MATRIZes

Matrizes
ISSN: 1982-2073
ISSN: 1982-8160
matrizes@usp.br
Universidade de São Paulo
Brasil

Adriana Bonin, Jiani

Aportes da obra *De Orwell al cibercontrol* para entender o cibercontrole

Matrizes, vol. 14, núm. 3, 2020, Septiembre-, pp. 197-211
Universidade de São Paulo
São Paulo, Brasil

DOI: https://doi.org/10.11606/issn.1982-8160.v14i3p197-211

Disponible en: https://www.redalyc.org/articulo.oa?id=143066629003

Aportes da obra *De Orwell al cibercontrol* para entender o cibercontrole

Contributions of the book De Orwell al cibercontrol *to understand cyber control*

JIANI ADRIANA BONIN[a]

Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Ciências da Comunicação. São Leopoldo – RS, Brasil

[1] Professora e pesquisadora do Programa de Pós-Graduação em Ciências da Comunicação da Unisinos. Orcid: https://orcid.org/0000-0001-8598-7411. E-mail: jianiab@gmail.com

RESUMO

Neste texto, são sistematizadas contribuições do livro *De Orwell al cibercontrol*, de Armand Mattelart e André Vitalis, para pensar a problemática do cibercontrole. São recuperados aportes para a compreensão do fenômeno em três dimensões: a) como nova forma de controle social, historicamente gestada e umbilicalmente ligada a interesses estatais, geopolíticos e econômicos associados ao desenvolvimento das tecnologias digitais; b) como nova modalidade de exercício do poder, distinta do poder disciplinar; e c) como campo de contradições, com possibilidades de resistência e de contestação social. Junto à restauração desses aportes, são exploradas algumas linhas complementares para a investigação do cibercontrole contemporâneo.

Palavras-chave: Cibercontrole, cibervigilância, Mattelart e Vitalis

ABSTRACT

In this text, contributions from the book *De Orwell al cibercontrol*, by Armand Mattelart and André Vitalis, are systematized to analyze the problem of cyber control. Their contributions serve as basis to understand the phenomenon in three dimensions: a) as a new form of social control, historically managed and umbilically linked to state, geopolitical and economic interests associated with the development of digital technologies; b) as a new type of exercise of power, distinct from disciplinary power; and c) as a field of contradictions, with possibilities of resistance and social protestation. Along with the restoration of these contributions, some complementary lines of thought are explored for the investigation of contemporary cyber control.

Keywords: Cyber control, cyber-surveillance, Mattelart and Vitalis

INTRODUÇÃO

Resistir à ascensão do Todo de segurança é restaurar a ideia de que as técnicas de controle não podem substituir a resolução política dos problemas de fundo da sociedade[1].
(Mattelart & Vitalis, 2015, p. 12)

O PROCESSO DE DIGITALIZAÇÃO das sociedades reconfigurou nosso ecossistema comunicativo, abrindo novas possibilidades para sujeitos, grupos, coletivos e movimentos sociais a partir da disseminação e do acesso a recursos de produção e da apropriação social das tecnologias digitais. Mas ele vem sendo acompanhado, também, de fortes contradições, como a concentração de propriedade e de negócios em um número reduzido de grupos econômicos transnacionais e a constituição de uma renovada forma de controle social, o *cibercontrole*, cuja natureza e consequências precisam ser criticamente investigadas.

Armand Mattelart tem se ocupado, desde a década de 1960, com a investigação da problemática do controle[2]. Suas análises nessa trajetória incluem o exame das formas de controle geopolítico de sistemas, meios, indústrias e fluxos da comunicação no mundo (Maldonado, 2015). Em suas últimas obras, essa preocupação passa a se orientar para o exame do cibercontrole, questão que adquire relevo e importância crucial com a expansão da digitalização. O foco do trabalho aqui desenvolvido é a contribuição que ele oferece no livro *De Orwell al cibercontrole*, lançado em 2015, escrito em parceria com André Vitalis, para pensar o cibercontrole, recorte pautado na atualidade e riqueza investigativa desta obra.

O itinerário do exame aqui desenvolvido está focalizado em três dimensões presentes no trabalho investigativo de Mattelart e Vitalis (2015), que considero chaves para a compreensão do cibercontrole, a saber: 1) os processos históricos de sua constituição; 2) as especificidades desta nova modalidade de exercício do poder; e 3) possibilidades de apropriação e resistência social. Junto a este movimento, exploro também algumas linhas complementares de reflexão a partir do diálogo com trabalhos de outros pesquisadores que vêm pesquisando o tema[3].

[1] No original: "Resistir al ascenso del *Todo securitario* es restaurar la idea según la cual las técnicas de control no pueden servir como sustituto de la resolución política de los problemas de fondo de la sociedad". Tradução da autora.

[2] Uma análise detalhada e consistente desta contribuição é realizada por Efendy Maldonado (2015).

