ABCiber
FLUXOS EMERGENTES & CONEXÕES EXPANDIDAS
NO ECOSSISTEMA DIGITAL
XI SIMPÓSIO NACIONAL DA ABCIBER
21 A 24 DE NOVEMBRO DE 2018
UFJF - JUIZ DE FORA | MG

O MARKETING DIGITAL COMO INSTRUMENTO DE CONTROLE NAS REDES SOCIAIS[1]

Luiz Agner[2]; Juliana Hofstetter[3]

Resumo:

Este trabalho procura analisar aspectos do modo de atuação do controle e do poder exercido pela vigilância na sociedade digital. A discussão proposta envolve a ética, a segurança e o potencial de controle dos algoritmos de aprendizado de máquina, que não só coletam dados dos usuários, mas os armazenam, combinam, analisam e criam padrões que revelam tendências a serem empregadas em estratégias digitais para gerar mais consumo e até influenciar decisões político-eleitorais. As tecnologias que usam inteligência artificial permitem que a persuasão seja construída de forma individualizada, criando um novo sistema de controle social e de manipulação da percepção. São discutidos empregos de algoritmos durante o debate político, assim como o escândalo do vazamento de dados de usuários na rede social Facebook. Para isso, aplicou-se o método de pesquisa bibliográfica e documental.

Introdução

Foucault (2016) conduziu suas reflexões para compreender as relações de poder ao longo da história e suas articulações - configurando sociedades disciplinares. O panoptismo foi usado pelo autor para fazer a analogia com um sistema de vigilância total e

---

[1] Artigo apresentado ao Eixo Temático 5: Educação aberta, educação online e aprendizagem no ecossistema digital, do XI Simpósio Nacional da ABCiber.

[2] Professor de Publicidade e Propaganda na FACHA – Faculdades Integradas Hélio Alonso. Doutor em Design (PUC - Rio). E-mail: luizagner@gmail.com

[3] Pós-graduanda em Marketing pela Solbridge International School of Business. Graduada em Publicidade e Propaganda pela FACHA. E-mail: juhofstetter@gmail.com

individualizante, em que a estrutura circular permitiria a observação sistemática dos vigiados, preservando a opacidade dos vigilantes.

Posteriormente, Deleuze (1992) irá teorizar sobre a sociedade de controle e sua formação, ao final do século XX. Em uma espécie de derivação da disciplina, o controle passa a operar em todos os campos da vida social.

Lyon e Bauman (2014) apontam que as armas de sedução do marketing utilizam basicamente os resultados da vigilância digital sistemática, em larga escala. Na vigilância do marketing digital, os bancos de dados, os algoritmos, os aprendizados de máquina e os perfis computacionais buscam a apropriação de dados comportamentais online dos consumidores a fim de dominar o passado, o presente e o futuro dos indivíduos. Segundo Bruno (2006), estamos diante de "máquinas de produzir futuro, de simular cenários, desejos, preferências, inclinações".

Para Domingues (2016), procurar conhecer e controlar o que os cidadãos pensam ou postam nas mídias sociais tem se tornado a estratégia central de marketing e de tomada de decisão a ser praticada por todo tipo de atores, como agentes de publicidade, iniciativa privada, governos, potenciais governantes, movimentos sociais, partidos políticos etc.

É possível dizer que vivemos em uma sociedade em que não se perde apenas a privacidade, mas também a liberdade de diferentes maneiras, em que o monitoramento avassalador e globalizado se tornou bem-vindo para as corporações e gigantes da internet.

Este artigo procura discutir aspectos do modo de atuação do controle e do poder exercido pela vigilância na sociedade digital. A discussão proposta envolve a ética, a segurança e o potencial de controle dos algoritmos online, que não só coletam dados dos usuários, mas os armazenam, combinam, analisam e criam padrões que revelam tendências a serem empregadas em estratégias digitais para gerar consumo e até influenciar decisões político-eleitorais. Para isso, aplica-se a metodologia de pesquisa bibliográfica e documental. São mencionados empregos de robôs durante o debate político brasileiro, assim como descrito o escândalo do vazamento de dados de usuários na rede social Facebook.

Por dentro da inteligência artificial

Atualmente há uma extensa corrida pelo emprego da inteligência artificial (IA) entre as grandes empresas da internet. O interesse cresce na mesma proporção do investimento em

pesquisa pura nesse campo. Há uma guerra em curso entre as companhias de tecnologia para atrair os melhores talentos da área, devido ao seu potencial econômico de crescimento futuro e ao ritmo promissor das inovações. Pesquisadores e cientistas da IA têm encontrado, por enquanto, nas empresas, um ambiente de liberdade de pesquisa e de publicação, com conferências, conversas com pares, flexibilização de propriedade intelectual, num clima próximo ao do mundo acadêmico. Nesse sentido, estas empresas têm trabalhado na mesma direção das universidades, em busca de respostas a problemas de pesquisa fundamentais.

