam meros fornecedores de dados. Nesse contexto, Lyon (2001) ressalta que a vigilância não apenas oferece benefícios como segurança e conveniência, mas também aumenta o poder das organizações em detrimento da privacidade individual, reforçando a desigualdade nas relações sociais, já que os usuários perdem o controle sobre suas informações e se tornam dependentes dos sistemas que utilizam.

Esse fetichismo digital, no entanto, vai além do campo econômico e entra na esfera

ideológica. Zuboff (2019) argumenta que o capitalismo de vigilância não apenas monetiza o comportamento humano, mas também exerce um controle invisível sobre a subjetividade e a conformação da opinião pública. Ao manipular algoritmos para mostrar conteúdo de forma personalizada, as plataformas criam uma relação de dependência e subordinação, onde a liberdade individual é constantemente ameaçada. Segundo Zuboff (2019), as empresas digitais possuem um controle significativo sobre as escolhas dos usuários, moldando suas preferências e comportamentos de forma invisível, o que compromete a autonomia desses indivíduos.

Essa lógica é reveladora quando pensamos no impacto que essas tecnologias têm sobre a opinião pública e os processos democráticos (Tufekci, 2018). A coleta e manipulação de dados, muitas vezes realizada sem o consentimento consciente do usuário, pode influenciar as preferências políticas, direcionar o consumo e até condicionar as formas de sociabilidade (Zuboff, 2019). Dessa forma, as corporações tecnológicas assumem o papel de 'curadoras' de informação, estruturando o fluxo de ideias e moldando o debate público, tudo isso sem a transparência necessária para que os usuários compreendam a extensão desse poder. Essa interferência, em última instância, serve para reforçar a lógica capitalista, pois orienta as subjetividades e decisões em favor dos interesses corporativos, muitas vezes criando um falso senso de liberdade e autonomia (Harari, 2018).

O fetichismo digital também incorpora uma forma particular de alienação (Marx, 2013). Os algoritmos e as plataformas digitais, que produzem e acumulam capital a partir desses dados, são percebidos como autossuficientes, como se funcionassem de forma neutra e independente da intervenção humana. No entanto, há um vasto trabalho invisível por trás dessas interfaces, incluindo o trabalho dos desenvolvedores de algoritmos e engenheiros de dados, cujo papel crucial no processo de exploração digital é constantemente ocultado (Bolanõ, 2000; 2002). O usuário, por sua vez, não reconhece que está, de fato, “trabalhando” ao gerar dados que alimentam essas plataformas (Lyon, 2001). Esse cenário reflete a lógica do fetichismo: o processo de produção de valor digital é obscurecido, e os usuários tornam-se, simultaneamente, produtores e consumidores de dados, prosumidores Dantas (2012; 2014). Autores ligados à Economia Política da Comunicação (ECP) apreendem que, no contexto de exploração econômica de usuários e usuárias das redes sociais, o produto que opera essa alienação da classe trabalhadora e é a principal fonte de riqueza das big techs é a “mercadoria audiência”, fruto do processamento das informações espoliadas pelos arranjos tecnológicos (Bolaño, 2000; 2002; Seto, 2024).

Essa alienação digital reflete-se também no distanciamento dos indivíduos em relação às suas próprias informações. Os usuários estão progressivamente se alienando dos dados que

produzem, frequentemente sem perceber que esses dados estão sendo transformados em capital, moldando suas experiências e comportamentos (Tufekci, 2018). Zuboff (2019) chama atenção para o surgimento de um novo tipo de poder, o instrumentarianismo, que se diferencia de formas anteriores de poder totalitário ao atuar de forma não coercitiva, mas, ainda assim, profundamente invasiva e manipulativa (Zuboff, 2019). No capitalismo de vigilância, o controle é exercido não por meio da força física, mas pela previsão e influência dos comportamentos futuros. As plataformas tecnológicas, ao utilizarem dados para modelar comportamentos, criam uma relação de dependência e subordinação, onde a liberdade individual é constantemente ameaçada. Zuboff (2019) destaca que as empresas digitais têm um poder sem precedentes para moldar e monitorar as escolhas dos indivíduos, criando um novo tipo de controle que é tanto invisível quanto abrangente, evidenciando como essa dinâmica compromete a autonomia dos usuários.

