Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Tecnologias da informação e comunicação, vigilância e neoliberalismo

Gisele Zanola & Otto Sanchez-Crespo da Rosa

Resumo: Em vista da discussão acerca da legitimidade do emprego de tecnologias de vigilância em massa no combate à pandemia do novo coronavírus, este artigo pretende investigar aquilo que, no fenômeno da vigilância, não é fruto de seu uso contextual, mas decorre da própria estrutura da produção e do consumo das Tecnologias da informação e comunicação, como argumenta Julian Assange. Nossa exposição considera que essas tecnologias operam segundo a racionalidade do neoliberalismo, entendida aqui no sentido de Dardot e Laval, enquanto expansão da lógica de mercado para todos os âmbitos da vida.
Palavras-Chave: pandemia; neoliberalismo; tecnologias de informação e comunicação; vigilância em massa.

Introdução

A partir de março de 2020, em resposta à eclosão da pandemia do novo coronavírus (SARS-CoV-2), muitos países instituíram medidas de isolamento social como parte de um plano de saúde pública para o controle da proliferação do vírus. Nesse contexto, as formas de sociabilidade presenciais se restringiram dramaticamente, dando um lugar cada vez maior às interações remotas, o que tornou mais perceptível a centralidade das tecnologias da informação e comunicação na organização da vida, seja para fins profissionais, educacionais, políticos ou de lazer. Assim, intensificou-se, com a finalidade de rastrear a propagação da doença Covid-19, a implementação de tecnologias informacionais de vigilância em massa. Argumentaremos ao longo do texto que essa finalidade, para a qual os esforços de aplicação das TICs têm sido voltados neste contexto específico, já está posta no cerne da organização das próprias tecnologias de informação e comunicação como um todo.

A tecnologia de vigilância mais evidente no contexto atual refere-se ao chamado "rastreamento de contatos" (*contact tracing*), considerado pelas autoridades governamentais de vários países como uma forma de rastreamento mais eficaz do que a realizada manualmente por telefonistas (*manual tracing*). Essa tecnologia digital de rastreamento de contatos mostrar-se-ia mais eficaz por sua capacidade de cruzar imediatamente informações de diversas fontes, como de câmeras de segurança, cadastramento biométrico, radares de trânsito, dados de *check-ins* de trens e aeroportos, drones, transações comerciais, dispositivos de posicionamento global (GPS), antenas de telefonia celular, buscas na Internet e outros dados provenientes dos dispositivos móveis dos cidadãos. O cruzamento dessas informações, aliado a um programa de testagem massiva da doença, forneceria uma base de dados consistente que possibilitaria o monitoramento da circulação de pessoas infectadas e igualmente de pessoas não infectadas.

As autoridades de vários países asiáticos aderiram à coleta compulsória desses dados. Em Hong Kong, para manter um alto índice de isolamento social, as autoridades implementaram uma

quarentena obrigatória de 14 dias para todas as pessoas recém-chegadas do exterior, exigindo delas que tivessem em seus celulares o aplicativo *StayHomeSafe*, ao mesmo tempo que utilizassem uma pulseira de tecnologia *geofencing*, capaz de identificar aqueles que infringem a reclusão, sob pena de seis meses de prisão e multa de US$ 3.200,00. Na Índia, medidas parecidas foram tomadas. Os cidadãos que não tivessem em seus dispositivos o aplicativo *Aarogya Setu* poderiam perder o emprego, ser presos ou pagar multa. Por sua vez, na Coreia do Sul, empresas privadas, além do governo, desenvolveram aplicativos como o *Corona100m*, que rastreia e comunica os usuários sobre pessoas infectadas em um raio de 100 metros. Junto ao dado sobre a infecção pelo coronavírus, o aplicativo mostra a data de diagnóstico do indivíduo infectado, nacionalidade, sexo, idade e informações do seu trajeto. Em Taiwan, foi desenvolvido um sistema de cruzamento de dados que combina o histórico de viagens de 14 dias dos pacientes infectados com suas informações de identificação, facilitando, assim, seu rastreamento contínuo. Na China, o banco de dados pessoais robusto de monitoramento das empresas *Alibaba* e *Tencent* foi utilizado pelo governo para a contenção da proliferação do vírus. Uma de suas técnicas foi o emprego de câmeras de vigilância na frente das casas de pessoas acometidas. Israel é outro exemplo da utilização de sistema de vigilância em massa, empregando o aparato de sua agência de segurança interna, Shin Bet, no seu plano sanitário (cf. LE, 2020).

Ainda que as agências de segurança interna de países ocidentais como o Reino Unido e os Estados Unidos possuam um histórico de acordos secretos com empresas de telecomunicações para a coleta de informações de todo o tráfego de telefonia e internet que passa por seu território, sem qualquer transparência e prestação de contas, como visto nas denúncias do ex-funcionário da NSA Edward Snowden, a legislação proíbe qualquer interceptação sem o consentimento do usuário (cf. GREENWALD, 2014, pp. 126-127). Dessa forma, nesses países, como na maior parte dos países europeus, que implementa o Regulamento Geral de Proteção de Dados (*GPDR*, na sigla em inglês), o rastreamento de contatos depende da adesão voluntária da população a aplicativos que identificam contatos próximos via *bluetooth* para a garantia de alguma eficácia na contenção da transmissão do vírus. Empresas privadas como Google e Apple, por exemplo, fizeram parceria com os governos do Reino Unido e da França para o desenvolvimento desses aplicativos.