O campo da inteligência artificial busca estudar princípios matemáticos do aprendizado que podem ser aplicados a computadores. Segundo Yoshua Bengio (2019), um programa tradicional de computador representa um processo passo-a-passo que insere na sua memória um conhecimento previamente existente. Mas o computador também pode ser programado para desenvolver a habilidade de aprender: por isso, o programa de aprendizado é, na verdade, um metaprograma. É como se ele recebesse uma receita de propósito geral que habilita o aprendizado, sendo que a única diferença serão os dados — os exemplos do mundo real com os quais o computador tem contato. Ou seja, os humanos podem ensinar às máquinas, mostrando-lhes exemplos, representados pelos dados.

Para Bengio (2019), o aprendizado humano não se limita à leitura de livros, ao acúmulo de fatos ou dados; é uma adaptação que acontece em resposta a estímulos do ambiente. O aprendizado significa integrar informações que obtemos pela experiência em abstrações que nos permitem tomar melhores decisões, compreender as conexões entre as coisas que vemos, e predizer o que acontecerá em seguida. Em inteligência artificial (IA) trabalha-se com a noção de generalização: a máquina pode generalizar a partir de coisas que já tenha visto e aprendido para novas situações, em um processo lento e gradual, totalmente baseado na experiência, através do contato com um grande volume de dados. É o que se chama aprendizado de máquina ou aprendizado estatístico.

Bengio (2019) cita alguns exemplos disruptivos de áreas de aplicação da inteligência artificial: a produção industrial, a medicina, o transporte, a agricultura, assistentes pessoais, traduções, reconhecimento de voz, reconhecimento facial, etc. Isto tudo poderia levar ao crescimento econômico e a maior progresso material para todos. Entretanto, entre perigos e ameaças antevistos estão: sistemas ubíquos de vigilância, robôs e armas autônomas para uso militar, reforço de discriminações com aumento do desemprego, maior concentração de poder

e mais desigualdades sociais, manipulações publicitárias ou visando a que pessoas mudem o seu comportamento. O potencial de ameaças ao futuro ainda é difícil de definir, pois esse tipo de inteligência de máquinas atualmente é limitado e focalizado em tarefas bastante específicas.

O aprendizado de máquina (*machine learning*) tem emergido como um tópico de grande interesse dentro do campo da pesquisa em inteligência artificial. Segundo Honda, Facure e Yaohao (2019), o aprendizado de máquina ocorre quando um sistema computacional busca realizar uma tarefa aprendendo a partir de experiências, procurando assim melhorar a sua performance. Um algoritmo de IA pode aprender a atingir seu objetivo a partir de um grande volume de dados que representam as experiências. Quanto mais dados, mais exemplos de padrões que o computador pode generalizar para tomar melhores decisões, em situações ainda não vistas. Entre as abordagens para o aprendizado de máquina podem ser citados o aprendizado supervisionado, o aprendizado não-supervisionado e o aprendizado por reforço.

O aprendizado supervisionado tem sido a área da inteligência artificial onde se concentra o maior número de pesquisas, experiências e de produtos bem sucedidos, e onde a maior parte dos problemas já estão bem definidos. De acordo com Honda, Facure e Yaohao (2019), a característica básica de sistemas de aprendizado supervisionado é que os dados utilizados para treiná-los contém a resposta desejada. Ou seja, os dados são previamente anotados com as respostas ou classes a serem previstas. Dentre suas técnicas mais conhecidas estão a regressão linear, regressão logística, redes neurais artificiais, árvores de decisão, entre outras.

No caso do aprendizado não supervisionado, nem todos os problemas podem ser resolvidos desta forma. Em alguns casos, conseguir dados previamente anotados é extremamente custoso ou impossível. Nesses casos, deve-se observar nos registros e dados se existem padrões repetidos que permitiriam a inferência de classes, perfis ou categorias. De uma forma geral, o aprendizado não supervisionado busca uma representação informativa mais simples dos dados, condensando a informação existente em pontos relevantes.