[3] Considero principalmente os trabalhos de Sérgio Amadeu Silveira, de Fernanda Bruno e de alguns pesquisadores que participaram do livro *Tecnopolíticas da vigilância*, lançado em 2018, fruto de um seminário promovido pela Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (Lavits), que opera desde 2009.

Inicio este percurso com a mirada histórica proposta pelos autores para dar conta da gênese do cibercontrole e de seu desenvolvimento.

A EMERGÊNCIA DO CIBERCONTROLE EM PERSPECTIVA HISTÓRICA

Um aspecto relevante da contribuição de Mattelart e Vitalis (2015) aqui examinada é a adoção de uma perspectiva histórica para entender o processo que leva à constituição do cibercontrole. Desse modo, a contribuição dos pesquisadores desafia visões que, abdicando da perspectiva histórica e abstraindo sua dimensão econômico-política, produzem compreensões limitadas do fenômeno que limitam as possibilidades de compreender de modo mais efetivo seu sentido político, suas especificidades e consequências sociais.

Na investigação realizada, os pesquisadores dedicam-se à construção de uma genealogia dos usos e funções das tecnologias de controle social, realizada a partir de um objeto específico, as técnicas de elaboração de perfis das pessoas com o objetivo de controlá-las. Trata-se do *perfilado*, termo procedente da linguagem policial ou industrial e que faz referência à forma de controle indireto das pessoas a partir da exploração das informações obtidas sobre elas. O perfilado é entendido como um *dispositivo tecnopolítico*. Para decifrá-lo, eles investigam o surgimento, os processos de experimentação, aperfeiçoamento e ampliação social desse dispositivo, desvendando sua articulação com interesses estatais, geopolíticos e mercadológicos que o engendram. No recorrido, os autores exploram suas transformações até sua expansão global, impulsionada pela razão mercantil da hegemonia neoliberal e pelo avanço desmedido das estratégias de segurança nacional, aliados às tecnologias digitais. Procuram examinar este fenômeno a partir da realidade local do Estado francês, explorando seus entrelaçamentos com dimensões globais do fenômeno. Discutem e denunciam os riscos à liberdade, à privacidade e à democracia instaurados nesse processo.

O olhar dos autores permite ver como os progressos políticos e relativos a direitos vêm acompanhados de formas de controle que limitam seus efeitos, e como a seguridade prescreve limites à liberdade. Mostra que as tensões entre liberdade e controle se complexificam historicamente e conhecem derivas, que se intensificam nos períodos de crise econômica, revolução política e de guerras, quando se faz ver de modo mais pronunciado o uso de meios de controle existentes bem como a invenção de tecnologias de vigilância mais eficazes.

Vale observar que a reconstrução histórica feita pelos pesquisadores abrange um período delimitado, detalhando estes processos a partir da realidade francesa e levando em conta principalmente suas articulações com o cenário europeu e estadunidense. Conforme os autores, o estado francês foi um dos primeiros a

experimentar técnicas de seguimento de populações, já em meados do século XIX, a partir de registros de pessoas delinquentes e reincidentes e da criação de um aparato estatal para medir e classificar crimes e delitos. Esse fenômeno não ficou circunscrito às instituições penais, expandindo-se para vários âmbitos das atividades econômicas e da vida cotidiana, o que, para os autores, expressa um *modo de governar*.

Para a finalidade de sistematização proposta neste trabalho, interessa recuperar traços fundamentais do processo detalhadamente examinado pelos pesquisadores. A reconstrução tem como ponto de partida o contexto da Revolução Industrial, mais especificamente a década de 1850, momento que marca um ponto de inflexão a partir do qual toma forma uma economia ancorada na divisão internacional do trabalho. O mercado se torna o eixo de um novo ordenamento das relações sociais, demandando liberdade de deslocamento de pessoas e mercadorias, fundamental para a realização da nova ordem econômica. Paradoxalmente, vão sendo criados e aperfeiçoados pelos Estados e, pela polícia, mecanismos de controle da circulação de nômades, profissionais ambulantes, sem-teto e imigrantes, demonstrando a obsessão dos poderes pelas populações marginalizadas. A estatística é posta a serviço dos controles policiais, colocando-se como ferramenta de regulação social, inaugurando a matematização da gestão das massas.

Neste período, a medição, o controle e a regulação do tempo passam a ordenar a experiência social. Ao controle das pessoas soma-se o de deslocamento contínuo das mercadorias. As fábricas se tornam um espaço-chave de experimentação e de aperfeiçoamento de dispositivos de controle, destinados ao seguimento dos deslocamentos dos trabalhadores e à cronometragem de seus gestos para desenvolver processos de maximização dos rendimentos dos fluxos de trabalho, na linha do taylorismo, alimentados também por estudos voltados à eficiência e à psicologia industriais.