No caso do Brasil, o ministro da Ciência, Tecnologia e Inovações, Marcos Pontes, buscou um acordo com as principais empresas de telecomunicações – Algar, Claro, Oi, Tim e Vivo – na tentativa de realizar monitoramento massivo e, de certa forma, também compulsório de dados de geolocalização de 222 milhões de linhas telefônicas móveis (cf. SARAIVA apud. LOURENÇO, 2020). Essa tentativa não foi bem sucedida, tendo sido desaconselhada pelo presidente Jair Bolsonaro. Entretanto, o próprio presidente postergou, por medida provisória, a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), altamente inspirada no seu correlato europeu, que enfim entrou em vigor em outubro de 2020. Mesmo assim, no que diz respeito ao controle da pandemia, vários governos estaduais e municipais contrataram o serviço de monitoramento de *startups*, como a Inloco, que, baseando-se em dados de geolocalização coletados por rastreadores (trackers) contidos em aplicativos de

celular diversos, como os de entregas, os bancários e os de compras online, produzia mapas de taxa de isolamento social. A empresa alegava que os dados coletados eram próprios dos dispositivos móveis e não identificavam seus portadores, o que supostamente garantiria anonimato na análise dessas informações. O fato é que, após a entrada em vigor da LGPD, a empresa se viu obrigada, por sua incapacidade de assegurar transparência no processamento dos dados, a encerrar tais atividades.[1]

Nos primeiros meses da pandemia, argumentou-se que o sucesso de países como Coreia do Sul, Taiwan, Vietnã, China e Hong Kong para conter o aumento do número de novos casos foi devido ao emprego compulsório do aparato de vigilância em massa (cf. ZASTROW, 2020). Segundo essa mesma lógica, o fracasso de países ocidentais nessa tarefa teria sido decorrente, em grande medida, por depender de uma adesão voluntária da maioria da população – ao menos 60%, segundo estudo de epidemiologistas de Oxford –, algo que não foi alcançado por nenhum deles (cf. LE, 2020). Contudo, outras análises indicam que não é possível estabelecer uma correlação entre a diminuição da transmissão e a coleta compulsória de dados pessoais. Fatores como o cumprimento das medidas de isolamento social, o uso de máscaras de proteção respiratória, a disposição individual de pessoas infectadas em identificar sua cadeia de transmissão, além da testagem em massa da população – o que implica em uma ação coordenada do sistema de saúde –, parecem ter sido mais decisivas para a diminuição de infecções em certos países do leste da Ásia (HUANG et. al., 2020).

Dito isso, ainda que a correlação entre vigilância em massa e o êxito no enfrentamento da pandemia não seja verificável, uma vez que outros fatores têm peso fundamental nesse processo, os diferentes usos das TICs foram continuamente legitimados em prol dessa correlação, como no caso do Brasil. No entanto, é preciso observar que a utilização da vigilância em massa durante a pandemia se tornou possível apenas na medida em que as TICs já dispunham de uma estrutura desenvolvida, dotada de enorme capacidade de coleta e armazenamento de dados. Nesse sentido, passaremos a uma análise de sua estrutura material, tendo em mente que as condições de sua produção nos permitem vislumbrar o fenômeno da vigilância em massa como um fenômeno mais abrangente, cujo desenvolvimento coaduna com a ascensão do neoliberalismo, entendido por nós como a expansão "da lógica do mercado como lógica normativa generalizada, desde o Estado até o mais íntimo da subjetividade" (DARDOT; LAVAL, 2016, p. 34). Em outras palavras, trata-se de compreender como o próprio objeto tecnológico é construído a partir de um reforço mútuo entre interesses econômicos e interesses políticos que culmina na vigilância em massa, ora para garantir a lucratividade dos investimentos, ora para expandir o poder de governo sobre as populações.

Estrutura das TICs, vigilância em massa e neoliberalismo

As Tecnologias de Informação e Comunicação são, mais do que dispositivos de comunicação, como os microcomputadores, os telefones celulares, ou a rede que os conecta – a internet –, uma estrutura muito complexa por meio da qual a própria existência dos dispositivos e da rede se

1 Ver nota da empresa sobre a descontinuidade dessas atividades: https://mapabrasileirodacovid.inloco.com.br/pt/.

torna possível. Por isso, na literatura especializada, as TICs são definidas como os meios técnicos de armazenamento, transmissão e manipulação de informações, o que pode congregar, além dos dispositivos pessoais, o extenso cabeamento transoceânico e mesmo as chamadas torres de servidores (*server farms*) (cf. YATSKO; SUSŁOW, 2015, p. 1). A complexidade dessa estrutura é analisada por Julian Assange na obra *Cypherpunks: liberdade e o futuro da internet*, de 2012, da qual extraímos o seguinte trecho:

> Com o passar do tempo, parece que desenvolvemos técnicas cada vez mais sofisticadas. Algumas dessas técnicas podem ser democratizadas; podem ser disseminadas para todo mundo. Mas a maioria delas – devido a sua complexidade – é de técnicas que se formam como resultado de organizações fortemente interconectadas, como a Intel Corporation. Talvez a tendência subjacente à técnica seja a de passar por esses períodos de descoberta da técnica, de centralização da técnica, de democratização da técnica, quando o conhecimento sobre como fazer transborda para a próxima geração que é educada. Mas penso que a tendência geral da técnica seja a de centralizar o controle naquelas pessoas que detêm seus recursos físicos.
> Algo como uma fabricante de semicondutores é, penso, o exemplo cabal disso, para a qual se precisa de uma tal ordem que o ar seja puro, para a qual se faz necessária uma planta de fábrica com milhares de pessoas dentro dela que tenham de usar toucas para isolar o processo de produção dos semicondutores de qualquer fragmento de pele e fio de cabelo, um processo de múltiplas etapas que é extremamente complicado. E há literalmente milhões de horas de conhecimento de pesquisa possuídas pela organização produtora de semicondutores. Se eles forem populares – e eles são, já que sustentam a internet –, então a fabricação de semicondutores está inscrita (*coded*) na liberação da internet. E na produção de semicondutores está inscrita a capacidade de que qualquer um que tenha o controle físico da fabricante de semicondutores possa extrair dela concessões enormes.
> Assim, fundamentando a revolução das comunicações de alta tecnologia – e a liberdade que extraímos dela – está toda a economia de mercado moderna, transnacional, globalizada e neoliberal. Na verdade, é seu ponto mais alto. Esse é o auge, em termos de realização tecnológica, do que a economia moderna globalizada e neoliberal pode produzir. A internet é sustentada por interações comerciais extremamente complexas entre fabricantes de fibra óptica, fabricantes de semicondutores, companhias de mineração que extraem todo esse material, e todos os lubrificantes financeiros que possibilitam o comércio, tribunais para garantir a aplicação das leis relativas à propriedade privada e assim por diante. Então na verdade ela [a internet] é o topo da pirâmide de todo o sistema neoliberal. (ASSANGE et al., 2012, p. 26-27; 2013, pp. 46-47, trad. própria)

Antes de tudo, é preciso frisar que a concepção de técnica empregada por Assange situa as TICs em um quadro ainda mais abrangente do que a definição usual dada pelos especialistas. Para o programador e fundador do Wikileaks, os objetos tecnológicos não podem ser analisados isoladamente das interações sociais que possibilitam sua produção, reprodução e circulação. Assim, a técnica é caracterizada pela "interação sistematizada" entre a estrutura social e os objetos tecnológicos (cf. id., 2012, p. 26; 2013, p. 46). Especificamente no que diz respeito às TICs, elas são dotadas de uma complexidade tal que sua criação, bem como seu desenvolvimento, torna-se possível apenas mediante a concentração dos recursos físicos necessários e do conhecimento técnico-científico historicamente acumulado.

A internet, enquanto parte fundamental das TICs, é considerada por Assange como a expressão máxima dessa concentração porque ela exige uma integração internacional não apenas de ordem tecnológica, mas também de ordem econômica, política e jurídica. Em termos mais objetivos, multinacionais mineradoras, indústrias de alta tecnologia (fabricantes de semicondutores), empresas de *software*, bancos de investimento, governos de vários países e uma legislação internacional de proteção à propriedade intelectual convergem no desenvolvimento da infraestrutura da internet, cada qual em seu respectivo ramo de atuação. Por sua vez, a internet reforça, em virtude de sua natureza centralizadora, a formação de oligopólios em nível mundial e a expansão de poder político

naqueles que concentram os recursos para a sua produção e manutenção. O que confere unidade e permite a reprodução de toda essa estrutura – material e jurídica – é, defendemos, a "racionalidade política e social articulada à globalização e à financeirização do capitalismo", em suma, a lógica do neoliberalismo (DARDOT; LAVAL, 2016, p. 190).

A compatibilidade que visualizamos imediatamente entre a concepção de neoliberalismo empregada por Assange e aquela de Dardot e Laval se justifica pela negação da ideia de uma exclusão da participação do Estado no projeto neoliberal. Pelo contrário, na passagem do estado de bem-estar social do pós Segunda Guerra ao neoliberalismo, a função do Estado é redefinida: ele, por meio do sistema jurídico, deixa de representar uma barreira ao funcionamento do mercado e passa a garantir e promover a mercantilização progressiva de novos setores. Assim, a lógica do Estado e a lógica empresarial se mesclam, aprofundando o cerceamento das liberdades individuais, tanto pela mercantilização das preferências pessoais – que é feita pelas empresas de software – quanto pelo aumento de poder de vigilância dos órgãos de segurança nacionais. Um breve percurso pela história das TICs, especialmente no caso da internet, ilustra a redefinição do papel do Estado em relação ao novo modelo de negócios dos oligopólios multinacionais nascentes, principalmente pela via da vigilância em massa.