Exemplos de aplicações de aprendizado não supervisionado são sistemas de recomendação de filmes ou músicas, detecção de anomalias e visualização de dados. Dentre as técnicas conhecidas estão as redes neurais artificiais, expectativa-maximização, clusterização hierárquica, análise de componentes principais, entre outras. Problemas de

aprendizado não supervisionado são consideravelmente complexos. Como consequência, esse modelo está na fronteira do conhecimento atual em aprendizado de máquina.

A terceira abordagem de aprendizagem de máquina é a chamada aprendizagem por reforço, em que a máquina tenta aprender qual é a melhor ação a ser tomada, dependendo das circunstâncias na qual esta ação será executada. Esta técnica leva em consideração a incerteza e incorpora eventuais mudanças no ambiente para o processo de tomada da melhor decisão. Baseia-se na psicologia behaviorista de Skinner: com o tempo e a repetição de experimentos, espera-se que o agente consiga associar as ações que geram maior recompensa para cada situação que o ambiente apresenta, e passe a evitar as ações que geram punição ou recompensa menor. Isto aplicado à realidade computacional implica que a máquina observa um "estado da natureza", dentre um conjunto de cenários possíveis, e, com base nisso, escolhe a ação a se tomar. Em seguida, recebe a recompensa associada a esta ação, nesse estado específico, obtendo assim a informação desta combinação. O processo se repete até que o computador seja capaz de escolher a melhor ação para cada um dos cenários possíveis (HONDA, FACURE, YAOHAO, 2019).

Algoritmos e vigilância digital

Orientadas por abordagens de inteligência artificial e aprendizado de máquina, aplicados ao marketing, as capacidades tecnológicas das redes constituem mecanismos que começaram a penetrar no próprio núcleo dos princípios democráticos das sociedades. Mais do que isto, a solução praticada na web de captura, processamento, cruzamento e classificação de informações começa a interferir em outras escalas da vida dos indivíduos, produzindo um novo modelo de controle social. Ao se conectar ao Facebook, por exemplo, os usuários concordam em entregar muitos dos seus dados pessoais, e o resultado disso é que governos, megaempresas ou outros atores podem reunir informações robustas para influenciar, por exemplo, o mercado financeiro ou a opinião pública, ao redor do mundo.

O temor da distopia tecnológica de vigilância em construção nas redes sociais costuma ser associado a processos de panoptismo, originalmente abordados por Michel Foucault (2013). O autor descreve o Panóptico como o "local privilegiado para tornar possível a experiência com homens e para analisar com toda certeza as transformações que se pode obter

neles.” Para o filósofo:

> O Panóptico funciona como uma espécie de laboratório de poder. Graças a seus mecanismos de observação, ganha em eficácia e em capacidade de penetração no comportamento dos homens (FOUCAULT, 2013).

Sempre que existir uma “multiplicidade de indivíduos a que se deve impor uma tarefa ou um comportamento” diz o autor, “o esquema panóptico poderá ser utilizado.” Cabe ressaltar que, da mesma forma que os mecanismos tecnológicos de rastreamento de dados e de práticas algorítmicas, o panoptismo se baseia num modo de atuação fundamentado na visibilidade dos vigiados em contrapartida à invisibilidade dos vigilantes:

> Para se exercer, esse poder deve adquirir o instrumento para uma vigilância permanente, exaustiva, onipresente, capaz de tornar tudo visível, mas com a condição de se tornar ela mesma invisível (FOUCAULT, 2013).

Dessa forma, o filósofo nos apontou o diagrama do Panóptico como sendo um modelo de tecnologia de utilização genérica, com o objetivo de otimizar e aperfeiçoar o exercício do poder, incluindo desdobramentos aplicados a sociedades futuras:

> Com o panoptismo, temos a disciplina-mecanismo: um dispositivo funcional que deve melhorar o exercício do poder tornando-o mais rápido, mais leve, mais eficaz, um desenho das coerções sutis para uma sociedade que está por vir (FOUCAULT, 2013).

Segundo Tufekci (2018a), as tecnologias panópticas que hoje empregam algoritmos de inteligência artificial permitem que a arquitetura da persuasão, no universo online, seja construída de forma individualizada, a exemplo das que suportam modelos de negócios como o do Facebook, Google, Amazon ou Alibaba.

Os dados que o Facebook coleta de bilhões de pessoas são meios de executar e desenvolver seu modelo de negócio, não só para vender publicidade. A coleta de dados é um recurso essencial que pode ser compartilhado por parceiros desenvolvedores para criarem jogos, questionários e aplicativos que mantêm usuários conectados e interessados em voltar à rede, num sistema deliberadamente projetado para que se passe o maior tempo possível nele. Do recurso também podem se beneficiar as agências de publicidade e consultorias de marketing político.