Em síntese, o capitalismo de vigilância representa uma nova configuração do fetichismo descrito por Marx (2013), onde os dados, e não apenas as mercadorias, se tornam fetiches que mascaram as relações sociais subjacentes de exploração. A análise do capitalismo de vigilância através da lente do fetichismo digital revela que a extração de valor dos dados pessoais não apenas disfarça o trabalho humano oculto, mas também amplia a alienação e o controle na era digital (Lyon, 2001). Além disso, esse sistema reforça a hegemonia das corporações de tecnologia, que não só acumulam capital, mas também moldam a opinião pública e as subjetividades de forma sutil. Harari (2018) destaca que essas empresas não apenas vendem produtos, mas têm o poder de manipular a informação que recebemos, criando realidades alternativas que servem aos seus próprios interesses, consolidando o poder econômico e ideológico no contexto do capitalismo contemporâneo.

Essa acumulação de riquezas mediada pela predição e manipulação de comportamentos com finalidades mercantis, apoiam-se na desregulamentação e desmonte de direitos que resguardam a população de práticas nocivas ao seu bem estar. Isso repercute em uma desarticulação sistemática de condições democráticas ao redor do mundo. Esse cenário de barbárie, em que esses dados de vigilância e predição de comportamentos são, inclusive, usados para invasões de territórios e ataques por potências que sediam grande parte dessas big techs, expressa aquilo que pesquisadores formulam como um colonialismo digital (Faustino; Lippold, 2023), baseado em uma acumulação pela espoliação e expropriação de direitos (Seto, 2024; Fontes, 2010; 2018).

CONSIDERAÇÕES FINAIS

A vigilância algorítmica nas plataformas digitais é uma realidade intrinsecamente ligada à lógica capitalista contemporânea, que subordina direitos fundamentais, como a privacidade e a autonomia, aos imperativos do lucro e da competitividade (Seto, 2014; Fontes, 2010; 2018). Ao longo deste artigo, foi possível observar como a personalização algorítmica, inicialmente projetada para aprimorar a experiência do usuário (Zuboff, 2019), se transformou em uma ferramenta de controle social e psicológico, operando sob uma estrutura econômica que prioriza a acumulação de capital em detrimento do bem-estar coletivo (Johnson, 2020; Chopra; Sharma, 2021).

Neste sentido, embora regulamentações como a GDPR na Europa e a LGPD no Brasil representem avanços importantes, elas são insuficientes para enfrentar as raízes do problema. Mesmo que tais legislações busquem proteger os dados pessoais, elas não desafiam diretamente a lógica exploratória que sustenta o capitalismo digital. Afinal, o cerne da questão não é apenas a proteção dos dados, mas o **uso predatório** desses dados pelas grandes corporações para moldar comportamentos e explorar subjetividades.

Portanto, a solução não pode ser reduzida à conscientização individual sobre práticas de uso saudável das plataformas. Isso, embora importante, desloca o foco das verdadeiras causas estruturais que perpetuam essa exploração. A responsabilidade recai sobre o sistema econômico que fomenta a extração de valor dos dados pessoais e que, ao criar uma falsa sensação de liberdade e personalização, encobre a alienação e a subordinação digital.

Se queremos realmente mitigar os impactos nocivos da vigilância algorítmica, é fundamental questionar o próprio arcabouço do capitalismo, que, ao se apropriar da tecnologia para maximizar o lucro, compromete os direitos e a dignidade dos indivíduos. Assim, mais do que regulamentações, precisamos de uma reconfiguração sistêmica que enfrente o modo de produção capitalista e suas formas de controle digital. Sem isso, as tentativas de mitigar os danos da vigilância algorítmica continuarão sendo superficiais e ineficazes.