Embora isso aconteça paulatinamente, a expansão e desenvolvimento das TICs coincide com o momento histórico de ascensão da racionalidade neoliberal, tanto em relação ao desenvolvimento da computação, quanto em relação à criação da rede mundial de computadores (a internet). Nesse percurso, entendemos que a história do computador possui uma única inflexão ao neoliberalismo, ao passo que o desenvolvimento da internet conta com quatro momentos específicos e progressivos até o aprofundamento completo da racionalidade neoliberal. São eles: i) até por volta de 1984, quando o neoliberalismo ainda não se fazia sentir na implementação da infraestrutura do sistema, com centralidade do financiamento e orientação estatais das pesquisas; ii) por volta de 1985 a 1991, primeiro momento neoliberal da internet, em que ocorre sua reorientação para os usos civil e privado, com a ampliação do acesso por meio de parcerias público-privadas; iii) de 1991 a 2001, segundo momento neoliberal, em que há mundialização da rede, privatização completa da administração e abertura das empresas do setor para o capital financeiro, além do fortalecimento dos direitos de propriedade intelectual; e iv) a partir de 2001, consolidação da virada neoliberal, em que o Estado e as corporações se associam no emprego irrestrito da vigilância em massa.

A despeito de uma consideração aprofundada da história da computação em particular, podemos dizer que a manifestação do neoliberalismo na computação é ligeiramente anterior àquela do neoliberalismo na internet. Se tomarmos a reflexão de Stallman à luz da concepção de neoliberalismo de Dardot e Laval, o ponto de inflexão para o neoliberalismo na computação ocorre quando, no começo dos anos 1980, a mercantilização se estende do *hardware* ao *software* agressivamente, já que a queda do preço do *hardware* impelia as companhias a encontrar outra fonte de lucro, como fez a Microsoft, ao impedir, por meio de licenças com direito de exclusividade ao proprietário, o acesso

e a modificação de seus códigos-fonte.[2] Além disso, é preciso observar que o desenvolvimento da internet é dependente do desenvolvimento avançado da computação, que, histórica e logicamente, é anterior a ele. Isto posto, pretendemos considerar a história da computação apenas na medida em que é subjacente ao funcionamento da internet. Trata-se de uma escolha teórica que tem como principal motivação um comentário preciso sobre o lugar que a internet ocupa no "topo da pirâmide de todo o sistema neoliberal" (ASSANGE et al., 2012, p. 26-27; 2013, pp. 46-47).

No que se refere à história da internet, no início dos anos 1980, as pesquisas para o desenvolvimento das TICs, que se concentravam majoritariamente nos Estados Unidos, eram financiadas, na sua maior parte, por governos e realizadas por órgãos militares e por universidades, com exceção de apenas alguns laboratórios privados, como o Bell Labs, o IBM Research e o Fairchild Semiconductor. A construção da ARPANET (acrônimo de *Advanced Research Projects Agency Network*), a primeira rede de computadores, exemplifica o enquadramento estatal nos primórdios da internet. Sob a administração do Departamento de Defesa dos Estados Unidos, ela interligava computadores das principais universidades do país, como MIT, UCLA, Stanford, Harvard, dentre outras, em uma rede de livre colaboração entre os pesquisadores. Isso permitiu que, entre 1981 e 1982 se realizasse, com o financiamento estatal da Fundação Nacional de Ciências (*National Science Foundation, NSF* na sigla em inglês), a padronização da internet em um único protocolo, o *Internet Protocol Suite* (TCP/IP), o que foi fundamental para sua disseminação. Logo, em 1983, a internet passou a ter seu desenvolvimento completamente civil, com a saída da administração militar por meio da criação de uma rede interna própria, a MILNET (cf. RYAN, 2010, p. 90).

Já a partir da segunda metade dos anos 1980, houve uma privatização paulatina da internet, em concordância direta com o projeto neoliberal de transferência de empresas públicas para o setor privado (cf. DARDOT; LAVAL, 2016, p. 190-191). Nesse contexto, a Fundação Nacional de Ciências e as empresas Merit, IBM e MCI compuseram uma ONG sem fins lucrativos – chamada ANS (*Advanced Network Service*) – cuja responsabilidade era a de instalar e realizar a manutenção de servidores e dos próprios backbones[3] da nova rede, a NSFNET (*National Science Foundation Network).*[4] Aqui, a privatização não representou a comercialização da internet em si, mas sim a entrada de empresas privadas na criação e manutenção de um sistema público. Apesar disso, pouco tempo depois, em 1991, as mesmas empresas e a Fundação Nacional de Ciências criaram uma subsidiária com fins lucrativos, a *Advanced Network Service Commercial plus Research and Education* (ANS CO + RE), a primeira provedora comercial de acesso à internet.

