

## Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância

---

Adriana Veloso Meireles<sup>1</sup> 

---

O fenômeno do monitoramento automatizado das experiências privadas, realizado por algoritmos inteligentes, com a intenção de induzir certos comportamentos, é conceituado na literatura como capitalismo de vigilância. O artigo acrescenta alguns elementos a essa teoria a partir dos seguintes argumentos: a falta de transparência dos algoritmos impossibilita inferir com precisão sua capacidade de modulação comportamental; a formação das preferências é um processo complexo e maleável, que abrange estratégias de resistência e subversão; para que a dominação ocorra, é necessário que haja conformidade dos dominados, o que não se observa a partir de marcos normativos em vigência; por fim, o exercício do poder é diferente de sua capacidade de influência. A partir desses pontos, conclui-se que é necessário regular o próprio funcionamento dos algoritmos como complemento à proteção de dados pessoais.

*Palavras-chave:* capitalismo de vigilância; privacidade; democracia; algoritmos; neoliberalismo

### Introdução

A humanidade nunca registrou e armazenou tantas informações como nos últimos anos. São dados gerados em diversos formatos – texto, imagem, vídeo, áudio –, por diferentes tecnologias, que vão de drones ao reconhecimento facial, do cartão de crédito aos mais diversos tipos de sensores, de temperatura, de movimento, entre outros. O ponto central é que a forma de registro dessas informações transforma-se radicalmente na passagem do analógico para o digital.

É nesse contexto que o direito à privacidade deixa de ser suficiente para lidar com a quantidade de informações pessoais produzidas pela sociedade contemporânea. O direito à proteção de dados pessoais emerge, portanto, para salvaguardar os indivíduos do uso indevido de suas informações, não apenas para fins de vigilância, como muitas vezes o tema é abordado, mas também para influenciar hábitos de consumo, preferências políticas, interferindo diretamente no exercício da cidadania e na autodeterminação informacional.

---

<sup>1</sup> Universidade de Brasília. Instituto de Ciência Política. Brasília (DF), Brasil.  
E-mail: <[dricaveloso@gmail.com](mailto:dricaveloso@gmail.com)>.

O dado pessoal passa a ter uma tripla natureza: refere-se ao indivíduo, sustenta a construção de políticas públicas e também é a essência da economia da intrusão (Silveira, 2017) ou do capitalismo de vigilância (Zuboff, 2019), conceitos que, em resumo, se referem à prática do tratamento de informações pessoais de forma comercial. Portanto, a regulação da propriedade dos dados é uma das questões contemporâneas mais complexas que a sociedade enfrenta, em face do tratamento indiscriminado de informações pessoais.

A mídia direcionada, o sistema de sugestões e os filtros de conteúdo observados no uso da internet e de aplicativos são exemplos cotidianos em que os algoritmos atuam na tentativa de influenciar as escolhas individuais. Os dados pessoais são coletados, extraídos, analisados, processados e tratados por máquinas para finalidades pouco transparentes. Algoritmos simples ou inteligentes analisam, comparam e tratam informações dos mais variados formatos a todo momento. A principal diferença entre eles é que, enquanto os algoritmos são códigos computacionais escritos para resolver problemas específicos, os algoritmos inteligentes – sejam eles chamados de inteligência artificial ou *machine learning* – são programados para solucionar problemas. O próprio programa assimila a resolução, mas, como “eles não aprendem ou raciocinam como os humanos, isso pode fazer com que seus resultados sejam difíceis de prever e explicar” (Tutt, 2016, p. 87). Seus efeitos podem ser simples, como um programa que fecha sem salvar o trabalho feito, mas também podem ser complexos, quando suas consequências incidem diretamente na sociedade.

Nesse contexto, é importante destacar a relevância da dimensão coletiva do tratamento das informações pessoais, que impacta toda a sociedade a partir da transição da coleta de dados do universo digital para o mundo físico. Se inicialmente o tratamento de dados pessoais focava o indivíduo, agora os algoritmos inteligentes querem compreender populações e seus comportamentos (Zuboff, 2019). O problema se intensifica quando as pessoas são objeto de tomadas de decisões realizadas por eles. A falta de transparência sobre seu funcionamento indica a tendência de que esses mecanismos segregam determinadas informações, privilegiando outras, reproduzindo padrões de preconceito e discriminação de gênero, de raça e de renda, entre outras, aprofundando ainda mais as desigualdades da sociedade.

O capitalismo de vigilância é um fenômeno característico da nova ordem neoliberal; o Estado burocrático é visto como limitador da inovação e do empreendedorismo tecnológico. A ausência de regulação desse setor, ancorada em sua estruturação privada, possibilita que empresas atuem fora da lógica liberal de mercado, erguendo um dos maiores monopólios contemporâneos. A lista das dez pessoas mais ricas do mundo em 2018 é um reflexo desse fato (Dolan, 2019). A autorregulação do setor, em contraposição a regras e leis, possibilita o fim da livre concorrência. Cada nova *startup* – para utilizar o jargão do setor – é adquirida por seus conglomerados, antes mesmo que sua tecnologia se comprove inovadora.

O artigo está dividido em quatro seções, além desta breve “Introdução”. Inicialmente, em “A conformação do capitalismo de vigilância”, destaca-se o contexto histórico, cultural, econômico, político e tecnológico, sem precedentes, que possibilitou a conformação do capitalismo de vigilância. O foco da análise é direcionado aos primeiros anos do milênio, quando se observa a convergência entre recursos e regras, ambos necessários para o exercício da dominação (Bourdieu, 2007). É nesse mesmo período que se consolida a transição de um modelo de capitalismo de mercado ao neoliberalismo, marcado pela ausência de regulamentação do setor tecnológico e do mercado financeiro. Além disso, essa mudança tem como característica fundamental a transformação do papel do Estado, que passa a atuar mais em defesa de interesses privados do que na proteção de direitos sociais (Harvey, 2008; Brown, 2015; Fraser, 2009; Laval e Dardot, 2016).

Em seguida, em “Relações de poder: autonomia e resistências”, ao enfatizar a ubiquidade do monitoramento constante de atividades privadas, debate-se o suposto poder preditivo e manipulador dessas tecnologias. Destaca-se que a capacidade de exercício do poder não pode ser igualada à sua influência efetiva. Ressalta-se que o processo de formação das preferências e das escolhas individuais é complexo e abrange estratégias de resistência, muitas vezes “invisíveis”, e decisões “contraditórias” (Scott, 1990; Sunstein, 2009). Nesse contexto, discutem-se as relações de poder e o conceito de autonomia, destacando-se que, para o exercício da dominação, é necessária a conformidade dos indivíduos. Tal concordância é contestada em especial a partir da vigência do Regulamento Geral de Proteção de Dados da União Europeia. Esse marco normativo busca o consentimento informado das pessoas e a revisão dos contratos assimétricos realizados com as empresas de tecnologia. Para ancorar a discussão em um caso empírico, apresenta-se, de forma breve, o estudo de caso das eleições estadunidenses de 2016, em que Benkler, Faris e Roberts (2018) analisam a influência da internet e das mídias digitais no resultado do pleito.

Na terceira seção, “Governança algorítmica”, discute-se o modelo de governança instaurado pela lógica neoliberal, que modifica as características do Estado e suas relações com a sociedade e o capital privado (Laval e Dardot, 2016). Destaca-se que a infraestrutura de telecomunicações foi erguida, em sua maior parte, por empresas, ou privatizada ainda na década de 1990. Essa forma de administração do Estado, que constitui um novo modelo de governabilidade, impõe desafios ao próprio conceito de democracia liberal, já que a economia é que orienta a política, e não o contrário. A partir da problematização do neoliberalismo, recorre-se ao conceito de governança para descrever o modelo de coparticipação entre Estado e corporações privadas, principalmente no setor de telecomunicações e tecnologia. Utiliza-se o termo justamente para sublinhar a necessidade de regular os algoritmos, em especial seus processos decisórios, que reproduzem assimetrias e reforçam desigualdades de gênero, renda e raça, entre outras.