REFERÊNCIAS

ANPD. Autoridade Nacional de Proteção de Dados multa C6 Bank por violações à LGPD. 2022. Disponível em: <https://www.anpd.gov.br/>. Acesso em: 11 out. 2024.

BLOOM, A. Data protection in the digital age: challenges and opportunities. **Journal of Information Ethics**, v. 30, n. 1, p. 45-56, 2021.

BLOOMBERG. **Amazon given record 888 million EU fine for data privacy breach**. 2021. Disponível em: <https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record->

888-million-eu-fine-for-data-privacy-breach. Acesso em: 11 out. 2024.

BOLAÑO, C. R. S. Trabalho intelectual, comunicação e capitalismo. A re-configuração do fator subjetivo na atual reestruturação produtiva. **Revista Soc. bras. Economia Política**, Rio de Janeiro, nº 11, p. 53-78, dezembro 2002. Disponível em: <https://eptic.com.br/wp-content/uploads/2020/06/Trabalho-intelectual-comunica%C3%A7%C3%A3o-e-capitalismo-Bola%C3%B1o.pdf> Acesso em 30 de dezembro de 2025.

BOLAÑO, C. R. S.; VIEIRA, Eloy Santos. Economia Política da Internet: sites de redes sociais e luta de classes. In: **Congresso Brasileiro de Ciências da Comunicação**, 36., Manaus: Intercom, 2012. Disponível em: <http://www.intercom.org.br/papers/nacionais/2013/resumos/r8-0126-1.pdf> Acesso em 14 de janeiro de 2026.

BORENSTEIN, M.; HEDGES, L. V.; HIGGINS, J. P. T.; ROTHSTEIN, H. R. **Introduction to Meta-Analysis**. Chichester: Wiley-Blackwell, 2009.

BRASIL. Lei Geral de Proteção de Dados Pessoais. **Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 9 out. 2024.

CHOPRA, R.; SHARMA, P. The digital self and its psychological impact on adults: a review. **Cyberpsychology, Behavior, and Social Networking**, v. 24, n. 2, p. 105-113, 2021.

CNIL. **CNIL's restricted committee imposes a financial penalty of 50 million euros against Google LLC**. 2019. Disponível em: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Acesso em: 11 out. 2024.

EUROPEAN PARLIAMENT. **General Data Protection Regulation. Regulation (EU) 2016/679**. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 9 out. 2024.

DANTAS, M. **Trabalho com informação: valor, acumulação, apropriação nas redes do capital**. Rio de Janeiro: UFRJ: Escola de Comunicação, 2012.

DANTAS, M. Mais Valia 2.0: Produção e apropriação de valor nas redes do capital. **Revista Eptic Online**, [S. l.], v. 16, n. 2, p. 89-112, 2014. Disponível em: <https://periodicos.ufs.br/epic/article/view/2167/1948> Acessado em 14 de dezembro de 2025.

GOLDSTEIN, H. Privacy policies: simplifying complexity for user empowerment. **Journal of Information Ethics**, v. 29, n. 2, p. 27-35, 2020.

HARARI, Y. N. *21 Lições para o Século 21*. São Paulo: Companhia das Letras, 2018.

FAUSTINO, D. M.; LIPPOLD, W. **Colonialismo digital: por uma crítica hacker-fanoniana**. São Paulo: Boitempo, 2023.

FONTES, V. **O Brasil e o capital-imperialismo: teoria e história**. Editora UFRJ. Rio de Janeiro, 2010.

FONTES, V. A transformação dos meios de existência em capital — expropriações, mercado e propriedade. In: Boschetti, Ivanete (Org.). **Expropriação e direitos no capitalismo**. São

Paulo, Cortez Editora, 2018, pp. 17-61.

HOGAN, B. Social media and the performance of self. In: BURGESS, J.; MARWICK, A.; POELL, T. (Orgs.). **The Routledge Handbook of Digital Media and Communication**. Routledge, 2020. p. 183-196.