Contudo, foi com o sistema de documentos de internet *World Wide Web*, publicado sob licença aberta no mesmo ano de 1991, que as tecnologias da informação e comunicação começaram a ser extensamente desenvolvidas e utilizadas mundo afora como ferramentas de mediação de boa parte

---

2 Sobre o movimento pelo software livre, ver STALLMAN, 2002, p. 173.

3 Backbones são supercomputadores que servem como nós por meio dos quais todo o tráfego da internet passa.

4 Se seguirmos a hipótese de Dardot e Laval acerca do sentido das parcerias público-privadas (2016, p. 306-307), a construção da NSFNET com apenas um terço de recursos públicos ocorreu devido à diminuição de recursos públicos disponíveis resultantes dos cortes neoliberais e ao discurso nascente de que a administração privada era mais eficiente do que a estatal.

das interações humanas. Ao mesmo tempo, ironicamente, com a permissão legal de transações comerciais na internet a partir de 1995 (cf. RYAN, 2010, p. 120), a expansão vertiginosa do mercado de ações das novas empresas do setor de telecomunicações e internet – o que criou a bolha da internet na bolsa de valores NASDAQ, que estourou em 2000 – e, também, o fortalecimento do arcabouço jurídico de propriedade intelectual,[5]foi consolidado o modelo privado da internet.

A reentrada do Estado na estruturação da internet ocorreu por meio das resoluções legislativas após os atentados de 11 de setembro de 2001. A formulação da emenda *Patriot Act* à Lei de Vigilância de Inteligência Estrangeira (FISA, na sigla em inglês), nos Estados Unidos, estabeleceu condições jurídicas para que o órgão de inteligência interna norte-americano NSA (*National Security Agency*) coletasse e armazenasse, sem a necessidade de mandado judicial, informações sensíveis de pessoas suspeitas de envolvimento com o terrorismo (JAEGER et al., 2003).[6] Pouco tempo depois, em 2005, denúncias de um funcionário da companhia de telecomunicação AT&T apontaram a existência de acordos sigilosos entre a empresa e a NSA, que incluíam "uma instalação de interceptação estratégica [...] que disponibilizava acesso a troncos de fibra óptica contendo tráfego em *backbones* de acesso à internet, possibilitando a vigilância de todo o conteúdo que passava pela instalação, tanto estrangeiro quanto nacional" (cf. ASSANGE et al., 2012, pp. 169-170; 2013, p. 60). A Emenda à FISA de 2008 institucionalizou, por sua vez, por meio da seção 702, essa prática de interceptação, com a condição de que a NSA entregasse relatórios anuais à Corte da FISA com "os alvos" do respectivo ano a fim de obter autorização para tal. Segundo a denúncia do ex-funcionário da NSA Edward Snowden, o órgão estatal construiu um programa de vigilância em massa denominado PRISM, no qual eram coletados conteúdos de e-mail, mensagens instantâneas, vídeos, fotos, transferências de arquivos, chamadas telefônicas por VoIP, videoconferências, logins e detalhes de contas de rede social, contando com a anuência de empresas do ramo de telecomunicações e internet, como Facebook, Google, Apple, YouTube, Microsoft, entre outras (cf. GREENWALD, 2014, p. 81-82).[7]

Conjuntamente à reformulação do papel do Estado nesse novo estágio de desenvolvimento e expansão das TICs, houve também uma reorientação do modelo de negócios das empresas do ramo, a partir do qual poderemos compreender como um aprofundamento ainda mais decisivo da lógica neoliberal, agora voltada ao mais "íntimo da subjetividade" (cf. DARDOT; LAVAL, 2016, p. 34). Após o fim da bolha da internet, as provedoras de serviços online sofreram com baixa lucratividade e, por isso, dificuldade de obtenção de financiamento. Na análise de Shosana Zuboff, a saída encontrada pelas empresas foi o chamado "capitalismo da vigilância", implementado pioneiramente pela Google sob a direção de Eric Schmidt. A partir de 2002, a empresa passou a utilizar seu grande aparato de armazenamento de dados provenientes de buscas – posto que já era predominante no mundo como ferramenta de buscas na internet – para identificar, no conjunto das

5 O Acordo TRIPs (sigla para Agreement on Trade-Related Aspects of Intellectual Property Rights, que em português significa Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio), de 1994, conferiu estatuto internacional à propriedade intelectual de softwares.

6 Legislações semelhantes foram promulgadas em outros países, como no Reino Unido, que permitiu o órgão de segurança Government Communications Headquarters (GCHQ) realizar a vigilância em massa, muitas vezes em trabalho conjunto com a NSA. Contudo, concentrare-mo-nos no exemplo norte-americano, visto termos, com a publicação dos arquivos vazados por Snowden em 2013 informações mais abrangentes sobre seu modo de funcionamento. As informações publicadas pelo denunciante continham arquivos sobre o GCHQ, mas se estabeleceu, naquele país, uma ordem de censura desse material.

7 Convém notarmos que a Emenda de Reautorização à FISA, de 2017, prevê a extensão da vigência da Seção 702 para mais 6 anos, até o final de 2023.

buscas de um determinado indivíduo, padrões comportamentais por meio dos quais era possível prever comportamentos futuros. O que a empresa passou a comercializar, no entanto, não foram os dados comportamentais em si mesmos, ou a previsão comportamental que sua análise oferece, mas sim a certeza de uma campanha publicitária eficiente para os anunciantes, garantida pela análise dos padrões comportamentais (ZUBOFF, 2018, pp. 92-97). Esse mecanismo, embora criado pelas empresas, serviu ao interesse das agências de segurança norte-americanas, que relacionaram a falha na prevenção contra os ataques de 11 de setembro de 2001 à falta de dispositivos fortes de vigilância (ibid., p. 113).