Na “Conclusão”, enfatiza-se que a internet e os meios digitais fazem parte de um ecossistema de mídia composto por outros veículos, caracterizados por uma assimetria de

discursos e interesses (Benkler, Faris e Roberts, 2018). Por outro lado, o monopólio das telecomunicações se transforma diante da conformação da economia de dados. É nesse sentido que se compreende que o “privado” nunca foi tão político como na atualidade.

Por fim, destacam-se características do capitalismo de vigilância, que indicam a necessidade de regulação e transparência dos algoritmos, ou uma governança algorítmica, compreendida aqui como uma necessária complementação aos direitos à privacidade e proteção de dados pessoais (Tutt, 2016).

### **A conformação do capitalismo de vigilância**

O capitalismo de vigilância é um fenômeno que ocorre há pelo menos duas décadas, ainda que o público em geral só tenha tido conhecimento sobre suas práticas com as declarações de Edward Snowden, em 2013. Suas revelações apontaram para uma convergência entre agências de defesa estadunidenses e empresas de tecnologia, a partir dos atentados de 11 de setembro de 2001, em Nova York.

Esse acontecimento fez com que a prioridade do governo estadunidense se tornasse a segurança; portanto, toda regulação relativa a questões de privacidade e proteção de dados pessoais tornou-se irrelevante no contexto de “guerra ao terror”. Essa conjuntura política, econômica e tecnológica, alicerçada em um modelo extremamente neoliberal de regulação, possibilitou a conformação do que Zuboff (2019) descreve como capitalismo de vigilância. Nos anos seguintes, qualquer tentativa de garantir o direito à privacidade era contestada como uma forma de interferência no mercado e na inovação tecnológica. De fato, as grandes empresas de tecnologia conhecidas pelo acrônimo FAMGA (Facebook, Apple, Microsoft, Google e Amazon) sempre realizaram um forte *lobby* junto ao governo estadunidense contra a regulação da proteção de dados pessoais e a privacidade (Molla, 2019).

O fato é que, em cerca de apenas 20 anos, o mercado de tecnologia se consolidou ancorado na coleta e tratamento de dados pessoais (ainda que cada empresa tenha uma abordagem diferente com relação ao tema). Para Zuboff (2019), o Google inaugurou essa prática. Lançado em 1998, o buscador se destacou dos concorrentes por uma série de motivos. O mais perceptível deles era seu aspecto visual, que contava com um *design* minimalista, ou seja, apresentava poucas informações na página, ao contrário de seus rivais à época, Altavista, Yahoo!, entre outros. Aliado a isso, a ferramenta era conhecida por não promover anúncios de forma ostensiva, estabelecendo com as pessoas que a utilizavam uma relação não baseada no consumo, mas na experiência de uso (*user experience*) (Rogers, Sharp e Preece, 2013).

Inicialmente, a empresa utilizava os dados – palavras-chave, padrões de termos de pesquisa, como uma consulta é feita, ortografia, pontuação, tempos de permanência nas páginas, padrões de cliques, localização, entre outros – exclusivamente para melhorar a ferramenta de busca e a experiência das pessoas ao utilizá-la. Essas informações

colaterais alimentavam o algoritmo do Google, em um “processo reflexivo de aprendizagem e melhoria contínuas” (Zuboff, 2019, p. 70). Quanto mais as pessoas utilizavam o buscador, mais relevantes tornavam-se os resultados procurados. O algoritmo original era simples, mas, à medida que foi aprendendo com a experiência dos usuários, começou a se tornar “inteligente”.

No final da década de 1990, sucedeu o fenômeno que ficou conhecido como a bolha da internet. Em resumo, ocorreu uma grande especulação em torno das empresas de tecnologia, que obtiveram um pico de alta em suas ações na bolsa de valores Nasdaq, seguido de uma queda brutal. A decaída dos investimentos levou muitas empresas de tecnologia a decretar falência, ser vendidas ou optar pela fusão. Foi essa situação de pressão que fez os fundadores do Google transformarem o negócio de um simples buscador destinado a organizar a informação da *web* na participação no ramo dos *e-mails*, textos, fotos, vídeos, geolocalização, reconhecimento facial, prevenção de doenças, carros autônomos, mapeamento da lua, entre outras atividades incorporadas pela Alphabet, fundada por eles em 2015.

Diante da crise, renunciaram a uma das regras que haviam adotado até então: a ausência de anúncios. “Se era para ter propaganda, ela deveria ser relevante. A publicidade deveria aparecer de uma forma direcionada a um indivíduo em particular (...), garantindo assim a relevância para as pessoas, e o valor para os anunciantes” (Zuboff, 2019, p. 75). Foi a partir daí que o Google alterou a forma de monetizar a publicidade na internet. O modelo de anúncios com mensalidades fixas foi substituído por taxas de conversão baseadas na quantidade de cliques/acessos ou de visualizações.

O surgimento do *marketing* direcionado promovido pelo Google teve como fundamento uma vantagem mercadológica incontestável: o conhecimento prévio sobre a forma com que as pessoas realizavam buscas em sua ferramenta. Para Zuboff (2019), essa mudança na forma de anunciar é um dos elementos que marcam o início do capitalismo de vigilância.

Em 2003, o Google começou a desenvolver e implantar algoritmos de inteligência artificial, que, assim como outras tecnologias, não possuem um caráter neutro. Nesse mesmo ano, quatro engenheiros da empresa submeteram uma patente intitulada “Gerando informação sobre o usuário para utilização em publicidade direcionada” (Bharat, Lawrence e Sahami, 2009). Em sua descrição, elencaram uma série de maneiras para gerar informações de perfil de usuário (*user profile information* ou UPI). Importante ressaltar que, em 2003, o Google ainda era apenas uma ferramenta de busca. As informações eram coletadas a partir dos endereços IP e de ferramentas simples, como os *cookies*, e não a partir de uma conta pessoal, que centralizasse as informações e facilitasse a identificação dos indivíduos. Essa patente representou também a capacidade da empresa em extrair dados de todas as páginas da internet, ampliando os destinos publicitários para além de sua busca. Essa mudança na forma de vender anúncios ficou conhecida como a “física dos cliques”, e ainda é a principal fonte de lucro da empresa.

O ano de 2003 foi especialmente relevante para o Google devido a outros motivos, em especial por sua aproximação com as agências de segurança estadunidenses. Nesse ano, o Google foi contratado pela Agência Central de Inteligência (CIA) “para customizar uma ferramenta de busca (...) para supervisionar informações supersecretas, secretas, sensíveis e não classificadas para ela e outras agências” (Zuboff, 2019, p. 84). Já a Agência Nacional de Segurança (NSA) contratou a companhia para “criar um algoritmo capaz de pesquisar 15 milhões de documentos em 24 idiomas” (Zuboff, 2019, p. 84). Esses dois contratos marcaram o início da colaboração entre o Google e o governo estadunidense, e constituem a base do capitalismo de vigilância.

A parceria continuou nos anos seguintes. Em 2004, o Google comprou a empresa Keyhole, que havia recebido investimentos da CIA para o mapeamento geográfico do planeta. O resultado foi o lançamento do Google Maps e do controverso projeto *Street View*, no ano seguinte. Essa colaboração entre o governo estadunidense e o Google é considerada sem precedentes, uma das principais características do neoliberalismo, ou seja, o Estado atuando na defesa de interesses privados, em vez de agir na proteção de direitos sociais (Harvey, 2008; Brown, 2015; Fraser, 2009; Laval e Dardot, 2016).

Portanto, se originalmente o Google se empenhava em aprimorar a experiência de seus usuários, a partir dessas transformações, as pessoas, sem o saberem, começaram a trabalhar gratuitamente para a empresa, ampliando seus lucros. Os dados pessoais e as experiências privadas tornaram-se a essência dos dados comportamentais, que, por sua vez, alimentavam os anúncios direcionados. A experiência individual privada converteu-se em fonte de renda das empresas de tecnologia. Ou, como bem resume o diretor executivo da Apple, Tim Cook: “se o serviço é gratuito, você não é o consumidor, mas o produto” (Malkin, 2018). Os dados pessoais transformaram-se em objeto de valor de forma silenciosa, enquanto a maioria das pessoas ignorava o que ocorria.