Logo vão se consolidar os processos de taylorização do consumo, alimentados pela comunicação de massas e pela indústria da publicidade em desenvolvimento. A partir da década de 1940, o consumo vai se convertendo em campo de experimentação de técnicas de sondagem para controle dos comportamentos dos consumidores, com vistas a conhecer e atuar sobre suas necessidades. Esses processos antecedem e alimentam o desenvolvimento das estratégias contemporâneas de mineração de dados desenvolvidas no ambiente digital para produção de perfis dos consumidores.

Depois da Segunda Guerra Mundial, emerge o Estado de bem-estar social no contexto europeu, dividido entre o papel providencial e securitário. No seu âmbito, são criadas medidas de proteção às populações empobrecidas e

instauradas formas de seguimento das populações assistidas. Desenvolve-se um sistema burocrático de administração e gestão de dados das populações. Expandem-se os bancos de dados públicos, assim como os privados, ampliando as formas de vigilância e as possibilidades de controle social. Técnicas estatísticas vão ser colocadas a serviço destas formas de seguimento e de regulação social.

No pós-guerra, num cenário de Guerra Fria, a segurança nacional é colocada em primeiro plano no âmbito das políticas dos Estados. Os Estados Unidos desenvolvem um complexo militar-industrial, onde serão posteriormente inventados os sistemas teleinformáticos que permitirão criar os dispositivos futuros de vigilância massiva.

Desde a década de 1940, os Estados Unidos passam a desenvolver uma economia de guerra permanente, para a qual as tecnologias de informação e de comunicação têm papel-chave. Satélites, sistemas informáticos de espionagem, tecnologias de geolocalização, drones e armas não letais são parte dos dispositivos desenvolvidos, testados e aperfeiçoados nessa esfera.

A partir da década de 1970, temos o declínio do Estado-providência, acompanhado de crises de governabilidade da democracia e do modelo de crescimento econômico, que abre caminho para o neoliberalismo e suas políticas de desregulamentação selvagem. As tecnologias de informação passam a ser vistas pelas sociedades industriais como saída para a crise. A partir daí, elas vão se disseminando socialmente, o que possibilita uma revolução informática do controle. Nesse contexto, multiplicam-se os tratamentos informatizados de dados pessoais.

No começo do século XXI, a segurança nacional volta a ganhar relevo nas estratégias dos Estados ocidentais, agora com o pretexto de combate ao terrorismo. Surge a figura do Estado vigilante. A partir dos atentados de 11 de setembro de 2001, o governo estadunidense passa a reforçar seu arsenal securitário, civil e militar. Deflagra-se uma mobilização generalizada dos Estados ocidentais para a seguridade, que se reforça a partir dos atendados de 11 de março de 2004 em Madri, de 7 de julho de 2005 em Londres e de 7 de janeiro de 2017 em Paris. O avanço das dinâmicas securitárias repercute nos processos de comunicação e de circulação de pessoas, mensagens e bens.

Nesse cenário, a guerra contra o terrorismo se internacionaliza e se torna um elemento comum das políticas, doutrinas e estratégias de segurança em várias partes do mundo, com os países ocidentais em primeiro plano. Fortalecem-se as sinergias interagências e intersetores. As doutrinas de guerra passam a se orientar para o campo da informação, com o objetivo de atuar na capacidade de compreensão e de ação do "inimigo". Para os Estados Unidos, fazer operativa essa guerra requer reestruturar os mecanismos de coleta e de disseminação da

informação em nível mundial, colocar em rede as agências de inteligência e amplificar sua capacidade de análise.

A interconexão de bancos de dados policiais e administrativos se acelera nesse contexto, impulsionada pela preocupação das autoridades públicas de identificar focos potenciais de comportamentos violentos ou desviados. As medidas progressivamente implementadas pelos Estados estabelecem as bases de uma estrutura renovada de controle, assentada no aumento de bancos de dados e de suas interconexões, na melhoria de identificação das pessoas (especialmente através da biometria) e na experimentação de métodos automáticos de classificação e de detecção.

Durante muito tempo, a construção de bancos de dados e de perfis havia sido realizada pelos Estados. No período entre guerras, o desenvolvimento da indústria da *publicidade* e do *marketing* moderno leva ao aperfeiçoamento de métodos de observação e de análise de comportamento dos consumidores para o estabelecimento de perfis voltados ao conhecimento dos públicos, junto ao incremento das novas tecnologias.

Com o avanço da digitalização, consolidam-se monopólios fundados na exploração mercantil de dados pessoais, em geral assentados no oferecimento de serviços públicos gratuitos e na participação das pessoas em redes sociais. O aumento da capacidade de memória dos suportes digitais, assim como a desterritorialização dos processamentos, a automatização da coleta, o uso de algoritmos e o entrecruzamento e a difusão de dados potencializam a exploração de dados das pessoas.