A afinidade eletiva entre interesse empresarial e interesse estatal que se verifica no fenômeno da vigilância em massa implicou, dessa forma, a cooperação entre esses domínios: "A aliança estreita entre as grandes empresas da *net* e os Estados transformou o ciberespaço num espaço de vigilância, no qual potencialmente não existem mais limites à intrusão dos poderes nos dados e nos intercâmbios pessoais" (DARDOT; LAVAL, 2017, p. 183-184). Se, por um lado, para o Estado, a vigilância em massa significa o aumento de poder político sobre as liberdades civis, já que a tecnologia usada para isso requer, para a identificação de suspeitos, a coleta de dados comportamentais – e portanto a violação do direito à privacidade – de todos os indivíduos; por outro lado, ela implica em um aumento do poder político e econômico do oligopólio das TICs – conhecido, enfim, pelo acrônimo GAFAM, isto é, Google, Apple, Facebook, Amazon e Microsoft –, visto que a coleta exigida pelos órgãos de segurança depende, na sua maior parte, da coleta de dados que essas corporações já realizam.

Muito embora a repercussão das denúncias de Snowden tenham levado a Suprema Corte dos Estados Unidos a considerar ilegal a prática de vigilância em massa sem mandado judicial de cidadãos norte-americanos, a falta de transparência do governo, bem como das estruturas burocráticas, não permite os cidadãos terem certeza de que isso não aconteça, em primeiro lugar porque isso é assegurado juridicamente apenas a cidadãos estadunidenses, e, em segundo lugar, porque "a tecnologia é inerentemente tão complexa, e a sua utilização, na prática, tão secreta, que não pode haver uma supervisão democrática expressiva" (ASSANGE et al., 2012, p. 42-43; 2013, p. 64). Quanto ao primeiro aspecto, há evidências do impacto geopolítico exercido pelo Estado norte-americano, garantido por sua lei interna nacional e possibilitado pelos serviços das empresas privadas, contra lideranças políticas estrangeiras, como mostraram os documentos do programa BLARNEY, que consistia na obtenção de "parcerias-chave exclusivas com empresas que permitam o acesso a cabos de fibra óptica, comutadores e/ou roteadores internacionais de alta capacidade localizados em diversas partes do mundo" para "melhorar a compreensão dos métodos de comunicação e seletores associados relativos à presidente brasileira Dilma Rousseff e seus principais consultores". Esse mesmo programa incluía a vigilância de outras figuras políticas, como o então candidato à presidência do México Enrique Peña Nieto (cf. GREENWALD, 2014, pp. 110, 147-148). O jornalista investigativo Glenn Greenwald, que participou da operação de publicação dos arquivos da NSA, frisa como a própria percepção de uma ameaça à segurança nacional, alegada constantemente

pelo governo estadunidense, é determinada pelo seu próprio poder político, levando a classificar como terroristas os dissidentes políticos, tais como "ativistas defensores do meio ambiente, várias facções de direita contrárias ao governo, ativistas antiguerra e associações relacionadas aos direitos palestinos", tornando-os alvos de vigilância, em flagrante violação de direitos políticos (GREENWALD, 2014, p. 198).

Já quanto ao segundo aspecto, o modo de funcionamento empresarial-estatal é ensejado pela própria infraestrutura tecnológica das TICs. Como observa Assange, houve, em um período de dez anos, um aumento exponencial da capacidade tecnológica de armazenamento de dados. Em cada vez menos espaço é possível armazenar uma quantidade cada vez maior de dados, acarretando uma coleta em massa intensa e constante. Somado a isso, é mais eficiente, técnica e economicamente, centralizar os servidores de diferentes empresas que realizam esse armazenamento com fins comerciais em um só lugar, em grandes *data centers*, já que, assim, a manutenção da refrigeração dos equipamentos é menos dispendiosa e o serviço adquire maior velocidade de transferência de arquivos. Essa concentração, orientada pela eficiência tecnológica e econômica, facilita a intercepção direta de órgãos de segurança como a NSA (cf. ASSANGE et al., 2012, p. 77; 2013, p. 92). Em uma visão mais ampla, o fato de os EUA concentrarem a maior parte dos *data centers* do mundo aponta para a força da centralização desses equipamentos, não apenas nacional, mas internacionalmente.[8]

Além disso, na esteira da lógica da produção neoliberal, o fato de a fabricação dos aparatos tecnológicos pressupor uma complexa divisão internacional do trabalho (emprego descomunal de pesquisa tecnológica, extração de minérios, mão-de-obra dentro de fábricas e máquinas, etc.) impossibilita rastrear as atividades de cada uma das empresas responsáveis por diferentes estágios da produção.[9] Isso, sob outra perspectiva, manifesta a centralização imposta pela própria estrutura de produção do objeto tecnológico, que de modo algum poderia ser realizada de outra forma. Não seria possível, por exemplo, em termos econômicos e sociais, descentralizar o processo de mineração do solo, visto que alguns dos materiais necessários para a fabricação das placas eletrônicas (semicondutores), os metais de terras-raras, somente podem ser extraídos mediante a aplicação de técnicas sofisticadas e escavadeiras de grandes proporções. Os oligopólios, com a supervisão e assentimento dos governos, podem deter o controle dessa complexa cadeia produtiva e distributiva porque detêm todos os recursos físicos e financeiros sem os quais a internet não se sustenta.