Para Zuboff (2019), esta é a primeira de três transformações sociais essenciais para compreender como opera o capitalismo de vigilância: a liberdade em explorar um amplo conhecimento sobre o público, sem sofrer interferências. Enquanto as pessoas ignoram de que forma suas informações pessoais são tratadas, esses dados financiam o conhecimento das empresas a seu respeito. O Estado neoliberal não intervém, pelo contrário, é parceiro do setor privado na implementação da infraestrutura tecnológica.

Em segundo lugar, a autora destaca que ocorre um abandono da reciprocidade orgânica com as pessoas, que já não são apenas consumidores, mas também fonte de material bruto para o desenvolvimento de produtos personalizados. O indivíduo é, ao mesmo tempo, consumidor e fonte de informação, fazendo com que a lógica da troca mútua não mais se aplique. Nesse sentido, é importante frisar que essas empresas auxiliam na transformação da força de trabalho, tornando turbulento um balanço secular entre o capitalismo de mercado e as democracias liberais. Para se ter uma ideia, “a General Motors empregou mais pessoas durante o pico da Grande Depressão do que Google e Facebook contratam juntos atualmente” (Zuboff, 2019, p. 468). Não se reduz apenas o

número de postos de trabalho, a lógica da concorrência entre os próprios assalariados, a gestão por metas e a avaliação individualizada do desempenho promovem justamente a precarização e a insegurança no trabalho (Lorey, 2015).

Em terceiro lugar, a indiferença radical em relação à visão coletivista da sociedade é observada quando o conteúdo da informação é julgado pelas empresas a partir de sua relevância em termos de números de cliques e curtidas, volume, profundidade e capacidade de gerar lucro. Não importa se o conteúdo é mentiroso, fraudulento ou contém discurso de ódio, desde que as pessoas cliquem nele. Os valores democráticos são ignorados para sustentar corporações de tecnologia e o sistema financeiro, que migra seus investimentos para esse setor (Dantas, 2019). O conteúdo não é avaliado conforme normas democráticas, como a livre imprensa, ou a liberdade de expressão, mas, sim, a partir dos termos de uso, determinados pelas empresas privadas. A suspensão de contas, ou retirada de conteúdos, dessas plataformas ocorre no tempo em que as próprias companhias determinam como adequado.

As transformações pelas quais o Google passou são centrais para compreender como a proteção de dados pessoais e a privacidade se tornam fundamentais nas democracias contemporâneas. E tudo isso ocorreu antes de 2005. Não havia o Twitter, nem o Facebook, muito menos o iPhone.

A tecnologia móvel representa um novo panorama, que Zuboff (2019) descreve como a segunda fase do capitalismo de vigilância. Sustentado pelo aumento de capacidade de armazenamento, processamento e tratamento de informações, também conhecido como *big data*, esse segundo momento representa a consolidação do monitoramento automatizado das experiências privadas, realizado por algoritmos inteligentes, com a intenção de induzir ou direcionar certos comportamentos.

Nesse contexto, é importante ressaltar que se observa a convergência entre recursos e regras, essenciais para o exercício da dominação (Bourdieu, 2007). Em outras palavras, as empresas de tecnologia possuem os recursos, e o governo não realiza nenhum tipo de intervenção, ou regulação, no setor. A transformação das relações entre o Estado, a sociedade e o sistema financeiro (do qual essas empresas fazem parte) é central para a expansão e consolidação do neoliberalismo.

Os termos de uso das plataformas e aplicativos digitais se caracterizam como consentimentos pouco esclarecidos, inclusive realizados em condições que limitam o exercício da liberdade, dos direitos e de relações mais autônomas (Pateman, 1988). As pessoas aceitam os termos de uso sem compreender bem o que será feito com suas informações pessoais, em troca de um serviço gratuito ou do uso de um aplicativo. O consentimento inicial é seguido de interferências arbitrárias – uma sugestão não solicitada, uma indicação de amizade de alguém que a pessoa odeia são alguns exemplos cotidianos. As empresas de tecnologia constroem as pessoas a aceitar seus termos de uso. É por isso que se questiona a presença do consentimento explícito em acatar esses contratos.

Essa dominação racional (Weber, 1991), amparada nos termos de uso, está longe de ser voluntária, esclarecida e autônoma.

Em contraposição, para que a dominação se perpetue nas relações de poder, é necessária a conformidade dos indivíduos, seja no nível pessoal, seja no nível institucional. No campo de resistência da sociedade civil, observa-se a relevância do uso de *softwares* livres, ou até mesmo de atitudes de sabotagem e outras formas de ação direta. Scott (1990) explica que o discurso público é diferente daquele realizado de forma íntima, e que, por trás de uma aparente conformidade e obediência, os sujeitos realizam constantemente atividades de insubordinação com relação ao poder instituído.

Há ainda uma contestação institucional a partir do Regulamento Geral de Proteção de Dados da União Europeia, em vigência desde 2018. A norma é uma resposta consistente sobre a ausência de regras e limites para a atuação das empresas de tecnologia, com foco no direito à privacidade e à proteção de dados pessoais. A partir de mecanismos de *accountability* – como sanções e multas –, a regra obriga o setor privado a atuar em conformidade com padrões de privacidade e consentimento informado. Além disso, determina uma revisão dos contratos assimétricos realizados entre as pessoas e as empresas, por meio dos termos de uso de seus serviços “gratuitos”.

Justamente por isso, o Regulamento Geral de Proteção de Dados impõe limites e restrições nesses acordos, além de estabelecer o direito da pessoa em suspender o contrato quando quiser, reforçando sua autonomia e autodeterminismo informacional, ou seja, o controle sobre os próprios dados.

Ainda que restrita aos cidadãos europeus, os impactos incidem diretamente na abordagem neoliberal, que privilegia a segurança e o desenvolvimento tecnológico, em detrimento da privacidade. Sobretudo, o Regulamento Geral de Proteção de Dados expõe visões distintas sobre princípios da democracia liberal, em especial com relação à garantia de direitos. Nesse contexto, o próprio conceito de democracia está em disputa, e os diferentes marcos regulatórios – dos Estados Unidos e da União Europeia – demonstram a distinção dessas visões.

Nos Estados Unidos, a privacidade e a proteção de dados pessoais são temas de regulação comercial, abordados como direito do consumidor. A regulação se dá a partir da Federal Trade Commission (FTC), que trata de temas como privacidade de dados (*data privacy*), retirando os sujeitos do protagonismo, ou seja, trata-se da privacidade das informações, não das pessoas. A União Europeia, por sua vez, coloca o Estado no papel de intermediário entre o setor privado e os direitos e liberdades individuais. A autorregulação do primeiro modelo entra em embate direto com leis e regras que buscam conformidade das empresas em relação ao respeito à privacidade e proteção de dados pessoais.

Identificam-se assim, na disputa dos marcos regulatórios, visões bem distintas da própria democracia liberal. Nos Estados Unidos, o monopólio das empresas de tecnologia é questionado a partir do direito à concorrência. O conjunto de leis antitruste do país busca regular o setor privado, proteger os consumidores, restringir a formação de cartéis, entre

outras medidas, para promover o livre comércio. Já na União Europeia, prevalecem marcos regulatórios, como o próprio Regulamento Geral de Proteção de Dados, que privilegiam direitos humanos fundamentais, como a liberdade de expressão e de escolha.

A privacidade é compreendida como fundamental para o exercício desses direitos, inclusive essencial para a conformação das próprias identidades. Nesse sentido, a disputa do entendimento de democracia é marcada por uma visão que coloca a economia e o livre mercado em primeiro lugar e por outra, antagônica, em que os sujeitos são mais importantes.

Pontuadas essas questões, prossegue-se para a próxima seção do artigo em que se debate o conceito de capitalismo de vigilância e modulação do comportamento, com vistas a verificar se eles são suficientemente robustos para descrever os processos sociais vivenciados no uso cotidiano das tecnologias. Parte-se de uma análise do caráter preditivo dos algoritmos inteligentes para destacar sua opacidade. Busca-se problematizar visões determinísticas, em que as pessoas estão sujeitas à manipulação, ao mesmo tempo em que se reconhece que essas tecnologias são projetadas com esses objetivos. Ressalta-se que a capacidade de exercer poder não significa sua consumação e que existem estratégias de resistência em curso.

