Vigilância por dados, privacidade e segurança: entre a exploração pelo mercado e o uso estatal

Data surveillance, privacy and security: between market exploitation and State use

Mateus de Oliveira Fornasier*

Norberto Milton Paiva Knebel**

Fernanda Viero da Silva***

RESUMO

Este artigo estuda a vigilância digital contemporânea, e a forma pela qual os dados sensíveis dos usuários são recolhidos e analisados para diferentes propósitos. Objetivos específicos: i) descrever formas tecnológicas de vigilância a partir de dados pessoais e comportamentais gerados nas comunicações online dos indivíduos; ii) estudar as relações entre a economia política do capitalismo contemporâneo e a privacidade; iii) compreender como Estados e organizações privadas se utilizam da vigilância de dados eletrônicos. Metodologia: método de procedimento hipotético-dedutivo, com abordagem qualitativa e técnica bibliográfico-documental.

Palavras-chave: Vigilância; Tecnologia; Dados; Capitalismo de Vigilância; Privacidade.

ABSTRACT

This paper studies contemporary digital surveillance, and how users' sensitive data is collected and analyzed for different purposes. Specific objectives: i) to describe technological forms of surveillance based on personal and behavioral data generated in individuals' online communications; ii) to study the relations between the political economy of contemporary capitalism and privacy; iii) to understand how states and private organizations use electronic data surveillance. Methodology: hypothetical-deductive procedure method, with qualitative approach and bibliographic-documentary technique.

Keywords: Surveillance; Technology; Data; Surveillance Capitalism; Privacy.

* Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Professor do Programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (Unijuí). Endereço: Rua do Comércio, 3000, Universitário, Ijuí, RS, CEP 98700-000. Telefone: (55) 3332-0200. E-mail: mateus.fornasier@gmail.com

** Mestre em Direito pela Universidade La Salle. Doutorando em Direito na Universidade Regional do Noroeste do Estado do Rio Grande do Sul (Unijuí). Advogado. Endereço: Rua Sete de Setembro, 244, Ijuí, RS, CEP 98700-000. Telefone: (51) 98287-2912. E-mail: norberto.knebel@gmail.com

*** Graduanda em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUÍ). Endereço: Rua do Comércio, 2425 apto 104, Pindorama. CEP: 98700-000. Ijuí, RS. Telefone: (55) 8108-5803. E-mail: fefeviero@gmail.com

INTRODUÇÃO

Estudar as interfaces entre a tecnologia, as atividades de vigilância e direitos fundamentais (principalmente no que tange à segurança e à privacidade) é algo de grande relevância social — e para as Ciências Sociais em geral —, pois isso contribui para o desvelamento de uma transformação talvez ainda pouco explorada do capitalismo na atualidade, embasado no conhecimento do comportamento dos usuários da internet ao arrepio de sua capacidade moral de decisão e de sua privacidade (eis que não cabe ao indivíduo escolher se irá compartilhar tais dados ou não, que dizem respeito a facetas de seu modo de ser que vão para além do consciente, penetrando até mesmo na álea dos desejos e de atitudes pessoalmente despercebidas). Juridicamente, é relevante tal estudo porque é focado em formas de comunicação social e de geração de economia que desafiam normas constitucionalmente estabelecidas em toda democracia: o respeito à vida privada e à adesão contratual. Toda rede social, aplicativo e/ou sítio da internet que captura dados expõe suas intenções em contratos eletrônicos de adesão tão longos e complexos que se torna impossível, em um cotidiano normal, ter tempo e conhecimento suficientes para compreender tais obrigações. Agrava-se essa ameaça a direitos o fato de que as ferramentas tecnológicas são cada vez menos prescindíveis para a realização da vida em sociedade, de atividades econômicas/laborais, entretenimento, etc.