Há, ainda, entre todos os aspectos por nós mencionados, mais um que requer certa atenção: o neoliberalismo como agente da subjetivação. Trata-se de olhar para a atuação das empresas de telecomunicações entendendo que

> a lógica que consiste em dirigir indiretamente a conduta é o horizonte das estratégias neoliberais de promoção da "liberdade de escolher". Nem sempre distinguimos a dimensão normativa que ne-

8 Essa centralização pode ser verificada pelo fluxo de informações que passa obrigatoriamente pelos Estados Unidos via cabos de fibra óptica submarinos. Ver <https://www.submarinecablemap.com/>.

9 Recorrentemente há denúncias por parte de organizações não-governamentais internacionais envolvendo condições de trabalho análogas à escravidão na produção de eletrônicos. As multinacionais muitas vezes alegam que não possuem conhecimento sobre o todo de sua cadeia produtiva, o que é plausível, dada a dimensão dessa cadeia. Um dos casos mais recentes é o do relatório da China Labor Watch (CLW) acerca das condições de trabalho na Foxconn, que monta os circuitos da assistente virtual Alexa, de propriedade da Amazon. Cf.: <https://www.dw.com/en/tech-supplier-foxconn-under-fire-again-over-labor-conditions/a-44156666>.

> cessariamente lhes pertence: a "liberdade de escolher" identifica-se com a obrigação de obedecer a uma conduta maximizadora dentro de um quadro legal, institucional, regulamentar, arquitetural, relacional, que deve ser construído para que o indivíduo escolha "com toda a liberdade" o que deve obrigatoriamente escolher para seu próprio interesse. (DARDOT; LAVAL, 2016, p. 216)

A lógica responsável por essa direção da conduta pode ser facilmente encontrada nas redes sociais *online*. Os gostos, os desejos, as amizades, as localizações, os cliques, a rolagem, cada visualização de imagem e de texto, cada pausa de leitura e cada mensagem dentro do serviço são condensados, por meio de *softwares*, em um banco de dados que fornece uma base consistente não apenas para que a empresa ofereça a segurança de uma campanha publicitária eficiente aos anunciantes (como no caso supracitado do Google), mas também para que ela tenha a segurança de que os usuários permaneçam utilizando seu serviço com a maior frequência possível. Nesse campo enevoado de aplicação de uma tecnologia informacional, o estímulo constante ao ato escolher que o sujeito sofre se funde à obrigação de fazê-lo, de modo que sua atenção seja fonte de matematização e de mercantilização, recurso extraível e extraído por uma "nova fronteira de negócios composta do conhecimento sobre o comportamento em tempo real, que cria oportunidades para intervir nesse comportamento e modificá-lo objetivando o lucro" (ZUBOFF, 2018, p. 56). Quanto ao aspecto do controle comportamental produzido pela experiência personalizada – inevitável nas redes –, vale mencionarmos que a própria forma de estruturação física, jurídica, econômica, política e social das TICs é fonte de práticas desse tipo, desde aspectos mais sutis e indiretos, que estão começando a ser estudados, até casos mais notáveis, de significativo impacto político.[10]

Dessa forma, embora Dardot e Laval não teorizem especificamente sobre o tema da internet, seu cabedal teórico, de forte inspiração foucaultiana e marxista, nos proporciona a análise de um fenômeno complexo como o das TICs, na compreensão do caráter intrusivo do neoliberalismo. Essa dinâmica própria das redes possibilitou, como possibilita, mais do que publicidade personalizada ou coleta compulsória de dados: é uma ferramenta de vigilância em massa.

Tendo em vista nossa breve incursão na história da internet, pretendemos ter verificado que a vigilância em massa, longe de ser fruto de usos momentâneos, resulta de uma lógica imbricada entre estruturação tecnológica e poder político-empresarial. Todas as ocorrências históricas e políticas mencionadas evidenciam como, no desenvolvimento das TICs, a mercantilização passou dos hardwares aos softwares, e então à estrutura da rede e, ainda mais profundamente, às próprias preferências pessoais. Tratando-se de um perigo incontestável às liberdades políticas, o problema da estrutura antidemocrática inscrita na complexidade tecnológica das TICs parece incontornável: sua imagem descritiva, segundo Julian Assange, consistiria no telefone celular como "tanque de guerra dentro do quarto" (ASSANGE et. al., 2012, p. 33; 2013, p. 53). Essa impossibilidade de mudança, contudo, não implica na inexistência de estratégias políticas de resistência, como pode parecer. De acordo com Assange, há o chamado à "luta criptográfica" – a utilização de ferramentas de comunicação criptografada – que consiste na realização de uma potência também contida na