Por fim, para concluir a seção, debate-se sobre a urgência em regular o modo de funcionamento dos algoritmos inteligentes, como parte da proteção de dados pessoais e defesa do direito à privacidade. Nesse contexto, a governança algorítmica se torna imperativa diante do modelo neoliberal de monitoramento automatizado das experiências individuais e coletivas, em especial quando as pessoas estão sujeitas a decisões tomadas por esses algoritmos. Argumenta-se que os algoritmos fazem algo muito mais perverso do que modular comportamentos, eles reproduzem assimetrias que reforçam preconceitos de gênero, raça e renda.

### **Relações de poder: autonomia e resistências**

A segunda fase do capitalismo de vigilância é caracterizada pela expansão das tecnologias móveis, pela geolocalização das informações e pela cultura do compartilhamento (Lyon, 2017). Nesta seção, aponta-se a opacidade dos algoritmos inteligentes, que sugerem produtos, filtram conteúdos, aconselham rotas, entre outras ações cotidianas, tentando influenciar as escolhas individuais nos mais diversos níveis.

Nesse contexto, retoma-se o debate sobre o caráter performativo dos algoritmos e sua capacidade de manipular comportamentos. Destaca-se que o processo de formação das preferências e escolhas individuais e a própria capacidade de agenciamento estão ancorados em processos complexos de subjetividade, que demandam uma análise abrangente dos fenômenos sociais. Antes de prosseguir, ressalta-se que a discussão sobre autodeterminação em contraposição à dominação é central no pensamento político e se faz presente a partir do momento em que alguns autores defendem a capacidade de

modulação do comportamento por parte dos algoritmos inteligentes (Zuboff, 2019; Silveira, 2017). A partir desse ponto de vista, a mídia direcionada atua diretamente no exercício da autonomia individual. A modulação nas redes digitais envolve tanto o controle da visualização de conteúdo como todo o sistema de categorização operado pelos algoritmos.

Uma importante característica da segunda fase do capitalismo de vigilância é a cultura do compartilhamento, ancorada na publicização das experiências privadas, que não são mais extraídas de dados de navegação e outras tecnologias, mas tornadas públicas de forma “voluntária”. Observa-se um processo de autoafirmação, em que a exposição da intimidade opera como um reforço da identidade, sendo, ao mesmo tempo, performática e participativa (Bruno, 2008; Lyon, 2017). A extração de dados é facilitada e abre espaço para um segundo momento da mídia direcionada: a exploração do estado emocional das pessoas.

Nesta seção discute-se a modulação comportamental dos algoritmos a partir da discussão sobre dominação e autonomia. Nesse sentido, destaca-se que os algoritmos inteligentes se caracterizam pela intenção de se colocarem como intermediários no processo decisivo, ao apontar sugestões e tentar direcionar disposições. Entretanto, ainda que se reconheça a capacidade de antecipar tendências, sustenta-se que esses códigos não são determinantes nos processos decisórios, caracterizados por suas maleabilidades, contradições, circunstâncias sociais, escolhas anteriores e opções disponíveis (Benkler, Faris e Roberts, 2018; Sunstein, 2009). Portanto, ainda que se reconheça que existem efeitos sociais complexos a partir do uso dessas tecnologias, aponta-se a necessidade de maior transparência sobre o seu funcionamento, uma governança algorítmica.

Zuboff (2019) sustenta sua teoria do capitalismo de vigilância sobre a premissa de que os algoritmos inteligentes possuem uma capacidade de predição. De fato, define o conceito como “uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e vendas” (p. 1). Para a autora, a atual geração já é refém de uma complexa estrutura de poder, dominação e vigilância, operada a partir dos algoritmos.

O ponto em questão é que não se trata de uma vigilância verticalizada, realizada por parte do Estado, ou por corporações de tecnologia, mas de um monitoramento automatizado realizado por algoritmos inteligentes. A vigilância digital é mais próxima do modelo de sociedade de controle de Deleuze (2006), que a enxerga diluída no tecido social. Entretanto, a experiência vivida na sociedade contemporânea não se caracteriza apenas pelo controle, pela divisão entre os vigiados e os que vigiam ou pela assimetria de conhecimento sobre o que ocorre. A vigilância acaba por ser “útil” para o cotidiano das pessoas e, por isso, ela não é percebida como intrusiva, controladora ou punitiva.

É nesse sentido que Deleuze (2006) empregou a noção de modulação para descrever a mudança das sociedades disciplinares para sociedades de controle. Para o autor, o indivíduo tornou-se divisível, ao passo que o *marketing* se tornou um instrumento

de controle social. É relevante essa observação sobre a divisibilidade do indivíduo: somos ao mesmo tempo muitas coisas, entre elas consumidores, trabalhadores, cidadãos, enfim, seres imersos em uma complexa malha de relações sociais caracterizada por preferências adaptativas (Sunstein, 2009). Para Deleuze (2006), a modulação opera como uma forma de controle, em um novo regime de dominação. Ou seja, cada molde social ao qual o indivíduo tem que se adaptar é uma forma de exercício de controle. Nesse sentido, observa-se uma convergência com o pensamento de Foucault (2012), em que a vigilância é mais produtiva, no sentido de produzir comportamentos desejados, do que punitiva.

Ancorando-se no conceito de modulação de Deleuze (2006), diferentes autores caracterizam os algoritmos inteligentes como agentes de modulação do comportamento. Para eles (Zuboff, 2019; Bruno, 2008; Silveira, 2017), nesses códigos está embutida uma característica performática, ao modelar dinâmicas, práticas e comportamentos. As mídias sociais, que exploram a experiência de uso nas emoções, estariam exercendo o paradoxo da liberdade controlada, ou seja, a capacidade de se expressar de acordo com parâmetros já definidos. A modulação comportamental dos algoritmos inteligentes se daria, portanto, justamente pela sensação de liberdade sob certas restrições, ou escolhas limitadas pelas opções disponíveis.

Nesse contexto, destaca-se o complexo conceito de dominação e um de seus aspectos antagônicos, a autonomia. Em primeiro lugar, é preciso fazer uma distinção analítica entre dominação e opressão. Para Weber (1991), a dominação é “a possibilidade de impor ao comportamento de terceiros a vontade própria” (p. 188), ou seja, o impedimento de decisões autônomas. A opressão, por sua vez, em suas cinco ou mais facetas<sup>2</sup>, seria a imposição de condições instrumentais que limitam a capacidade de um indivíduo se desenvolver, tornando-o mais vulnerável em determinadas situações (Young, 1990). Ainda assim, é importante destacar que a opressão não se realiza necessariamente como coerção. A própria sociedade liberal impõe restrições a determinados indivíduos que limitam o amplo exercício de suas liberdades de escolha.

Em segundo lugar, é preciso enfatizar que a dominação é uma forma específica de poder, caracterizando-se como um exercício assimétrico de autoridade por parte de um agente que controla os recursos, materiais ou simbólicos (Pettit, 1997). Os dominados estariam submetidos a comportamentos que beneficiam os que detêm o poder (Miguel, 2018). Nesse contexto, as grandes empresas de tecnologia controlariam os mecanismos materiais e simbólicos, e a assimetria dessa relação refletiria a dominação, compreendida aqui como uma forma de exercício do poder de manipulação dos comportamentos.

Nessa perspectiva, os sujeitos teriam sua autonomia constrangida, em parte por razões individuais, mas, em especial, por valores socialmente construídos, já que toda preferência é socialmente produzida (Miguel, 2018). Estaríamos vivenciando a incorporação do ponto de vista do dominante (Bourdieu, 2007). O uso das tecnologias –

---

<sup>2</sup> Young (1990) elabora um modelo de justiça a partir do que considera as cinco facetas da opressão: exploração, marginalização, impotência, dominação cultural e violência.

aplicativos e sistemas – estaria legitimando as hierarquias sociais, assim como o consumo cultural exerceu esse papel no campo simbólico em décadas passadas. De fato, para Benkler, Faris e Roberts (2018), a mídia *online* reflete as assimetrias do ecossistema de comunicação de outros meios, como rádio e televisão, entre outros.