A hipótese principal desta pesquisa é que nossa sociedade é mediada por (e, por que não afirmar, em grande medida, dependente de) tecnologias de informação e comunicação (TICs) em rede: atividades econômicas em geral (fornecimento de produtos, de serviços, relações de trabalho e emprego, etc.), educação (e obtenção de conhecimento em geral), relacionamentos interpessoais, procedimentos democráticos, resolução de conflitos... Enfim, praticamente tudo que diga respeito à vida em sociedade encontra seu correlato virtual/digital. Entretanto, a partir dessa vida digital — que, muito significativamente, reflete o comportamento pessoal e dados sensíveis dos usuários — são coletados dados acerca dos usuários, que podem servir a diversos propósitos: ora benéficos aos interesses dos usuários; ora prejudiciais aos seus direitos fundamentais, principalmente no que tange à sua vida privada. Configura-se, assim, um cenário onde uma nova forma de vigilância ganha espaço na sociedade: a vigilância a partir de dados. A forma de se obter dados é complexa, e tem como base o uso crescente e cada vez mais elaborado de algoritmos capazes de realizar seu recolhimento e organização, que não apenas alimentam uma nova forma de capitalismo caracterizado por tal sistemática, como também abastecem grandes bancos de dados de instituições públicas e organizações privadas. Os riscos nem sempre são conhecidos pelos usuários ao concederem permissões online quando utilizam aplicativos ou dispositivos eletrônicos.

Nesse sentido, o objetivo geral do presente artigo é estudar a vigilância digital contemporânea, e de qual forma os dados sensíveis dos usuários são recolhidos e analisados para diferentes propósitos. Sua hipótese principal é a de que, com o advento das tecnologias digitais e o desenvolvimento de um ciberespaço, foram possibilitadas novas modalidades de vigilância que, em que pese sejam benéficas aos interesses dos usuários em diversas circunstâncias, também acarretam diversos riscos a seus direitos fundamentais, com especial destaque àqueles relacionados à vida privada.

Para a consecução do seu objetivo geral, o artigo foi dividido em três seções. A primeira delas se ocupa da descrição das formas tecnológicas de vigilância a partir de dados pessoais e comportamentais gerados nas comunicações online dos indivíduos.

Já a segunda estuda as relações entre a economia política do capitalismo contemporâneo e a privacidade. Por fim, a terceira parte busca compreender como Estados e organizações privadas se utilizam da vigilância de dados eletrônicos.

Metodologicamente, a presente tem natureza exploratória, sendo seu método de procedimento hipotético-dedutivo, sua abordagem qualitativa, e sua técnica de pesquisa bibliográfica-documental.

TECNOLOGIAS DIGITAIS COMO NOVAS FORMAS DE VIGILÂNCIA EM MEIO A OBTENÇÃO E ANÁLISE DE DADOS

Não seria exagero ou equívoco gritante afirmar que a atual sociedade é qualificada, cada vez mais, pelo adjetivo *digital*, onde novas tecnologias de informação e comunicação (TICs) têm constante influência cotidiana, se configurando como mediadoras das relações sociais, da economia e até a mesmo a forma de se produzir/disseminar o conhecimento; pairam formas de absorção de conhecimento acerca dos usuários de modo ubíquo, de modo que as TICs podem ser tidas como novas formas de vigilância (LUPTON, 2015, p. 02; p. 189). As TICs digitais desempenham um papel crucial no processo de globalização como fenômeno caracterizado pela ampla circulação de pessoas, ideias e hábitos, que embora não tenha se iniciado historicamente com as tecnologias, se desenvolve em uma alta velocidade através destas (DE MUL, 2015, p. 106).

No inglês, o termo *surveillance*, que designa a vigilância, é derivado do verbo francês *surveillir*, que, por sua vez, é relacionado ao termo *vigilare*, do latim. E, de acordo com Gary T. Marx (2015, p. 735), essa terminologia se encontra atrelada a verbos como "olhar", "observar", "supervisionar", "controlar", "inspecionar", "monitorar", "guardar" ou até mesmo "seguir". Muitos dos exemplos para entender as formas contemporâneas de se obter informações se pautam em habilidades cognitivas através de artefatos tecnológicos tais como softwares e processos automatizados. Entretanto, tais meios técnicos também podem envolver formas sofisticadas de manipulação com a sedução, coerção, engano, informações inequívocas e demais formas especiais de observação (MARX, 2015, p. 735-737). A vigilância se tornou mais enganosa com o passar dos tempos, e pode ser vista como algo mais difícil de derrotar do que anteriormente, afinal muitas formas são tão onipresentes que geralmente presumem-se onipotentes (MARX, 2015, p. 736).