Revisitando o caso Cambridge Analytica

Em 2018, a maior rede social do mundo esteve envolvida em um dos maiores escândalos da história da América, acusada de não proteger os dados de seus usuários. Sob fortes críticas, iniciou-se, ao redor do mundo, um movimento de abandono da rede social, apoiado por personalidades internacionais.

Mark Zuckerberg, fundador da empresa, teve que se explicar em audiências no Senado e na Câmara de deputados dos EUA. O CEO do Facebook admitiu falhas da rede e uma grande quebra de confiança com seus usuários e prometeu trabalhar para assegurar a segurança dos dados pessoais no futuro. O problema é que Zuckerberg tem repetido sistematicamente o mesmo discurso a cada nova crise de confiança.

O caso mais controvertido envolveu a Cambridge Analytica, uma empresa britânica de marketing político, que prestou serviços para a campanha presidencial de Donald Trump em 2016, a partir da identificação de perfis eleitorais de usuários do Facebook (Tufekci, 2018). Dois anos antes, a empresa extraiu dados de 270 mil perfis que baixaram o aplicativo de teste de personalidade *thisisyourdigitallife* e, mais do que isso, recolheu dados dos amigos conectados a esses perfis, totalizando cerca de 87 milhões de usuários, sem que eles fossem avisados (Fake America…, 2018). Com um investimento de um milhão de dólares no desenvolvimento de algoritmos visando ao tratamento desses dados, a C.A. projetou uma campanha política explorando fragilidades emocionais, perfis de personalidade e até mesmo a suscetibilidade dos usuários ao medo.

Christopher Wylie, ex-funcionário da empresa, reuniu a imprensa britânica e demonstrou o uso dos dados pessoais dos usuários. No papel de *whistleblower,* apontou responsabilidades da consultoria inglesa Cambridge Analytica e da própria rede social. Segundo a investigação da comissão parlamentar da Inglaterra, o experimento de manipulação da opinião pública norteamericana se deu com base em três empresas que compartilhavam o mesmo endereço em Los Angeles: Breitbart News, um site de extrema direita especializado em *fake news* e desinformação; Glittering Steel, uma produtora de vídeos para campanhas publicitárias; e a empresa SCL (Strategic Communication Laboratories), entidade mantenedora da consultoria de processamento de dados Cambridge Analytica. Estas empresas eram ligadas ao bilionário ultraconservador Robert Mercer e ao especialista em mídias sociais Steve Bannon, um declarado simpatizante de ideias de extrema direita. Nesse endereço, se

desenrolou a parte obscura da campanha presidencial de Trump: a SCL compilou e analisou bilhões de dados de usuários com o objetivo de identificar o que determinava e motivava o comportamento emocional do eleitor (Fake America…, 2018).

A SCL havia sido fundada, há 25 anos, com quatro vertentes: publicitária, militar, eleitoral e analítica; a empresa especializou-se em *op-psy* (no jargão militar, as operações psicológicas). A empresa planeja e executa ações que visam a influenciar comportamentos, através da manipulação da opinião pública. Entre seus clientes encontram-se a OTAN, o Ministério da Defesa Britânico, a National Security Agency (NSA) e o Departamento de Estado norteamericano, entre outros. A SCL teve a oportunidade de auxiliar o Departamento de Estado a identificar líderes de opinião no Afeganistão para facilitar a intervenção norte-americana no país. Um dos objetivos seria manipular as pessoas, sem que elas percebam, para que se comportem de acordo com objetivos preestabelecidos, uma prática utilizada por regimes totalitários.

A mensagem institucional no site da Cambridge Analytica afirmava que eleições são vencidas quando se conseguem mobilizar votos específicos, considerados cruciais. Por isso, seria necessário enviar a mensagem certa, à pessoa certa, no momento certo, em vez de gastar fortunas com anúncios ou *spam* sob a forma de emails. Esse foi o modelo que a empresa se comprometeu a exercer com sua técnica de modelagem de dados. Mas a realidade era mais complexa: a empresa executou uma operação inédita e mapeou bilhões de dados da população americana, de forma oculta (Fake America…, 2018). Os usuários da internet deixam diariamente bilhões de dados pessoais na rede: endereço, idade, renda, passatempos, religião, compras, se possui ou não arma de fogo. A consultoria comprou outras informações legalmente de cartões de crédito, bancos, previdência e também de gigantes da internet. Assim, conseguiu reunir até cinco mil informações de cada um dos 230 milhões de cidadãos adultos que vivem nos EUA.