Entretanto, existem algumas especificidades relacionadas à mídia direcionada que se diferenciam daquelas relativas aos meios de comunicação de massa. Essa variação pode, por um lado, aprofundar o poder simbólico e, por outro lado, ampliar o autodeterminismo digital. É nesse sentido que Sunstein (2002) reconhece que as mídias sociais possibilitam que cada pessoa seja o curador de seu próprio conteúdo, e destaca indicadores de estudos comportamentais, anteriores à internet, que ressaltam que as pessoas buscam evidências sobre aquilo em que já acreditam (viés de confirmação) e se aproximam de outras com pontos de vista semelhantes (homofilia). Sendo assim, as câmaras de eco, conhecidas como “bolhas”, estariam reforçando um fenômeno social anterior às tecnologias de informação e comunicação.

O uso das redes sociais é tido como central em processos eleitorais recentes, devido às técnicas de *marketing* comportamental aplicadas a anúncios personalizados *online*. Para averiguar a hipótese da influência da internet nesses fenômenos, Benkler, Faris e Roberts (2018) analisaram mais de 4 milhões de notícias veiculadas antes e depois do período eleitoral estadunidense de 2016. Utilizaram técnicas de análise de rede, com foco nos padrões de interligação entre as notícias, com o objetivo de compreender a relação de autoridade e credibilidade entre os publicadores e os padrões de atenção na mídia. Os resultados indicam que as notícias falsas, o uso de mecanismos automatizados (*bots* e robôs) e as técnicas de *marketing* comportamental aplicadas a anúncios personalizados (utilizadas oficialmente ou extraoficialmente) são fenômenos que tiveram resultados pouco significativos no processo eleitoral de 2016, nos Estados Unidos.

Os autores defendem que relacionar fenômenos como a polarização política ou as notícias falsas à internet é um erro de diagnóstico. Ao observar as relações de longo prazo entre as tecnologias, as instituições, a política e a cultura, os autores explicam que a internet está inserida em um ecossistema de mídia caracterizado pela radicalização conservadora, em um processo que ocorre há pelo menos 30 anos. Nesse período, os meios de comunicação de massa, ao divulgarem e reproduzirem discursos conservadores, acabaram por legitimá-los. Sendo assim, a assimetria do ecossistema de mídia *off-line* se reproduz *online*. Em outras palavras, as câmaras de eco são um fenômeno anterior ao surgimento da própria internet.

Reforçando os argumentos de Benkler, Faris e Roberts (2018), destacam-se outras ressalvas a ser consideradas quando se discute a capacidade de dominação das tecnologias da informação e de seus algoritmos inteligentes em prever e até mesmo moldar comportamentos, como defendem os behavioristas radicais (Zuboff, 2019; Bruno, 2008; Silveira, 2017). Primeiramente, o fato é que, como os algoritmos são patenteados, não se

pode inferir com exatidão suas características e potencialidades de predição. Entretanto, isso não significa que essa tentativa de modulação não tenha efeitos na sociedade.

Em segundo lugar, há de se considerar o fato de que as preferências não são fixas, e sim maleáveis (Sunstein, 2009). São processos dinâmicos em que as sugestões dos algoritmos podem ora fazer sentido, ora indicar absurdos e contradições. É importante reconhecer que existem conformações sociais que buscam restringir a liberdade e o exercício da autonomia, e as tecnologias são apenas um de seus aspectos. As opressões de raça, gênero e classe operam de forma muito mais verticalizada do que o controle distribuído.

Em terceiro lugar, é preciso considerar que, para que a dominação persista, é necessário que haja certa conformidade dos dominados (Miguel, 2018). Nesse sentido, ainda que a sensação de impotência individual diante dos gigantes da tecnologia esteja presente, há de se lembrar que existem instituições globais que combatem o tratamento indiscriminado de dados pessoais. Por mais que as pessoas se acomodem, há um Regulamento Geral de Proteção de Dados vigente. Tribunais, conselhos, autoridades, entre outros, atuam para transformar o modelo de negócios dessas empresas. Trata-se de um questionamento institucional, caracterizado por visões distintas sobre a democracia liberal e o papel do Estado na regulação das relações entre o setor privado e os direitos individuais. São autoridades que atuam diretamente na transformação do modelo de negócios das empresas de tecnologia. Portanto, a dominação não é exercida verticalmente sem que haja certa resistência, inclusive institucional, o que, novamente, não significa que que os efeitos na sociedade ocorram de forma determinística.

Inclusive, logo que entrou em vigor o regulamento europeu, o austríaco Mark Schrems fundou a organização sem fins lucrativos None of Your Business (NOYB) (Schrems, 2014), com o objetivo de defender os direitos previstos na legislação. Uma de suas primeiras iniciativas (Scally, 2018) foi uma ação contra o Google e o Facebook, alegando que as empresas agem de forma coercitiva para que as pessoas aceitem os termos de uso de suas plataformas. Na ação, em que as empresas podem ser multadas em quase 4 bilhões de euros, Schrems questiona justamente a ausência do consentimento explícito e esclarecido determinado pela norma. Em 2011, ele já havia tomado iniciativa semelhante. Por meio da ONG Europe x Facebook (Schrems, 2011), ele denunciou ao Conselho de Proteção de Dados da Irlanda, onde a empresa mantém sua filial europeia, o tratamento indevido dos dados. Ao solicitar as informações pessoais coletadas pela plataforma, ele recebeu um documento com mais de 1.200 páginas por meio do qual descobriu, entre outras coisas, que até as mensagens apagadas eram gravadas em uma categoria intitulada "deleted".

O Regulamento Geral sobre a Proteção de Dados já foi utilizado em diversos casos, entre os quais o mais conhecido é o do Cambridge Analytica. A empresa obteve dados de milhões de pessoas do Facebook, utilizando as informações em campanhas políticas, como a do presidente estadunidense Donald Trump e a da saída do Reino Unido da União

Europeia, conhecido como Brexit.

A autoridade de proteção de dados da Inglaterra, o Information Commissioner's Office (ICO), multou o Facebook em 500 mil libras (Waterson, 2018), apenas pelo vazamento de dados dos britânicos. Já a Itália, pelo mesmo motivo, multou a empresa em 10 milhões de euros (Efe, 2018). Mas foi na sede da companhia, nos Estados Unidos, que ocorreu a multa de valor mais significativo: 5 bilhões de dólares, em determinação aplicada pela Comissão Federal de Comércio (Federal Trade Commission) (G1, 2019a). Até o Brasil, por meio da Secretaria Nacional do Consumidor, puniu o Facebook em R\$ 6,6 milhões pelo mesmo motivo (G1, 2019b).

Somado a isso, há de se levar em conta que o exercício do poder é diferente de sua capacidade de influência. A intenção não significa realização. É reconhecível que existe a motivação de influenciar comportamentos, hábitos de consumo, preferências políticas. Entretanto, como destacam Benkler, Faris e Roberts (2018), é um erro de diagnóstico apontar as tecnologias e outros fenômenos contemporâneos como responsáveis pelos processos de polarização política, verificados a partir do uso das tecnologias digitais. É necessário observar toda a conformação do espectro eletromagnético e a infraestrutura de comunicação, historicamente constituída pelo setor privado. Note-se que não se trata apenas dos discursos conservadores mobilizados por meios de comunicação de massa, como rádio, jornais e televisão. O ecossistema de telecomunicações, gerenciado em âmbito internacional pela União Internacional de Telecomunicações (International Telecommunications Union), envolve as ondas curtas e frequências alocadas para tecnologias móveis – como o recente 5G – como também os cabamentos submarinos e protocolos de rede, como o IPV6. Ou seja, até na própria infraestrutura de telecomunicações os interesses privados são colocados em primeiro plano. Um simples exemplo desse fato é a exploração comercial da banda larga no Brasil, em que a fibra ótica não chega às favelas, ou cidades de pequeno porte.

Por fim, a falta de transparência sobre como operam os algoritmos não permite afirmações sobre sua capacidade de influenciar comportamentos, ainda que se reconheça que existam efeitos sociais complexos em andamento. Como argumenta O'Neil (2016), a falta de transparência sobre o funcionamento dos algoritmos indica a tendência de que esses mecanismos segreguem determinadas informações, privilegiem outras, reproduzindo padrões de preconceito e discriminação, reforçando, assim, o aprofundamento das desigualdades da sociedade. Observa-se a atuação desse tipo de inteligência artificial em atividades como processos seletivos para empregos, aplicação de tarifas de planos de saúde, obtenção de crédito, indústrias do varejo e do entretenimento.