A vigilância pode, de forma sucinta, se dar sobre a rotina humana, o "piloto automático" semiconsciente e muitas vezes até mesmo o instinto biológico de nossos receptores sensoriais que estão prontos para receber constantemente informações de quem quer que esteja territorialmente próximo (MARX, 2016, p. 16). Essas noções permitem distinguir duas formas de vigilância, pelo menos: uma tradicional e uma nova. A vigilância tradicional confia nos sentidos desassistidos, e é característica das sociedades pré-industriais. Com o desenvolvimento da linguagem, numérica e escrita, e de formas distintas de organização social envolvendo entidades políticas maiores, surgiram formas mais complexas e sistemáticas de vigilância, baseadas em contagem, registro, interrogatório, informação, infiltração, confissões. e o uso expandido de testes (MARX, 2016, p. 17). Com o surgimento da sociedade industrial surgiram novas ferramentas de vigilância e comunicação, que aprimoraram os sentidos e a cognição

O visual é geralmente um elemento de vigilância, mesmo quando não é o meio inicial de coleta de dados, e a nova vigilância pode ser definida como escrutínio de

indivíduos, grupos e contextos através do uso de meios tecnológicos para extrair, inferir ou criar informações (MARX, 2016, p. 19-20). Exemplos de tal fenômeno podem ser encontrados em perfis de computadores, que possuem grandes conjuntos de dados, câmeras de vídeo, dados acerca da análise de DNA, GPS, monitoramento eletrônico, testes de drogas e o monitoramento possibilitado pelas mídias sociais e telefones celulares. A nova vigilância se apresenta de forma mais intensiva e extensiva, ampliando os sentidos, diminuindo assim custos e chegando a locais mais remotos; se baseia preponderantemente em agregar dados e no *big data*; sendo assim, tem uma menor visibilidade e envolve diretamente a conformidade involuntária do indivíduo (MARX, 2015, p. 735-736).

A nova vigilância instaurada na contemporaneidade é o exame minucioso de indivíduos e grupos, através do uso de meios tecnológicos altamente sofisticados, capazes de extrair informação. Nesse sentido o uso de meios técnicos para extrair e criar as informações implica na capacidade de ir além do que é naturalmente oferecido aos sentidos e mentes ou o que é relatado voluntariamente (MARX, 2015, p. 736). A indústria da *big data* instaura um sistema na sociedade contemporânea, onde o mundo e a vida são transformados ou mediados por dados, e tal feito constitui uma mudança de paradigma fundamental para a sociedade contemporânea (BERALDO; MILAN, 2019, p. 01). A natureza dos bancos de dados é inerente a qualquer *software*, que basicamente realiza programação de dados que podem ser divididas em quatro operações (DE MUL, 2015, p. 106): a) adicionar; b) pesquisar; c) mudar; e d) destruir (comando esse que pode ser classificado pelas opções de inserir, selecionar, atualizar e deletar). Juntos, esses comandos constituem a dinâmica da ontologia dos bancos de dados.

A dinâmica dos bancos de dados não é necessariamente digital, uma vez que listas telefônicas e índices são formas de agrupar dados também, entretanto, bancos de dados digitais se apresentam na contemporaneidade de forma mais flexível, pela facilidade de adicionar ou excluir informações (DE MUL, 2015, p. 106). Os dados estão sendo transformados cada vez mais em um elemento imprescindível no que tange o repertório de ação, onde hoje existem diversas disputas políticas. Transformar dados em ativismo de dados é de fato um tópico complexo, onde os dados são definidos a partir de sua função ou utilidade na vida das pessoas; e a ênfase fica a cargo da destinação humana/política, e não necessariamente em seu tamanho (BERALDO; MILAN, 2019, p. 04). Atualmente o que se percebe é uma sofisticação nas formas de se analisar dados e os operacionalizar de forma com que sejam utilizados para propósitos específicos; neste mesmo âmbito, as próprias tecnologias que coletam dados são capazes de oferecer serviços para proteger os dados e os usuários (COWLS, 2018, p. 145).

Petzold (2015, p. 158) estabelece noções acerca dos algoritmos humanos, e de que forma eles estão estruturados em "andaimes". Tal metáfora se atribuí ao fato de que andaimes sugerem algo que está constantemente atrelado a conceitos como combinação, adaptação e substituição. Assim, as ferramentas fundamentais para o andamento destas estruturas sociais são as mudanças provocadas pela evolução tecnológica. Com a automatização de dados através da dependência de algoritmos é possível entender que há uma combinação de elementos que podem servir para diversos sistemas e aplicações, e posteriormente podem vir a ser recombinados de diversas formas possíveis no âmbito virtual.