Enquanto empresas de marketing tradicionais usam dados demográficos e geográficos para segmentar eleitores em públicos-alvo, a Cambridge Analytica combinou e processou com algoritmos mais de 5.000 tipos de informações incluindo nacionalidade, opinião política, comportamento de consumo e estilo de vida, relacionados a cada eleitor nos EUA. Mais do que isso, criou perfis com base nos dados psicológicos de personalidade, consciência,

extroversão, amabilidade e neurose, capazes de identificar aspectos como motivação e senso de organização. Com base em tecnologias disruptivas de aprendizado de máquina, os seus algoritmos trabalharam rastreando e analisando, além de dados pessoais, as curtidas, comentários, amizades e posts de usuários do Facebook para categorizar suas opiniões políticas, convicções religiosas, personalidade, inteligência, grau de satisfação, orientação sexual, etc. Isto a ajudou a criar uma classificação precisa de cada eleitor e dos temas que lhes despertam maior engajamento emocional. Os resultados dessas experiências foram impressionantes. Estudos demonstraram que, com dez *likes* analisados no Facebook, o algoritmo de IA pode prever reações de um usuário de modo mais preciso que um colega de trabalho; com cem *likes* processados, o conhece melhor que sua família; com 230 likes, o algoritmo conhece o usuário melhor que o próprio cônjuge. A técnica empregada se baseia na psicometria, ciência das medidas psicológicas, ensinada na Universidade de Stanford (Fake America…, 2018).

A ferramenta para atingir o eleitor qualificado utilizou o chamado *dark ad*: uma mensagem hiperpersonalizada que não é revelada para os demais usuários, de tal modo que um jornalista não saberia que esta existiu pois não é pública e será apagada em seguida. A partir disso, foi possível à C.A. definir estratégias precisas de *micro-targeting,* com o direcionamento de mensagens individuais produzidas por psicólogos, analistas de dados e especialistas em campanhas, contemplando valores éticos e reações emocionais.

Com a estratégia de uso da massa de dados, a consultoria C.A. propôs seus serviços ao candidato Donald Trump, pelos quais recebeu cerca de 11 milhões de dólares. Assim, mesmo perdendo as eleições a nível nacional, a campanha se concentrou estrategicamente nos grandes eleitores em estados-chave – Michigan, Wisconsin e Pensilvânia – trabalhando com a reversão do voto de pessoas indecisas. Os afro-descendentes foram especificamente endereçados nesta campanha. A empresa conseguiu definir 32 tipos de perfis de personalidade, em diversas partes do país, aos quais enviou centenas de milhares de mensagens individualizadas nos três estados-chave, visando pessoas nervosas ou inquietas e, portanto, propensas a sensibilizar-se com uma carga de ansiedade maior contida nas mensagens pró-Trump. Desta forma, cerca de 77 mil votos somados nos três estados-chave deram a vitória ao candidato do Partido Republicano, embora este tenha recebido, nacionalmente, três milhões de votos a menos. Uma tática minuciosamente engendrada para

ganhar, baseada nas particularidades do escrutínio indireto americano (Fake America…, 2018).

Podemos observar que o escândalo Cambridge Analytica compõe o desdobramento natural do modelo de negócios do Facebook, que tem submetido as interações dos indivíduos ao seu silencioso e sofisticado sistema de vigilância, com captura detalhada de dados e de metadados, para mantê-los o maior tempo possível na rede, clicando em anúncios. Isto tem permitido à gigante da internet gerar sua capitalização de mercado de mais de meio trilhão de dólares (TUFEKCI, 2018).

Ressalta-se ainda que, mais do que coletar dados comportamentais na web, o Facebook os mescla com dados *offline,* como compras em lojas físicas. Além disso, segundo o jornal New York Times, o Facebook compartilha dados com mais de 150 empresas – entre elas de tecnologia, fabricantes de automóveis e organizações de mídia – com o objetivo de atrair usuários e aumentar a receita de publicidade. Os maiores parceiros recebem acesso muito mais invasivo que o da Cambridge Analytica. Empresas como Yahoo, Netflix, Spotify, Microsoft, Rotten Tomatoes, Amazon e Huawei foram algumas que receberam acesso aos recursos. A parceria incluiu mensagens trocadas pelos usuários no Facebook Messenger, além de nomes, gênero, fotos de perfil, e-mail, telefone, entre outros dados, sem o conhecimento ou consentimento dos usuários (VALENTINO-DEVRIES, 2019).