Ainda assim é preciso reconhecer que é uma mudança significativa o fato de que os algoritmos determinem o que é apresentado às pessoas. Mas existe uma diferença entre detectar comportamentos e tendências e manipulá-los, já que as pessoas possuem outros estímulos e bagagens. Além disso, observam-se diversas formas de resistência, seja no nível individual, como a recusa de utilizar determinados aplicativos, ou redes sociais, seja

no âmbito institucional. Com a entrada em vigor do Regulamento Geral de Proteção de Dados, a concentração de poder e o monopólio neoliberal exercido pelas empresas de tecnologia são questionados.

Antes de continuar, é importante sublinhar que, por todos esses fatores, o capitalismo de vigilância é um fenômeno característico da nova ordem neoliberal (Laval e Dardot, 2016; Fraser, 2009; Brown, 2015). Inclusive, devido ao fato de que ocorre uma confluência das empresas de tecnologia com o próprio capital financeiro, já que muitas delas são controladas diretamente por grupos de investidores (Dantas, 2019). Zuboff (2019) é certa em apontar que a ausência de regulação e a associação entre as empresas de tecnologia e o governo estadunidense foram processos fundamentais para a consolidação do fenômeno da vigilância em massa.

Diante de todas essas questões, pode-se concluir que o Regulamento Geral de Proteção de Dados da União Europeia é um avanço, entretanto não é suficiente para conter o monitoramento automatizado das experiências pessoais. Esse fenômeno é responsável não só por modular comportamentos, mas também pela automatização de processos decisórios, que reproduzem assimetrias e aprofundam desigualdades de gênero, raça e renda.

Sendo assim, é necessário regular o funcionamento dos próprios algoritmos. Esses códigos são o outro lado da moeda no debate sobre proteção de dados pessoais e privacidade. Compreender como funcionam é central para inferir seus impactos nas sociedades, ainda que a simples abertura dos códigos não signifique que seja possível controlar seus efeitos. A transparência é apenas um passo para compreender a complexidade de suas repercussões, além de ser complementar ao debate sobre proteção de dados pessoais e privacidade. Os algoritmos não são neutros, são instrumentos que operam de acordo com finalidades predeterminadas. Justamente por isso suas decisões não são tomadas com base em análises isentas, ou critérios de justiça, mas operadas de acordo com interesses, em sua maioria comerciais. Por isso a urgência de haver transparência sobre a forma como operam, em especial quando as pessoas estão sujeitas às decisões tomadas por eles.

É precisamente nesse sentido que a ausência de regulação dos algoritmos ameaça as democracias liberais. Ao se colocarem como intermediários dos processos de decisão, eles reforçam assimetrias e preconceitos de raça, gênero e renda. O fenômeno pode ser observado na seleção prévia e categorização realizadas por setores, como planos de saúde, obtenção de crédito e o próprio sistema de segurança pública. Ao deslocar o poder decisório para os algoritmos, ocorre uma ruptura com a própria lógica do Estado democrático de direito, essencial para as democracias liberais.

Antes de prosseguir, é importante enfatizar dois aspectos do Regulamento Geral de Proteção de Dados da União Europeia. Em primeiro lugar, a legislação é bem objetiva em determinar que os sujeitos, tratados como titulares de dados, possuem o direito a não estar sujeitos a decisões baseadas exclusivamente em meios automatizados. Ou seja,

restringe a tomada de decisão indiscriminada pelos algoritmos que afetam as pessoas. A regulação determina que, caso isso ocorra, é possível solicitar uma revisão das decisões.

Somado a isso, é importante considerar que as tecnologias são construídas sobretudo em países industrialmente mais desenvolvidos. Portanto, países em que não existem leis de proteção de dados e em que a privacidade não é tida como um direito estão sujeitos a tecnologias experimentais, que envolvem biometria, manipulação de DNA, reconhecimento facial, entre outras, cada vez mais avançadas e pouco transparentes com relação a sua forma de funcionamento. Dessa forma, países que não fazem parte da União Europeia estão em condições de subalternidade.

Pontuadas essas questões, prossegue-se para a seção seguinte do artigo, em que se debate o uso do conceito de governança, amplamente empregado em diversos setores da sociedade para descrever formas de compartilhar os processos decisórios. Utiliza-se o termo para problematizar a opacidade dos algoritmos e destacar a urgência de uma regulação sobre as formas como operam.

### **Governança algorítmica**

Conforme mencionado na seção anterior, o conceito de governança é importado da área de administração para descrever uma nova forma de governabilidade imposta pelo neoliberalismo (Laval e Dardot, 2016; Brown, 2015). Ele expõe a dependência dos Estados em relação ao poder corporativo privado, em especial do mercado financeiro. A governança pode ser compreendida também como a coprodução público-privada das normas internacionais, em políticas de integração nacionais, ou regionais, para o mercado mundial globalizado, uma adaptação do Estado à nova realidade neoliberal (Laval e Dardot, 2016, p. 277). A ampla adoção do termo governança pelos mais diversos setores da sociedade expõe o fato de que o neoliberalismo não é uma ideologia, mas sim uma “ordem prática”, ou uma nova racionalidade.

Para Laval e Dardot (2016), essa nova racionalidade representa o esgotamento da democracia liberal – ainda que o conceito esteja em constante disputa. Para os autores, as características dessa nova fase neoliberal podem ser resumidas em quatro aspectos: o mercado como realidade construída, a concorrência como norma, a transformação do Estado em “empresa” e a conformação de “neossujeitos” empreendedores.

Por outro lado, o modelo de governança não teria apenas aspectos perversos, como a adoção da lógica empresarial pelo Estado e o desprezo pela justiça social. Sua busca pela eficiência e eficácia traria como benefício uma maior *accountability* governamental (em especial, a prestação de contas, mas também a responsabilização). Ao envolver diversos atores interessados em um modelo multissetorial, transformaria os processos decisórios em ações mais plurais, agregando diversos pontos de vista. O principal exemplo de aplicação do modelo multissetorial é o próprio ecossistema de governança da internet, detalhado adiante.

Longe de esgotar as controvérsias possíveis, o fato é que a governança se tornou a forma de administração neoliberal, sendo adotada pelo Parlamento Europeu, por grandes corporações e pela própria Organização das Nações Unidas (ONU). No contexto do debate sobre o ecossistema de telecomunicações e a internet, é relevante ressaltar que a União Internacional de Telecomunicações foi célere em adotar o modelo de governança. Fundada em 1865 para negociar a alocação do espectro eletromagnético, entre outras atividades, é considerada a organização internacional mais antiga do mundo, sendo responsável, no âmbito da ONU, por liderar o debate sobre governança da internet.

Em 2001, a Assembleia Geral das Nações Unidas aprovou a proposta da realização da Cúpula Mundial sobre a Sociedade da Informação para tratar de questões relacionadas à expansão das tecnologias de comunicação e informação pelo mundo. O primeiro evento ocorreu em Genebra, em 2003, e o segundo, em 2005, em Túnis, Tunísia, ambos organizados pela União Internacional de Telecomunicações.

Os eventos foram marcados pela pressão da comunidade internacional por um debate sobre a gestão dos recursos da internet, principalmente pelo fato de a entidade responsável pelo controle dos endereços e da internet, a Corporação da Internet para Atribuição de Nomes e Números (em inglês ICANN – Internet Corporation for Assigned Names and Numbers), estar associada ao departamento de comércio dos Estados Unidos. O objetivo era “globalizar” o órgão, permitindo a participação de outros países e diversos setores da sociedade em sua gestão.

Como resultado direto, os eventos geraram os Documentos da Cúpula Mundial sobre a Sociedade da Informação (WSIS, 2005), que foram estruturantes para os próximos passos da ONU e da União Internacional de Telecomunicações, em especial a criação do Fórum de Governança da Internet, a partir de 2006. Inclusive, esses documentos adotam terminologias da governança neoliberal: “plano de ação”, “gestão de metas”, “estratégias digitais”, entre outras.