HUGHES, T.; BROWN, L. The impact of mobile devices on data collection: a comprehensive overview. **Journal of Data Science**, v. 17, n. 3, p. 221-239, 2019.

IDC. **The digitization of the world: from edge to core**. 2019. Disponível em: <https://www.idc.com>. Acesso em: 10 out. 2024.

JACKSON, M.; MILLER, K.; DAVIS, R. Digital wellbeing and the role of time management tools in social media platforms. **Journal of Cyberpsychology**, v. 10, n. 3, p. 85-98, 2021.

JOHNSON, A. The social media algorithm and its psychological toll: how platforms can promote healthier online habits. **Psychology of Media Journal**, v. 15, n. 2, p. 53-68, 2020.

KRAMER, A. D. I.; GUILLORY, J. E.; HANCOCK, J. T. Experimental evidence of massive-scale emotional contagion through social networks. **Proceedings of the National Academy of Sciences of the United States of America**, v. 111, n. 24, p. 8788–8790, 2014.

LOWE, D.; ROBARDS, B. Aging and the digital divide: the role of social media surveillance in elderly isolation. **Journal of Aging Studies**, v. 33, n. 1, p. 15-23, 2019.

LYON, D. **Surveillance Society: Monitoring Everyday Life**. Buckingham: Open University Press, 2001.

MARX, K. **O Capital: Crítica da Economia Política**. São Paulo: Boitempo, 2013.

PARISER, E. **The Filter Bubble: What the Internet Is Hiding from You**. New York: Penguin Press, 2011.

PETERS, J. The Amazon Algorithm and Consumer Behavior: A Study of the Digital Market. **Journal of Consumer Research**, v. 18, n. 2, p. 112-125, 2021.

PYMNTS. **Amazon facing EU antitrust complaints over seller data**. 2020. Disponível em: <https://www.pymnts.com/amazon/2020/amazon-facing-eu-antitrust-complaints-over-seller-data/>. Acesso em: 12 out. 2024.

SMITH, A. The rise of targeted advertising: how Google changed the game. **Journal of Digital Marketing**, v. 12, n. 4, p. 43-57, 2019.

SMITH, L.; TAYLOR, R. Disconnect to reconnect: the benefits of digital detox. **Journal of Digital Wellbeing**, v. 7, n. 1, p. 22-37, 2019.

SOUZA, M. C.; OLIVEIRA, D. M. Conscientização para Transformação Social: Apontamentos para a Psicologia Social Comunitária. **Revista de Psicologia**, v. 11, n. 2, p. 58-75, 2020. Disponível em: <http://www.revistapsicologia.ufc.br>. Acesso em: 15 out. 2024.

SUSSKIND, R. **The Future of the Professions: How Technology Will Transform the Work of Human Experts**. Cambridge: Harvard University Press, 2020.

SUSHCHIK, M. The privacy paradox: understanding anxiety in the age of surveillance. *International Journal of Cyber Behavior, Psychology and Learning*, v. 11, n. 2, p. 34-47, 2021.

TUFEKCI, Z. YouTube, the Great Radicalizer. **The New York Times**, 10 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html>. Acesso em: 15 out. 2024.

TWENGE, J. M.; MARTIN, G. N.; SPITZER, M. Social media use and mental health in adolescents: trends and implications. **Journal of Adolescent Health**, v. 66, n. 4, p. 47-52, 2020.

VAID, S. S. Paradigm shifts in digital personalization. **Nature Reviews Psychology**, v. 2, n. 7, p. 390, 2023.

SETO, K. S. **O algoritmo e o capital**: ensaios Introdutórios à Economia dos Meios Digitais. Curitiba: Appris, 2024. Arquivo Digital – Epub.

ZUBOFF, S. **A Era do Capitalismo de Vigilância**. Rio de Janeiro: Intrínseca, 2019.