Zuboff (*apud* Singer, 2019) sugere que as inovações dos serviços digitais propostas pelo Facebook, entre outras grandes empresas, conformam uma espécie de "capitalismo de vigilância". Ela argumenta que serviços desenvolvidos pelas gigantes representam uma forma de mercado problemática que se baseia em comercializar futuros comportamentais. Esse novo tipo de capitalismo teria sua engrenagem operada na opacidade, no sigilo corporativo e na força tecnológica, com perspectivas nocivas para a coletividade. Críticos também advertem que notícias falsas e manipulação de dados, como o revelado no escândalo envolvendo a Cambridge Analytica, são sintomas, sendo que a verdadeira doença seria o controle econômico sobre a comunicação social.

Mesmo com graves acusações de vazamento de dados de usuários nos EUA e a consequente possibilidade de manipulação, o Facebook (e sua plataforma de mensagens

instantâneas, o Whatsapp) não deixaram de exercer papel fundamental, talvez decisivo, desta vez nas eleições presidenciais do Brasil.

Desde 2014, a crescente influência digital entrou em disputa por empresas que mapearam perfis de eleitores, com algoritmos capazes de ler em português e de processar toneladas de informações. É o caso da Stilingue, por exemplo, empresa que conta com 35 desenvolvedores em Ouro Preto (MG), que monitoram as redes sociais e conteúdos publicados na imprensa. O roteiro brasileiro foi parecido: exploração do medo, desejos, ambições e utilização de *fake news* e *social bots* (MOTA, 2018). Durante a campanha de 2018, pressionado pelos escândalos internacionais, o Whatsapp (e o seu proprietário Facebook) baniram diversas contas de perfis automatizados associadas às agências de publicidade brasileiras Quickmobile, Yacows, Croc Services e SMS Market, por motivo de suspeita de práticas eleitorais ilegais (MELLO, 2018).

”Devemos todos apenas sair do Facebook?” pergunta-se Tufekci (2018), mas talvez a resposta não seja tão simples. Dados digitais são a nova energia da sociedade e da democracia influenciando o modo como nos comunicamos e trocamos informações. As redes sociais têm importante papel na sociedade do século XXI, tornando possível a existência de comunidades que se organizam em prol de causas legítimas e importantes, possibilitando campanhas e dando voz a ativistas, voluntários, movimentos políticos e à organização de protestos.

Embora denúncias do potencial efeito negativo causado pela prática de coleta de dados do Facebook esteja desencadeando a formulação de leis ao redor do mundo, a exemplo do do *General Data Protection Regulation* (GDPR) ou a lei brasileira de proteção de dados (LGPD), e a rede social se comprometa a ser transparente no uso desses dados, isoladamente isto não resolveria o problema, questiona-se Tufekci (2018), pois os dados já estão comprometidos. O que o Facebook coleta de bilhões de pessoas são meios de executar e desenvolver seu modelo de negócio, não só para vender publicidade. A coleta é também um recurso essencial que pode ser usada por desenvolvedores para criarem jogos, questionários e aplicativos que mantêm os usuários conectados e interessados em voltar à rede.

A discussão hoje inclui enxergar mais do que o uso ilegal de dados pessoais pela Cambridge Analytica ou as consequências deletérias nas eleições. O principal problema é que bilhões de dólares estão sendo ganhos às custas da esfera pública e política, e decisões

cruciais estão expostas ao alinhamento com interesses unilaterais, sem qualquer recurso de proteção ou responsabilidade. Mais do que a construção de uma distopia em favor do marketing e do lucro, as informações filtradas que os algoritmos de inteligência artificial organizam na *timeline* de cada usuário do Facebook tornam, aos poucos, o debate público impossível, ao apresentar conteúdos tóxicos que nos levam gradativamente à polarização e à intolerância (TUFEKCI, 2018).

Pontos para reflexão

Somente agora começamos a identificar e a abordar os problemas levantados pela rápida introdução dos algoritmos de inteligência artificial e *machine learning* em áreas importantes no âmbito social. A partir dos escândalos trazidos pelo emprego da IA em 2018, questões fundamentais emergiram para reflexão: quem será responsabilizado quando sistemas de aprendizado estatístico começam a prejudicar os cidadãos? O *gap* de responsabilidade torna-se presente quando se observa o atual emprego crescente dos algoritmos para amplificar a vigilância digital sobre a sociedade, no âmbito do marketing ou da política, especialmente em associação a tecnologias disruptivas com potencial de maximizar o controle social e, possivelmente, no caso de alguns governos, a opressão. Grandes players do mercado de internet precisam estar atentos e se responsabilizar pelas consequências do uso indiscriminado de suas tecnologias.