Após mais de uma década, a ICANN continua operando de forma central os recursos da internet, metas como a universalização do acesso à rede foram prorrogadas e o poder das empresas de tecnologia se consolidou. A promessa da governança colaborativa e multissetorial nunca se concretizou. De fato, o próprio modelo de um suposto compartilhamento de decisões parece legitimar ainda mais as ações e atividades dessas empresas. A reação dos Estados é lenta em regular o setor e, ao mesmo tempo, os países concorrem entre si para dominar o futuro do mercado de tecnologia. A corrida pela tecnologia do 5G, em que figuram embates entre os Estados Unidos e a China, é um exemplo concreto desse fato.

Por outro lado, o conceito de governança pode ser útil para solucionar o embate sobre a transparência dos algoritmos. Em uma realidade cada vez mais digital, a regulação da forma como operam esses códigos é cada vez mais imperativa. Tutt (2016), que é advogado do Departamento de Justiça do governo dos Estados Unidos, defende um modelo regulatório para os algoritmos nos moldes da agência nacional do Departamento de Saúde

e Serviços Humanos, a Food and Drug Administration (FDA). O autor descreve como a autarquia foi criada diante de uma crise sem precedentes de saúde pública, em 1906 (p. 120). Para ele, entre os modelos regulatórios adotados nos Estados Unidos, esse seria o mais adequado para se chegar a uma governança algorítmica.

O paralelo com um momento de crise realizado pelo autor é certo. Conforme destacado anteriormente, diante dos ataques de 11 de setembro de 2001, a regulação da privacidade e da proteção de dados ficou em suspenso nos Estados Unidos. A associação, sem precedentes, entre empresas de tecnologia e agências de segurança do país possibilitou tanto a conformação do capitalismo de vigilância como o surgimento do monopólio de companhias de tecnologia. Por outro lado, essa aliança afeta diretamente o direito à concorrência, uma das bases do capitalismo e da democracia liberal.

Inclusive quase duas décadas depois da conformação do fenômeno do capitalismo de vigilância, um conjunto de procuradores provenientes de diversos locais dos Estados Unidos investiga as corporações de tecnologia por violações das leis antitruste do país (Welle, 2019). A abordagem novamente destaca os direitos do consumidor de liberdade de escolha entre os concorrentes, destacando como as empresas agiram para sufocar eventuais competidores.

O fato é que cada vez mais se questiona a concentração de poder das empresas de tecnologia e do sistema financeiro por meio de uma abordagem que enfatiza os direitos dos consumidores ou a proteção de dados pessoais e privacidade. O ponto de convergência entre esses questionamentos é justamente a forma como esses sistemas funcionam, portanto, uma governança algorítmica.

Esses códigos são o outro lado da moeda no debate sobre proteção de dados pessoais e privacidade. E eles não são neutros. Suas decisões não são tomadas com base em análises isentas. Cada vez mais a regulação dos algoritmos é uma questão de justiça social. Portanto, um modelo de governança algorítmica se faz necessário para que os Estados consigam, em cooperação com as empresas (já que esse é o mote neoliberal), regular os sistemas “inteligentes” e impedir que seus processos decisórios, pouco transparentes, reproduzam as assimetrias sociais e aprofundem ainda mais as desigualdades.

## **Conclusão**

O conceito de privacidade, estruturado a partir da distinção entre público e privado, remete a uma metáfora espacial que perde sentido com a introdução das tecnologias da informação. A proteção de dados pessoais ganha relevância a partir do momento em que os algoritmos permeiam os mais diversos aspectos da vida em sociedade. A dimensão coletiva dessas questões as torna objeto de reflexão no contexto das teorias contemporâneas da democracia.

A esfera privada, historicamente negligenciada na teoria política, torna-se a

principal origem de informação do mercado de dados. Nesse contexto, é desafiador pensar que a privacidade, defendida como um direito humano fundamental, seja cotidianamente deixada de lado por metade da população mundial, que utiliza as tecnologias de informação e comunicação. Esse paradoxo é justamente o que a torna objeto de uma questão coletiva. As pessoas são levadas a ignorar a questão da privacidade e da proteção de seus dados pessoais não por descaso, mas por desconhecimento sobre a forma como os algoritmos operam. São situações sociais complexas, já que cada vez mais as tecnologias fazem parte dos mais diversos aspectos da vida social. O tratamento de dados pessoais incide cada vez mais no exercício da cidadania, dos direitos e das liberdades individuais. As normas jurídicas e instituições não podem mais negligenciar o que ocorre na esfera privada, que se torna cada vez mais política.

O artigo buscou acrescentar elementos para o debate sobre o capitalismo de vigilância, conceito que se refere ao monitoramento automatizado de experiências privadas, com a intenção de induzir ou direcionar comportamentos. Apesar de reconhecer a convergência sem precedentes de recursos e regras necessárias ao exercício da dominação, argumenta-se que a efetivação dessa influência não ocorre de forma determinística, ou direta, ainda que se reconheça que ocorram efeitos sociais complexos a partir da disseminação dessas tecnologias. De fato, a própria tentativa de opressão pode ter efeitos contrários como subversões individuais cotidianas, entre outras estratégias de resistência. Nesse sentido, destaca-se que a possibilidade de exercício do poder não significa sua efetivação e que o processo de formação das preferências é adaptável e influenciado por diversos fatores, tais como condições estruturais para o exercício da autonomia, escolhas passadas, circunstâncias sociais, opções disponíveis, dentre outros elementos.

Somada a essas questões, observa-se uma contestação às práticas de monitoramento e vigilância no campo coletivo e institucional a partir da vigência do Regulamento Geral de Proteção de Dados da União Europeia. Ainda que nos Estados Unidos a questão seja abordada a partir do direito dos consumidores e do direito concorrencial, a legislação desse país não foi suficiente para conter a expansão do capitalismo de vigilância. Como resultado, observa-se a concentração de poder das corporações de tecnologia, que cada vez mais impactam todo o ecossistema de mídia.

Sobretudo, buscou-se sublinhar como o fenômeno do capitalismo de vigilância é consequência de um arranjo neoliberal, em que houve a aliança do setor de tecnologia com o sistema financeiro, amparado em um modelo de regulação em que as intervenções do Estado são mínimas. Sendo assim, a atividade de monitoramento automatizado das experiências privadas, realizada por algoritmos inteligentes, se consolidou de forma silenciosa ao longo das últimas duas décadas.

Diante disso, enfatizou-se a necessidade da transparência das formas de funcionamento e tomadas de decisão dos algoritmos, que cada vez mais impactam a sociedade. Argumentou-se que, muito mais do que moldar comportamentos, os algoritmos

reproduzem padrões de discriminação de raça, gênero e renda, reforçando assimetrias e aprofundando as desigualdades sociais. Diante disso, destacou-se a necessidade de regular não apenas a proteção de dados pessoais, como também o próprio funcionamento desses códigos, ou seja, uma governança algorítmica. A transparência com relação às decisões tomadas por esses sistemas é um primeiro passo para que se compreenda como operam e, conseqüentemente, como impactam a sociedade.

### Referências bibliográficas

- BENKLER, Y.; FARIS, R.; ROBERTS, H. *Network propaganda: manipulation, disinformation, and radicalization in American politics*. Reino Unido: Oxford University Press, 2018.
- BHARAT, K.; LAWRENCE, S.; SAHAMI, M. "Generating user information for use in targeted advertising" (online). Google, 2009. Disponível em: <<https://patents.google.com/patent/US20050131762A1/en>>. Acesso em: 7 fev. 2019.
- BOURDIEU, P. *A distinção crítica social do julgamento*. São Paulo: Edusp, 2007.
- BROWN, W. *Undoing the demos: neoliberalism's stealth revolution*. New York: Zone Books, 2015.
- BRUNO, F. "Monitoramento, classificação e controle nos dispositivos de vigilância digital". *Revista Famecos: Mídia, Cultura e Tecnologia*, Porto Alegre, nº 36, p. 10-16, 2008.
- COHEN, J. L. Rethinking privacy: autonomy, identity, and the abortion controversy. In: WEINTRAUB, J.; KUMAR, K. (eds.). *Public and private in thought and practice: perspectives on a grand dichotomy*. Chicago: The University of Chicago Press, 1997.
- DANTAS, M. "The financial logic of internet platforms: the turnover time of money at the limit of zero". *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, vol. 17, nº 1, p. 132-158, 2019.
- DELEUZE, G. "Post-scriptum sobre las sociedades de control". *Polis Revista Latinoamericana*, nº 13, p. 1-7, 2006.
- DOLAN, K. "The world's billionaires" (online). *Forbes*, 2019 Disponível em: <<https://www.forbes.com/billionaires/list/#version:static>>. Acesso em: 7 fev. 2019.
- EFE, A. "Itália multa Facebook em € 10 milhões por vender dados de usuários" (online). *G1*, 2018. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/2018/12/10/italia-multa-facebook-em-euro-10-milhoes-por-vender-dados-de-usuarios.ghtml>>. Acesso em: 2 jan. 2020.
- FRASER, N. "Feminism, capitalism, and the cunning of history". *New Left Review*, Londres, nº 56, p. 97-117, 2009.
- FOUCAULT, M. *Vigiar e punir*. Rio de Janeiro: Vozes, 2012.
- G1. "Facebook pagará multa recorde de US\$ 5 bilhões por violação de privacidade" (online). *G1*, 2019a. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/2019/07/24/facebook-pagara-multa-de-us-5-bilhoes-por-violacao-de-privacidade.ghtml>>. Acesso em: 2 jan. 2020.