O panorama contemporâneo de centralização da internet em torno de grandes corporações privadas, apontado por Mattelart e Vitalis (2015), é também considerado por outros pesquisadores, como Fiormonte e Sordi (2019), que reconhecem que as Gafam – Google, Apple, Facebook, Amazon, Microsoft, todas corporações estadunidenses – vêm dominando as diferentes facetas da rede em escala planetária. Pressionadas atualmente pelo império chinês, elas vêm procurando estender sua penetração através da inteligência artificial e da internet das coisas que o 5G fará possível.

Em termos de regulação, ao examinar os marcos desenvolvidos pelo Estado francês e estabelecer relações com outros do contexto da União Europeia e dos Estados Unidos, Mattelart e Vitalis (2015) constatam uma dessincronização cada vez mais manifesta entre os ritmos dos processos de informatização e os esforços jurídicos para proteção de seus abusos. Ainda assim, consideram sua importância simbólica, pois formalizam e precisam os direitos dos cidadãos sobre suas informações numa sociedade democrática. Eles apontam ainda as fortes distinções entre o modelo regulatório estadunidense e europeu em termos de

proteção da privacidade das pessoas. Refletem que a regulação deveria intervir desde a concepção desses automatismos, direção colocada pelo enfoque *privacy by design*, que propõe atuar na concepção de materiais, programas e arquiteturas de modo a garantir o respeito à vida privada.

A perspectiva de Shoshana Zuboff (2018) ajuda a complementar o exame de Mattelart e Vitalis (2015) em termos da especificidade do capitalismo emergente neste processo. A pesquisadora compreende que está em curso a emergência de uma nova lógica de acumulação, o *capitalismo de vigilância*, que se constitui gradualmente a partir da última década do século XX com a digitalização e sua penetração social, possibilitando um registro persistente e contínuo de dados que alimentam a lógica emergente do capitalismo.

Os métodos de produção de dados a partir da extração cotidiana de informações e as formas como adquirem valor refletem outras características dessa lógica, assentada na indiferença formal e na ausência de reciprocidades estruturais no relacionamento da empresa com seus "usuários". As pessoas são as fontes da extração de dados e os alvos finais das ações que tais dados produzem. A obscuridade dessas práticas é outra face da indiferença. Outro aspecto desse processo é a necessidade de aprimoramento de padrões, que leva à realização de experimentos contínuos.

Reconfigurações nas estruturas de poder se realizam nessa lógica emergente. O poder passa a se vincular à propriedade dos meios de modificação comportamental. A falsa consciência é produzida, também, pelos fatos ocultos da modificação mercantilizada do comportamento. Nessa nova forma de poder, o contrato e o Estado de direito são postos à prova. Na visada de Zuboff (2018), o trabalho da vigilância não leva à corrosão dos direitos de privacidade, mas à sua redistribuição. Esses direitos vão sendo concentrados em atores de vigilância privada e pública. Assim, a lógica de acumulação inclui capital e ativos de vigilância, mas também, direitos.

Não é possível finalizar as considerações sobre esse eixo da reflexão sem deixar de mencionar o cenário recente no qual se desenha um acirramento das suas lógicas: a crise deflagrada pela expansão mundial da covid-19, que convulsiona o conjunto das relações sociais do planeta. No contexto da pandemia, a necessidade de distanciamento físico associada a uma reorientação de atividades para o mundo digital vem beneficiando exponencialmente as corporações que têm seus modelos de negócio baseados na exploração de dados das pessoas. Além disso, vários Estados passaram a aplicar estratégias de vigilância digital com o intuito de controlar a disseminação da doença. Coreia do Sul, Singapura, China e também Taiwan e Hong Kong desenvolveram sistemas de cibervigilância a partir de aplicativos para *smartphones* com a finalidade de realizar seguimento

digital de cidadãos com a doença ou que estiveram presentes em zonas de contágio. O modelo, baseado no uso massivo de dados e associado a sistemas de videoproteção, vem sendo adotado também em países como Alemanha, Reino Unido, França e Espanha. Dados de provedores de telefonia móvel e de internet têm sido utilizados por Estados para prevenir a expansão da doença e monitorar os infectados. Os gigantes da internet Google e Apple também se associaram ao propósito de rastrear os infectados pela doença e vêm desenvolvendo tecnologias para alertar as pessoas quando elas chegarem perto de alguém que teve teste positivo para o novo coronavírus. Nesse processo, aprofundam-se os riscos diante da possibilidade de que as medidas de exceção adotadas possam permanecer no futuro, particularmente as que se vinculam à cibervigilância e ao biocontrole (Ramonet, 2020).

A NOVA FORMA DE GOVERNO INAUGURADA PELO CIBERCONTROLE

Na obra que estamos examinando, Mattelart e Vitalis (2015) refletem sobre a nova forma de governo inaugurada pelo cibercontrole. Para compreender suas especificidades, relacionam e distinguem essa forma de governo com aquela constituída na sociedade disciplinar. Partindo das reflexões de Deleuze sobre a *sociedade de controle*, os pesquisadores procuram demarcar distinções que expressam a passagem de um tipo de regime a outro.