Algoritmos de *machine learning* têm contribuído amplamente para ampliar a vigilância social generalizada. Isso ocorre não somente com o rastreamento de dados dos usuários pelo marketing, mas também com o emprego crescente de redes de sensores, manipulação de percepções, reconhecimento facial e usos panópticos das redes sociais. Há o perigo de novas ameaças, ao mesmo tempo em que se ampliam preocupações antigas, exaustivamente discutidas por autores como Foucault, Deleuze, Bauman, Lyon, entre outros. O emprego de técnicas de reconhecimento afetivo é outra ameaça em ascensão, habilitado pelo aprendizado de máquina, e tem incentivado tentativas de leitura de emoções íntimas através da análise detalhada de rostos, com alegações espúrias sobre a saúde mental e a culpabilidade de indivíduos. Algumas tecnologias de IA podem ser usadas para fins discriminatórios, preconceituosos ou antiéticos, sem o conhecimento das pessoas envolvidas, por

empregadores, governos ou instituições pouco democráticas, representando sérios riscos aos direitos humanos e às liberdades civis em diversos países.

Pasquale (2015) nos alerta que só agora estão sendo investigadas as consequências humanas de uma sociedade tecnológica cada vez mais orientada por grandes volumes de dados e por algoritmos de inteligência artificial. O problema é que estas técnicas e ferramentas estão hoje encapsuladas em caixas pretas, guardadas como segredos comerciais, a que os cidadãos não têm acesso e cujo funcionamento não podem compreender.

Sendo assim, como mitigar os efeitos prejudiciais da prática algorítmica? Dada a importância do tema, tornam-se necessários mais estudos que desenvolvam uma maneira de todos sermos capazes de compreender e estabelecer limites à manipulação de dados de nossas vidas. A resposta à "sociedade da caixa preta", segundo Pasquale (2015), precisa ser a total transparência e o consentimento informado: revelar os algoritmos e aprovar o uso de cada dado, com o propósito de reforçar a transparência e mesmo de evitar o seu uso em determinados casos sensíveis.

Desde as considerações de Foucault e Deleuze, não se alterou o objetivo de vigiar, pelo contrário, este foi ampliado e pluralizado, à medida que as possibilidades da internet e das redes foram sendo descobertas. As novas tecnologias de poder se desenvolveram inevitavelmente associadas ao desenvolvimento contemporâneo do marketing. O acesso de governos e de empresas a dados de indivíduos no mundo inteiro só fez aumentar -- com ou sem o seu consentimento prévio - o que configura um dos aspectos mais perturbadores e relevantes do que Domingues (2016) propôs chamar de "Publicidade de Controle".

Se, por um lado, são inegáveis as vantagens dos recursos tecnológicos e das redes de informação, e muito pode ser citado nesse sentido (inovações na educação, conectar pessoas, reconectar amigos distantes, mobilização e engajamento em causas sociais, facilidade em pesquisas, liberdade de expressão, rapidez na informação, etc), por outro, os usos estatísticos e exponenciais que as empresas fazem de dados pessoais de bilhões de indivíduos, e demais rastros deixados na rede, despertam a atenção para perigos, vulnerabilidades e restrições a que pessoas vêm sendo submetidas.

O Facebook, como a maior rede social da atualidade, é um dos principais responsáveis por influenciar massivamente o comportamento e decisões de quem utiliza suas ferramentas, principalmente no que diz respeito ao incentivo ao consumo de produtos, serviços e

informações. Assim, o interesse das marcas e empresas em estar presente no espaço digital para aproveitar as possibilidades do *big data* produz um efeito colateral antidemocrático no que diz respeito à manipulação dos desejos, da percepção e das emoções.

Cabe ressaltar que um dos efeitos da era digital foi o enfraquecimento dos *gatekeepers* tradicionais, como a mídia e a academia, em prol de novos *gatekeepers* algorítmicos. Ao mesmo tempo que fortaleceu algumas abordagens e visões alternativas, as redes sociais as desempoderou na medida em que produziu uma esfera pública confusa, poluída e repleta de ruídos, onde proliferaram discursos extremistas e desinformação. Para Tufekci (2018b), os novos *gatekeepers* algorítmicos não apresentaram a desejada neutralidade, uma vez que seus modelos de monetização e financiamento incentivam fortemente as preferências enviesadas, assim como conteúdos de polarização e ódio que garantem cliques e capturam a atenção.