G1. "Ministério da Justiça multa Facebook em R\$ 6,6 milhões em apuração sobre compartilhamento de dados" (online). *G1*, 2019b. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/2019/12/30/ministerio-da-justica-multa-facebook-em-r-66-milhoes-em-apuracao-sobre-compartilhamento-de-dados.ghtml>>. Acesso em: 2 jan. 2020.

HARVEY, D. *O neoliberalismo: história e implicações*. São Paulo: Loyola, 2008.

LAVAL, C.; DARDOT, P. *A nova razão do mundo: ensaios sobre a sociedade neoliberal*. São Paulo: Boitempo, 2016.

LOREY, I. *State of insecurity: government of the precarious*. New York: Verso Books, 2015.

LYON, D. "Surveillance culture: engagement, exposure, and ethics in digital modernity". *International Journal of Communication*, nº 11, p. 824-42, 2017.

MALKIN, M. "Google is collecting data on schoolkids" (online). *Mind Matters*, 2018. Disponível em: <<https://mindmatters.ai/2018/09/google-collecting-data-on-schoolkids/>>. Acesso em: 7 fev. 2019.

MIGUEL, L. F. *Dominação e resistência: desafios para uma política emancipatória*. São Paulo: Boitempo Editorial, 2018.

MOLLA, R. "Google, Amazon, and Facebook all spent record amounts last year lobbying the US government" (online). *Vox*, 2019. Disponível em: <<https://www.recode.net/2019/1/23/18194328/google-amazon-facebook-lobby-record>>. Acesso em: 7 fev. 2019.

O'NEIL, C. *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York: Broadway Books, 2016.

PATEMAN, C. *The sexual contract*. Palo Alto, California: Stanford University Press, 1988.

PETTIT, P. *Republicanism: a theory of freedom and government*. Reino Unido: OUP Oxford, 1997.

ROGERS, Y.; SHARP, H.; PREECE, J. *Design de interação*. Porto Alegre: Bookman Editora, 2013.

SCALLY, D. "Max Schrems files first cases under GDPR against Facebook and Google" (online). *Irish Times*, 2018. Disponível em: <<https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177>>. Acesso em: 7 fev. 2019.

SCHREMS, M. "Europe x Facebook" (online). 2011. Disponível em: <<http://europe-v-facebook.org/>>. Acesso em: 23 set. 2019.

\_\_\_\_\_. "None of your business" (online). *Noyb*, 2014. Disponível em: <<https://noyb.eu/>>. Acesso em: 23 set. 2019.

SCOTT, J. *Domination and the arts of resistance: hidden transcripts*. New York: Yale University Press, 1990.

SILVEIRA, S. A. *Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais*. São Paulo: Edições Sesc São Paulo, 2017.

SUNSTEIN, C. R. *Republic.com*. Princeton: Princeton University Press, 2002.

SUNSTEIN, C. R. "Preferências e política". *Revista Brasileira de Ciência Política*, Brasília, nº 1, p. 219-54, 2009.

TUTT, A. "An FDA for algorithms". *Administrative Law Review*, vol. 83, p. 83-123, 2016.

WATERSON, J. "UK fines Facebook £500,000 for failing to protect user data" (online). *The Guardian*, 2018. Disponível em: <<https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica>>. Acesso em: 7 fev. 2019.

WEBER, M. *Economia e sociedade*, vol. 1. Brasília: Editora UnB, 1991.

WELLE, D. "Facebook e Google são investigados por práticas antitruste" (online). *Deutsche Welle*, 2019. Disponível em: <<https://p.dw.com/p/3PDev>>. Acesso em: 23 set. 2019.

WSIS. "Documentos da Cúpula Mundial sobre a Sociedade da Informação" (online). *WSIS*, 2005. Disponível em: <<https://www.itu.int/net/wsis/index.html>>. Acesso em: 14 nov. 2018.

YOUNG, I. *Justice and the politics of difference*. Princeton: Princeton University Press, 1990.

ZUBOFF, S. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs, 2019.

## Abstract

### *Algorithms and autonomy: power and resistance relations in surveillance capitalism*

The phenomenon of automated monitoring of private experiences, performed by intelligent algorithms, intended to induce certain behaviors, is conceptualized in the literature as surveillance capitalism. The article add some elements to these theories from the following arguments; the lack of transparency of algorithms makes it impossible to accurately infer their capacity for behavioral modulation; the preference formation is a complex and malleable process, that encompasses strategies of resistance and subversion; for domination to occur, there must be conformity of the dominated, which is not observed from currently normative frameworks; finally, the exercise of power is different from its ability to influence. The conclusion is that it is necessary to regulate the proper functioning of the algorithms as a complement to the protection of personal data.

**Keywords:** surveillance capitalism; privacy; democracy; algorithms; neoliberalism

## Resumen

### *Algoritmos y autonomía: relaciones de poder y resistencia en la vigilancia del capitalismo*

El fenómeno del monitoreo automatizado de experiencias privadas, realizado por algoritmos inteligentes, destinados a inducir ciertos comportamientos, está conceptualizado en la literatura como capitalismo de vigilancia. El artículo agrega algunos elementos a esta teoría a partir de los siguientes argumentos; la falta de transparencia de los algoritmos hace que sea imposible inferir con precisión su capacidad de modulación de los comportamientos; la formación de preferencias es un proceso complejo y maleable, que abarca estrategias de resistencia y subversión; para que ocurra la dominación, debe haber conformidad de los dominados, lo que no se observa desde los marcos normativos vigentes; finalmente, el ejercicio del poder es diferente de su capacidad de influencia. A partir de estos puntos, se concluye que es necesario regular el funcionamiento adecuado de los algoritmos como complemento de la protección de datos personales.

**Palabras clave:** capitalismo de vigilancia; privacidad; democracia; algoritmos; neoliberalismo

## Résumé

### *Algorithmes et autonomie: relations de pouvoir et de résistance dans le capitalisme de surveillance*

Le phénomène de surveillance automatisée des expériences privées, effectué par des algorithmes intelligents, destinés à induire certains comportements, est conceptualisé dans la littérature sous le nom de capitalisme de surveillance. L'article ajouter quelques éléments à cette théorie à partir des arguments suivants; le manque de transparence des algorithmes ne permet pas de déduire avec

précision leur capacité de modulation comportementale; la formation de préférences est un processus complexe et malléable, qui englobe des stratégies de résistance et de subversion; pour qu'il y ait domination, il faut qu'il y ait conformité des dominés, ce qui n'est pas observé dans les cadres normatifs en vigueur; enfin, l'exercice du pouvoir est différent de sa capacité d'influence. De ces éléments, on peut conclure qu'il est nécessaire de réglementer le bon fonctionnement des algorithmes en complément de la protection des données à caractère personnel.

*Mots-clés:* surveillance du capitalisme; la vie privée; la démocratie; algorithmes; néolibéralisme

Artigo submetido à publicação em 26 de setembro de 2019.

Versão final aprovada em 7 de janeiro de 2021.

*Opinião Pública* adota a licença Creative Commons CC-BY.