Para De Mul (2015, p. 107) o que diferencia preponderantemente a Web 1.0 da 2.0 não é sua característica social — afinal, as primeiras aplicações virtuais já contavam com possibilidades de conversação interpessoal online e análogos —, mas sim, a presença

de softwares capazes de gerar páginas através de entradas do banco de dados onde cada fragmento está pronto para ser remontado novamente, permitindo inúmeras recombinações e correções aninhadas; ou seja, a Web 2.0 é baseada em dados, não em páginas. A partir dessas constatações é possível entender que a Web 2.0 opera através de um processamento de software em vez de renderizar um arquivo. Além disso, na era da big data, esses bancos de dados estão cada vez mais conectados entre si e com fluxos de dados conectados, como pesquisas no Google, interações em mídias sociais (Twitter, Facebook, Instagram, LinkedIn, Reddit, etc.) e comércio online. Essas conexões derivadas da big data são rastreadas e usados para fins de configuração de perfil de usuário e mineração de dados em tempo real por organizações privadas e públicas (DE MUL, 2015, p. 107-108). Dessa mesma lógica pode-se inferir que, em razão de dados provenientes de processos de produção, transferências de dinheiro, dispositivos de GPS, câmeras de vigilância, medições biométricas e uso de smartphones e outros dispositivos localizáveis, um imenso banco de dados global está sendo formado e transformará os modos de vida, de trabalho e de pensar (DE MUL, 2015, p. 107).

Tal cenário narrado inclui de certa forma inúmeros fatores de risco da infraestrutura assimétrica para a coleta de dados, uma distorção sistemática na análise dos dados e de suas formas discriminatórias pelas quais os insights dos sistemas algorítmicos são implantados (COWLS, 2018, p. 145). A própria linguagem humana pode ser observada com um sistema de códigos complexos, afinal permite a continuidade da produtividade, que por sua vez é equipada com as tecnologias. Algoritmos humanos, por sua vez, se referem também a impulsos provocados pela diversidade linguística atual, cuja a relação desta com linguagens artificiais é altamente complexa (PETZOLD, 2015, p. 160-162).

A linguagem no contexto digital e tecnológico, bem com suas traduções, são capazes de multiplicarem sentidos, e desempenham papéis significativos no que tange ao aumento das redes sociais. Entretanto existem diversos riscos neste âmbito, como por exemplo, a entrega de resultados inesperados ou incertezas econômicas (PETZOLD, 2015, p. 166). Pode-se entender que o impacto dos bancos de dados é vasto, uma vez que não se limita somente ao universo da computação, já que evocam atos no mundo material. Exemplos disso são os bancos de dados biotecnológicos utilizados para fins da engenharia genética, implementações em robôs industriais e o sistema de detecção de perfis em aeroportos, com o objetivo de identificar eventuais terroristas (DE MUL, 2015, p. 107). Em tese tudo o que pode ser identificado através de dados se torna um objeto de controle de tais bancos de dados.

Entre o poder humano e o computacional, tais processos às vezes permitem uma ampliação acerca dos fundamentos da diversidade, literalmente a novas alturas; mas às vezes desencadeia o efeito inverso (PETZOLD, 2015, p. 168). As mídias digitais resultaram em novas formas de vigilância participativa, uma vez que diversos sites e as próprias redes sociais oferecem aos usuários a oportunidade de fazer upload de imagens, arquivos e informações textuais sobre si e os demais ao redor, para que outras pessoas possam ter acesso. O objetivo de tais plataformas é de fato manter esse conteúdo sob o escrutínio de outras pessoas, atendendo-se assim, ao desejo em ser visto, à autopromoção e ao compartilhamento de informações e observações sobre o outro (LUPTON, 2015, p. 177).

Celebridades, políticos e outras personalidades públicas estão submetidas ao monitoramento constante (seja em ambiente público, seja no privado) e os grandes facilitadores dessa exposição não são somente os *paparazzi* — afinal de contas, qualquer pessoa com algum dispositivo móvel pode fazer uma transmissão ao vivo

instantânea. Nesses casos, resta claro que há a incidência do sinóptico participativo atrelado a vigilância e suas formas de operar (LUPTON, 2015, p. 177). A identidade humana consiste de vários elementos heterogêneos que conflitam entre si muitas vezes, e nos expressamos em interações cotidianas, através de nosso vestuário, de nossas rotinas mais variadas, e isso nos denota a construção da "autoimagem" do indivíduo (DE MUL, 2015, p. 99-100).