A solução, segundo Tufekci (2018), deveria ir além das simples regulamentações legislativas de proteção de dados, e dar o direito concreto aos usuários de limitar - sem longas páginas de termos - o uso de suas informações pessoais, ou até mesmo de ter acesso aos dados que as empresas coletaram, tudo de forma simples e verdadeiramente consensual. Para a autora, é indispensável que o debate não seja postergado, e que a economia digital seja forçada a mudar, trazendo ao mercado não só mais proteção, mas também mais inovações.

Ao que tudo indica, quase nenhum setor da sociedade restará imune aos efeitos causados pela atuação dos sistemas online e algoritmos de inteligência artificial — do consumo à informação, do comportamento social ao posicionamento político-ideológico. Os dados digitais, processados em gigantescos volumes, pelo aprendizado de máquina, serão a nova energia da sociedade e da democracia, influenciando o modo como nos comunicamos, trocamos informações, e como construímos consensos.

Isto não é em si ruim, mas os grandes players da tecnologia não podem fugir à sua responsabilidade e ao controle ético da sociedade.

Palavras-chave: Sociedade de controle; vigilância; marketing; machine learning; Facebook.

Referências

BAUMAN, Zygmunt. **Vigilância Líquida: Diálogos com David Lyon**. Rio de Janeiro: Zahar, 2014. Introdução por: David Lyon; Tradução de: Carlos Alberto Medeiros.

BENGIO, Yoshua. **Yoshua Bengio on intelligent machines.** Disponível em: <https://youtu.be/ePUSElR0o9o>. Acesso em 07 janeiro 2019.

BRUNO, Fernanda. **Máquinas de ver, modos de ser: visibilidade e subjetividade nas novas tecnologias de informação e de comunicação.** Revista Famecos, [s.l.], v. 11, n. 24, p.110-124, 12 abr. 2008. EDIPUCRS. http://dx.doi.org/10.15448/1980-3729.2004.24.3271. Acesso em: 08 set. 2017.

DELEUZE, Gilles. **Política: Post-Scriptum sobre as sociedades de controle.** In: _____. Conversações: 1972-1990. São Paulo: 34, 1992. Cap. 5. p. 219-226. Tradução de: Peter Pál Pelbart.

DOMINGUES, Izabela. **Publicidade de Controle: consumo cibernética, vigilância e poder**. Porto Alegre: Sulina, 2016. 337 p.

FAKE America Great Again. Ogum Filmes. Disponível em: < https://vimeo.com/295576715>. Acesso em 17 Outubro 2018.

FOUCAULT, Michel. **Microfísica do poder.** 4. ed. Rio de Janeiro | São Paulo: Paz e Terra, 2016. Organização, Introdução e Revisão técnica de: Roberto Machado.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão.** 41a. ed. Petrópolis, RJ: Vozes, 2013.

MELLO, Patrícia C. **Whatsapp notifica agências que disparam mensagens anti-PT**. Disponível em: <https://www1.folha.uol.com.br/poder/2018/10/whatsapp-notifica-agencias-que-disparam-mensagens-anti-pt.shtml > Acesso em: 30 janeiro 2019.

MOTA, Camilla Veras. **Robôs e 'big data': as armas do marketing político para as eleições de 2018.** 2017. Disponível em: <https://www.bbc.com/portuguese/brasil-41328015>. Acesso em 20 dezembro 2018.

PASQUALE, Frank. Introdution: The Need to know. In: PASQUALE, Frank. **The Black Box Society: The Secret Algorithms That Control Money and Information.** London: Harvard University Press, 2015. Cap. 1. p. 1-18. Disponível em: raley.english.ucsb.edu/ wpcontent/ Engl800/ Pasquale-blackbox.pdf. Acesso em: 5 nov. 2017.

SINGER, Natasha. **The Week in Tech: How Google and Facebook Spawned Surveillance Capitalism.** The New York Times. New York. Disponível em: <https://www.nytimes.com/2019/01/18/technology/google-facebook-surveillance-capitalism.html> Acesso em: 15 janeiro 2019.

TUFEKCI, Zeynep. **Facebook's Surveillance Machine.** The New York Times. New York. Disponível em: <https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html>. Acesso em: 6 jul 2018.

TUFEKCI, Zeynep. **How Social Media Took Us From Tahir Square to Donald Trump.** MIT Technology Review. Disponível em: < https://www.technologyreview.com/s/611806/how-social-media-took-us-from-tahrir-square-to-donald-trump/>. Acesso em: 1 setembro 2018.

VALENTINO-DEVRIES, Jennifer. **5 Ways Facebook Shared Your Data.** The New York Times. New York. Disponível em: <https://www.nytimes.com/2018/12/19/technology/facebook-data-sharing.html> Acesso em: 27 jan. 2019.