A sociedade disciplinar, atuante por mais de três séculos na perspectiva de Foucault (1975 citado por Mattelart & Vitalis, 2015) e instaurada a partir do Renascimento, conforme Elias (1973 citado por Mattelart & Vitalis, 2015), caracteriza-se por inscrever a normalização social no interior do indivíduo. É marcada pela visibilidade de sua arquitetura e de seus dispositivos disciplinares. Essa visibilidade disciplinar induz ao controle do comportamento. O sujeito participa de sua normalização por meio de autorrestrição e autocontrole. Já na sociedade do cibercontrole, as tecnologias se caracterizam, de modo geral, pela invisibilidade e pela automatização. Sua eficácia, inclusive, se assenta na invisibilidade. O indivíduo é aparentemente livre, mas está permanentemente vigiado. Ele é objeto da informação e, em caso de comportamento desviante, são tomadas decisões que são imediatamente aplicadas.

O sistema de vigilância contemporâneo é marcado também pela fluidez, pela mobilidade e pela conectividade, características impulsionadas pelas tecnologias e redes de comunicação e de informação. Esse entorno digital facilita a comunicação, ao mesmo tempo em que se constitui como um cenário de controle permanente. Os conteúdos podem ser transmitidos instantaneamente,

armazenados e processados em qualquer lugar do planeta. Além disso, os dispositivos de controle se encontram, hoje, desterritorializados.

Nesses processos, emerge uma nova forma de governo fundada em predição e, sobretudo, em prevenção de comportamentos mediante a aplicação de algoritmos a quantidades massivas de dados para elaboração de perfis e estruturação do campo de ações possíveis dos indivíduos. Seus usos incluem redução de riscos e intervenção, pela detecção automática de comportamentos anormais antes que se produzam os atos delitivos e previsão de necessidades e desejos das pessoas a partir do trato de seus dados para performar o consumo. Esse viés antecipador e seu imediatismo são traços distintivos da cibervigilância em relação a outras formas de controle. Vale considerar que, embora se instaure uma nova forma de governo, isso não significa que a disciplina não continue atuando e que novas tecnologias de informatização e comunicação não possam, inclusive, prolongá-la.

Em relação a essa dimensão de análise, é interessante considerar outros aportes que convergem com a discussão de Mattelart e Vitalis (2015) e trazem elementos que a complementam. Alimentando-se das proposições foucaultianas[4], Silveira (2017) também concebe que, no contexto contemporâneo, inaugura-se um novo modo de governo no qual os algoritmos, como tecnologia, têm um papel fundamental. Em suas reflexões, o pesquisador procura examinar os algoritmos como tecnologia que tem um *logos* e que não é neutra. Como características, os algoritmos são "invisíveis, complexos e escritos em linguagem matemática" (p. 272). São produzidos dentro de uma racionalidade positivista, articulada pelo neoliberalismo, que reforça os discursos de tecnologia neutra. Como um conjunto de instruções codificadas para resolver problemas, expressando uma solução computacional relacionada a condições lógicas (conhecimentos sobre os problemas) a partir de estratégias destinadas à sua resolução, os algoritmos são desenvolvidos, em geral, dentro de empresas e corporações do mercado e expressam as intenções de seus criadores. Eles corporificam finalidades originais, mas essas podem ser alteradas pelos usuários e pelos próprios algoritmos se eles contiverem codificações de autocorreção e de aprendizagem.

Silveira (2017) salienta a necessidade de recuperar a crítica e pensar dimensão pública e as implicações políticas dos algoritmos. Eles envolvem a automatização do processo de análise de dados e, também, de tomada de decisão. Essa segunda dimensão comporta riscos para a sociedade. Seus resultados também não são previsíveis no caso daqueles que detêm capacidade de aprendizagem

[4] Silveira adota a perspectiva foucaultiana de governo que, em síntese, envolve "estruturar o eventual campo de ação dos outros (Foucault, 1995, citado por Silveira, 2017, p. 270). Assim, o governo inclui a condução de condutas e não se expressa apenas como confronto, mas se constitui, também, a partir de vínculos.

ou de correção a partir das ações realizadas anteriormente, o que dá a estas tecnologias uma autonomia decisória difícil de estimar. Outra característica é que são dispositivos performativos, podem engendrar práticas e procedimentos. Isso tem implicações que devem ser consideradas em várias dimensões, como nas decisões do setor público, em que "a responsabilidade pelos atos de gestão, transparência e estabilidade jurídica é fundamental" (p. 275).