10 Um caso decerto notável é o denunciado por um ex-funcionário da empresa de consultoria Cambridge Analytica. Desde 2014 a empresa utilizava dados coletados do Facebook de mais de 80 milhões de usuários, fornecendo perfis pessoais consistentes a campanhas políticas de figuras como Ted Cruz e Donald Trump nas eleições de 2016.

estrutura da tecnologia, capaz de “criar novos espaços fechados àqueles que controlam a realidade física, porque a tarefa de nos seguir nesses lugares demandaria recursos infinitos”, em outras palavras, garantir, ao menos em alguns momentos, o direito à privacidade (id., 2012, p. 4; 2013, p. 27). Isso abriria caminhos seguros para futuras revelações públicas, por meio de denúncias, anônimas ou não, sobre o abuso de poder das corporações e dos Estados.

Bibliografia

ASSANGE, J. et al. *Cypherpunks*: freedom and the future of the internet. Londres: OR Books, 2012.

_____. et al. *Cypherpunks*: liberdade e o futuro da internet. Trad. Christina Yamagami. São Paulo: Boitempo Editorial, 2013.

_____. *Quando o Google encontrou o WikiLeaks*. Trad. Cristina Yamagami. São Paulo: Boitempo Editorial, 2015.

CHUN, W. H. *Updating to remain the same*: habitual new media. Cambridge: MIT Press, 2016.

DARDOT, P. Neoliberalismo "clássico" e novo neoliberalismo. Trad. Gisele Zanola Carvalho e Otto Sanchez-Crespo da Rosa. *Sens Public*, Montreal, 2021. Disponível em: http://sens-public.org/articles/1562/. Acesso em: 25 de janeiro de 2021.

_____; LAVAL, C. *A nova razão do mundo*: ensaios sobre a sociedade neoliberal. Trad. Mariana Eschalar. São Paulo: Boitempo Editorial, 2016.

_____; LAVAL, C. *Comum*: ensaio sobre a revolução no século XXI. Trad. Mariana Eschalar. São Paulo: Boitempo Editorial, 2017.

ELLUL, J. *A técnica ou o desafio do século*. Trad. Roland Corbisier. Rio de Janeiro: Paz e Terra, 1968.

GREENWALD, G. *Sem lugar para se esconder*: Edward Snowden, a NSA e a espionagem do governo americano. Trad. Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

HUANG, Y.; SUN, M.; SUI, Y. How digital contact tracing slowed covid-19 in East Asia. *Harvard Business Review*, 2020. Disponível em: https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia. Acesso em: 28 de dezembro de 2020.

JAEGER, P. T.; BERTOT, J. C. McCLURE, C. The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly*, n°20, 2003, pp. 295–314.

LOURENÇO, E. A vigilância massiva será o legado da pandemia? *Coalizão Direitos na Rede*, 2020. Disponível em: https://direitosnarede.org.br/2020/09/23/a-vigilancia-massiva-sera-o-legado-da-pandemia/. Acesso em: 28 de dezembro de 2020.

LE, S. Contact tracing in a global pandemic. *Data Smart City Solutions*. Harvard Ash Center for democractic governance and innovation, 2020. Disponível em: https://datasmart.ash.harvard.edu/news/article/contact-tracing-global-pandemic. Acesso em: 03 de janeiro de 2021.

REBELLO, A. Da Placa de carro ao cpf. Conheça o Córtex. *The Intercept Brasil*. Disponível em: https://theintercept.com/2020/09/21/governo-vigilancia-cortex/. Acesso em: 29 de dezembro de 2020.

RYAN, J. *A history of the Internet and the digital future*. Londres: Reaktion Books, 2010.

SCHWARTZ, M. Facebook failed to protect 30 million users from having their data harvested by Trump campaign affiliate. *The Intercept*, 2017. Disponível em: https://theintercept.com/2017/03/30/

facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/. Acesso em: 29 de dezembro de 2020.

STALLMAN, R. *Free Software, Free Society*: Selected Essays of Richard M. Stallman. Org. Lawrence Lessig e Joshua Gay. Boston: Free Software Foundation, 2002.

WINNER, L. *Autonomous technology*. Cambridge: The MIT Press, 1978.

ZASTROW, M. South Korea is reporting intimate details of COVID-19 cases: has it helped? *Nature*, 2020. Disponível em: https://www.nature.com/articles/d41586-020-00740-y. Acesso em: 30 de dezembro de 2020.

YATSKO, A; SUSŁOW, W. *Introduction to Information Technologies and Computer Science*. Varsóvia: De Gruyter Open, 2015.

ZUBOFF, S. "Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação". In: BRUNO, F. et al. (org.). *Tecnopolíticas da viligância*: perspectivas da margem. São Paulo: Boitempo, 2018.

_____. *The age of surveillance capitalism*: the fight for a human future ate the new frontier of power. Nova Iorque: Public Affairs, 2019.