Vale mencionar aqui, em relação aos riscos que os algoritmos podem comportar, aqueles sistematizados por Doneda e Almeida (2018) a partir do exame de trabalhos contemporâneos: "manipulação, viés, censura, discriminação social, violações de privacidade e dos direitos de propriedade, abuso do poder de mercado, efeitos sobre capacidades cognitivas, além da crescente heteronomia" (p. 145).

Em relação a essa discussão, Fiormonte e Sordi (2019) ajudam a pensar os algoritmos como dispositivos produtores de personalização, elemento-chave na produção da experiência do mundo digital das pessoas. A personalização colabora para manter sujeitos engajados a uma experiência das redes que se desenvolve integralmente nos limites traçados pelos algoritmos da plataforma. Os algoritmos também atuam no controle do tempo, instituindo uma obsolescência programada principalmente no âmbito dos usos. Assim, tais usos podem ser repetidos com intervalos curtíssimos, já que os algoritmos sempre serão capazes de organizar e inserir conteúdos novos.

Fernanda Bruno (2008) também reflete sobre a vigilância digital, entendida por ela como processo vinculado ao "monitoramento sistemático, automatizado e à distância de ações e informações de indivíduos no ciberespaço, com o fim de conhecer e intervir nas suas condutas ou escolhas possíveis" (p. 11). A reflexão sobre a natureza dos perfis gerados neste processo é interessante à discussão do cibercontrole. O processamento de dados não é mais voltado à extração de regularidades (médias) no seio de uma população para daí derivar normas. O perfil remete a padrões de ocorrência de certos fatores, a tendências e potencialidades, não a uma lei. Apropriadamente, a autora considera estas taxonomias como *máquinas epistêmicas*.

Outro aspecto interessante é a reflexão sobre estes perfis enquanto *máquinas identitárias*, que apresentam modos específicos de individualização. Os perfis são simulações de identidades, "tanto no sentido de antecipação como no de modelização" (Bruno, 2008, p. 14). Em contraste às vigilâncias disciplinares, que foram assentadas sobre modelos de individualização descendente, o controle digital é caracterizado pela "individualização transversal ou combinatória". Esse modo de individualização não apaga o anterior, mas se sobrepõe a ele. As pessoas mais conectadas, visíveis e participativas nas redes informacionais são

mais amplamente vigiadas. Os perfis também configuram efeitos de identidade na medida em que são preditivos e atuam performativamente.

POSSIBILIDADES DE RESISTÊNCIA E DE CONTESTAÇÃO SOCIAL

O olhar de Mattelart e Vitalis (2015) não deixa de considerar as contradições, fissuras e possibilidades de resistência ao cibercontrole. Os pesquisadores reconhecem as possibilidades trazidas pelas novas tecnologias digitais para as sociedades em termos de geração e de compartilhamento de conhecimentos e de informações, de acessibilidade às condições de produção de conteúdos, de estabelecimento de vínculos estendidos, de experimentações diversas, de constituição de novos movimentos e ativismos, de reflexão e criação estética. Também consideram as possibilidades de construção de autonomia informacional no contexto do cibercontrole.

A *mobilização da opinião pública* é um elemento importante para o questionamento e para impulsionar ações que permitam controlar tanto governos quanto nas instituições privadas em termos de abusos. Mais recentemente, tem se ampliado a partir de revelações sobre processos de vigilância e espionagem, como aqueles realizados por Snowden em julho de 2013 em relação ao programa clandestino *Prism*, que deu à National Security Agency (NSA) e ao Federal Bureau of Investigation (FBI) acesso a dados da companhia telefônica Verizon e de empresas de internet como Microsoft, Yahoo, Google, Facebook, YouTube e Apple. Os *hackers*, por sua competência técnica e suas ideias libertárias, têm ocupado a vanguarda nos processos de crítica e de protesto, sendo o WikiLeaks um exemplo emblemático a este respeito.

No *campo dos usos*, Mattelart e Vitalis (2015) discutem as possibilidades das pessoas também acederem às ferramentas de controle utilizadas pelos controladores e se converterem em vigilantes. Nesse sentido, apontam várias formas de uso de tecnologias a serviço da vigilância cidadã para denunciar os métodos e as formas de abuso dos vigilantes. No cotidiano, pessoas com maior competência técnica apresentam maiores possibilidades de se proteger do cibercontrole através do uso de ferramentas que preservem o anonimato ou de encriptação. Elas também podem exercer práticas de desconexão ou, ainda, eleger não utilizar ambientes cujas práticas abusivas vão sendo conhecidas.

Em relação à dimensão dos usos e apropriações digitais realizados pelas pessoas, David Lyon (2018) permite agregar outros aspectos a essa discussão. O pesquisador argumenta sobre a necessidade de investigação do que chama de cultura da vigilância para dar a ver mais claramente as relações do controle digital com as pessoas na vida cotidiana. A noção de cultura de vigilância, em

construção pelo pesquisador, alude aos modos de vida constituídos pelos sujeitos que experimentam a vigilância digital. Inclui pensar as práticas e significações relativas à vigilância nos ambientes digitais, ou seja, as compreensões e formas de atuar dos sujeitos nestes contextos permeados pelo cibercontrole. Tal cultura é multifacetada e varia conforme países, regiões e uma série de outros fatores. É socialmente construída e, portanto, pode ser desafiada e reconstruída, o que abre caminho para a agência em termos de construção da cidadania digital. Nesse sentido, acrescentaria, deveríamos pensar em culturas de cibervigilância no plural, dado que está constituída diversamente em termos de práticas e de concepções sociais.

A perspectiva de pensar o cibercontrole desde os usos e apropriações de sujeitos, grupos e coletivos é, a meu ver, uma dimensão fundamental de investigação, em conexão com uma problematização mais ampla de tais processos. Para investigar essa dimensão, é importante considerar competências, práticas e significações relativas à vigilância nos ambientes digitais, ou seja, compreensões, saberes e formas de atuar nesses contextos permeados pelo cibercontrole. Essas relações são complexas e podem incluir formas de reprodução, cumplicidade, negociação e/ou resistência ao cibercontrole nas práticas comunicativas digitais.

Algumas investigações que tenho orientado nos últimos anos, voltadas a entender apropriações das mídias digitais por coletivos e movimentos sociocomunicacionais, têm incluído questões relativas à cibervigilância. É o caso da pesquisa de doutorado de Marina Albuquerque (2018), que investigou os usos das redes digitais por dois coletivos vinculados a novos movimentos sociocomunicacionais urbanos de Porto Alegre. Em relação a essas questões a pesquisa, cujos dados foram coletados em 2016 e 2017, evidencia que os sujeitos entrevistados tinham conhecimento de aspectos da vigilância digital, inclusive porque informações digitais de integrantes foram usadas pela polícia para criminalizar pessoas dos coletivos. Entretanto a reflexão sobre essa problemática não havia alcançado espaço mais amplo nos coletivos nem o desenvolvimento de estratégias e/ou táticas mais efetivas para lidar com o cibercontrole.

Explorações empíricas desenvolvidas entre 2018 e 2019 com integrantes de coletivos vinculados ao movimento feminista de Porto Alegre e de Salvador, realizadas por Bruna Lapa Guia, que desenvolve tese de doutorado sob minha orientação, apontam que a preocupação com o cibercontrole estava presente em vários desses cenários, sobretudo a partir da nova conjuntura brasileira vinculada ao governo Bolsonaro, iniciado em 2019, que trouxe riscos mais amplos de criminalização para os movimentos sociais. Diante da insegurança e do receio de vigilância estatal e civil nas redes sociais, as mulheres vinham debatendo alternativas, como a migração a aplicativos mais seguros, a espaços

digitais alternativos e livres. Um dos coletivos abordados vinha substituindo gradualmente os sistemas operacionais dos suportes usados (como computadores e celulares) para *softwares* livres. Outra medida tomada era o desligamento de celulares em reuniões. Além disso, outra tática, motivada por uma apreensão diante da crescente possibilidade de criminalização dos movimentos sociais, era o afastamento dos meios tecnológicos e o investimento na comunicação cara a cara, menos passível de vigilância. Essa retração em relação a usos tecnológicos também se vinculava à percepção de que as mensagens emitidas e compartilhadas no meio digital nem sempre conseguiam atingir as mulheres com quem os movimentos feministas pretendiam dialogar, devido a limitações de acesso e às configurações algorítmicas da internet.

* * *

Recuperei neste texto contribuições da obra *De Orwell al cibercontrole*, de Armand Mattelart e André Vitalis (2015), para pensar o cibercontrole. Elas nos permitem dimensioná-lo como um fenômeno situado historicamente, que se constitui a partir de um processo em que se podem ver conexões e pontos de ruptura com outras formas de controle social. Nesse processo, os dispositivos foram sendo testados, experimentados e renovados em função de interesses estatais, geopolíticos, econômicos e de suas conexões.

Outro aporte da obra é relativo à compreensão das especificidades dessa nova modalidade de exercício do poder e às suas distinções com o controle disciplinar que o precedeu (ainda operante em nossas sociedades). O cibercontrole se caracteriza por sua invisibilidade, opacidade, automatização, por ser fundado na predição e, sobretudo, na prevenção de comportamentos a partir da aplicação de algoritmos a quantidades massivas de dados para construção de perfis e performação do campo de ações possíveis dos indivíduos.

A obra também nos permite refletir sobre possibilidades de resistência, contestação e regulação do cibercontrole. As contribuições examinadas reconhecem contradições no campo das regulamentações vinculadas à agressividade das estratégias das corporações e à velocidade das inovações tecnológicas; atentam para o papel da mobilização da opinião pública, particularmente através da divulgação massiva de fatos associados ao cibercontrole e para possibilidades derivadas da apropriação social das tecnologias a partir do conhecimento das ferramentas e da vigilância cidadã.

É fundamental, do meu ponto de vista, incluir a problematização do cibercontrole nas pesquisas contemporâneas que se debruçam sobre fenômenos vinculados à comunicação digital. E, nesse âmbito, o trabalho desses autores

oferece uma contribuição efetiva e instigante, tanto pela riqueza da investigação e das compreensões que oferece quanto pelos interrogantes que abre à investigação. A obra também brinda subsídios importantes para aprofundar os processos formativos nos âmbitos acadêmicos e sociais sobre as lógicas do cibercontrole.

Sinalizo aqui duas demandas investigativas provocadas pela reflexão do trabalho de Mattelart e Vitalis (2015). Uma delas é relativa à necessidade de nossas pesquisas comunicacionais investirem na compreensão das especificidades deste processo histórico e de suas nuances contemporâneas no contexto brasileiro e latino-americano. Em direção convergente a essa demanda, Domenico Fiormonte e Paolo Sordi (2019) argumentam sobre a necessidade de uma história crítica das tecnologias de controle que deve levar em conta, entre outros elementos, o lugar do Sul nestes processos. Uma das dimensões a ponderar é a construção material do mundo digital: boa parte dos recursos naturais que alimentam sua constituição procede de países do sul do mundo. O Sul, nesse cenário, ocupa o lugar de provedor de recursos e de produtor de dados a partir de um trabalho não remunerado. Um novo colonialismo se instaura na visão destes pesquisadores: o *colonialismo de dados*.

Outro campo que requer esforço investigativo é relativo aos processos de avanço do cibercontrole no contexto da pandemia do coronavírus. Nessa dimensão, serão necessários investimentos para dar conta das diferentes facetas vinculadas ao aprofundamento do cibercontrole durante a pandemia e seus desdobramentos futuros, em distintas dimensões, como a vinculada ao teletrabalho e à teleducação.

Essas são algumas das provocações que nos traz a obra de Mattelart e Vitalis (2015), uma obra que inquieta, instiga, desafia e convida a assumir o desafio científico, ético e político de aprofundar a compreensão desse fenômeno complexo e multifacetado, e de colaborar para a produção de resistências e de alternativas aos processos perversos que o cibercontrole engendra.

REFERÊNCIAS

Albuquerque, M. Z. (2018). *Entre as redes sociais digitais e as ruas: Processos comunicacionais dos coletivos Defesa Pública da Alegria e Bloco de Lutas* [Tese de doutorado, Universidade do Vale do Rio dos Sinos]. Repositório Institucional da UNISINOS. http://bit.ly/38p7Yfh

Bruno, F. (2008). Monitoramento, classificação e controle nos dispositivos de vigilância digital. *Revista FAMECOS*, *15*(36), 10-16. https://doi.org/10.15448/1980-3729.2008.36.4410

Doneda, D., & Almeida, V. A. F. (2018). O que é governança de algoritmos? In F. Bruno, B. Cardoso, M. Kanashiro, L. Guilhon, & L. Melgaço (Orgs.), *Tecnopolíticas da vigilância: Perspectivas da margem* (pp. 141-148). Boitempo.

Fiormonte, D., & Sordi, P. (2019). Humanidades Digitales del Sur y GAFAM: Para una geopolítica del conocimiento digital. *Liinc em Revista*, *15*(1), 108-130. https://doi.org/10.18617/liinc.v15i1.4730

Lyon, D. (2018). Cultura da vigilância: Exposição e ética na modernidade digital. In F. Bruno, B. Cardoso, M. Kanashiro, L. Guilhon, & L. Melgaço (Orgs.), *Tecnopolíticas da vigilância: Perspectivas da margem* (pp. 151-179). Boitempo.

Maldonado, A. E. (2015). *Epistemología de la comunicación: Análisis de la vertiente Mattelart en América Latina*. Ciespal.

Mattelart, A., & Vitalis, A. (2015). *De Orwell al cibercontrol*. Gedisa.

Silveira, S. A. (2017). Governo dos algoritmos. *Revista de Políticas Públicas*, *21*(1), 267-281. http://dx.doi.org/10.18764/2178-2865.v21n1p267-281

Ramonet, I. (2020, 30 de abril). Ante lo desconocido la pandemia y el sistema-mundo. *Le Monde Diplomatique*. http://bit.ly/34wJeRi

Zuboff, S. (2018). Big other: Capitalismo de vigilância e perspectivas para uma civilização da informação. In F. Bruno, B. Cardoso, M. Kanashiro, L. Guilhon, & L. Melgaço (Orgs.), *Tecnopolíticas da vigilância: Perspectivas da margem* (pp. 17-68). Boitempo.

Artigo recebido em 30 de setembro e aprovado em 15 de dezembro de 2020.