Todos aqueles que atualmente são usuários das mídias sociais podem se envolver em práticas de autovigilância para Lupton (2015, p. 179) afinal são capazes de gerenciar o conteúdo que vão publicar e assim por consequência apresentar um certo tipo de identidade desejada. Os indivíduos no geral podem exercer um elevado grau de relevância em meio as mídias sociais no que tange o olhar do telespectador; grandes perfis com muitos seguidores e até mesmo celebridades e líderes mundiais possuem controle sobre o conteúdo que geram e disseminam nas redes sociais, entretanto, em contrapartida se colocam como objetos do olhar de outras pessoas, sendo alvos de um intenso escrutínio derivado das noções de vigilância e observação sinóptica (LUPTON, 2015, p. 178).

Trabalhando com a temática da tecnologia e o que surgiu a partir desta, dada sua ampla possibilidade de destinações, esta primariamente não se parece compatível à empatia humana. A empatia, de acordo com Craig e Seïler (2016, p. 57) é considerada uma habilidade muito humana, e de fato não há como se negar que os computadores são considerados uma verdadeira antítese do pensamento empático, e isso é capaz de se refletir em nossa linguagem.

Quando uma pessoa não possui empatia costumamos a descrevê-la como um robô ou máquina, afinal tal característica é parte do que parece ser o conceito de ser humano; em outro ângulo, o se um computador emocional, isso também é visto como algo ruim, também sabemos que os computadores são capazes de processar dados com mais rapidez e podem executar cálculos com base em informações para humanos, assim, é natural que devamos estar um pouco apreensivos com os computadores que desenvolvem nossas maiores humanidades, para que não excedam nossa posição de autoridade (CRAIG; SEÏLER, 2016, p. 57). Atualmente culturas de auto rastreamento surgiram em um contexto sociocultural, no qual se pautam diversas razões, discursos e práticas tecnológicas que estão convergindo entre si. De certa forma, para Lupton (2016, p. 113) isso inclui conceitos complexos como o autoconhecimento, a autoconsciência e o auto empreendedorismo. Assim se instaura um ambiente social e político no qual a capacidade das tecnologias digitais em monitorar uma crescente variedade de aspectos do corpo humano, comportamentos, hábitos e ambientes se dissemina em ambientes virtuais através de novas tecnologias de vigilância, que por sua vez se diversificam.

Os aplicativos de aparelhos móveis estão disponíveis no mercado há mais de uma década, e classicamente foram apresentados pela Apple em 2008 através de sua loja online (*App Store*) e logo tal feito foi seguido pela loja de aplicativos do Google (a *Google Play*). Hoje, cada uma dessas lojas online oferece milhões de aplicativos dos mais diversos gêneros, com uma ampla variedade de propósitos e funções, e entre eles os aplicativos relacionados à saúde compreendem uma categoria-chave amplamente buscada (LUPTON, 2019, p.02).

De acordo com Lupton e Williamson (2017, p. 781), as crianças se tornam cada vez mais alimentadas por dados através das tecnologias, como mídia móvel, plataformas de mídia social e softwares educacionais, e os dados gerados por essas tecnologias são frequentemente usados para vigilância ou para o monitoramento e avaliação de

tais jovens, por si próprios ou por outros que podem incluir o registro e avaliação de detalhes de aparência, crescimento, desenvolvimento, saúde, relações sociais, humor, comportamento, padrões e avaliações educacionais, entre outros.

Para muitos usuários de tais tecnologias fica evidente que elementos biográficos, corporificados, interpessoais e situacionais de suas vidas fornecem uma base para o desejo de monitorar de perto seus aspectos comportamentais e a motivação para continuar; ficou evidente, para Lupton (2019, p. 7) em sua pesquisa de campo, que pessoas que utilizam práticas de rastreamento automático são imbuídas de emoção, afinal o prazer e a satisfação decorrentes dessas práticas são essenciais para continuar com elas como parte de suas rotinas diárias. Nessa mesma pesquisa restou claro que tais aplicações operam como formas do agente "sentir-se mais no controle" e de lidar melhor com riscos, ansiedades e seus medos e incertezas sobre seu futuro.

São inúmeros os dispositivos "inteligentes" que possuem a capacidade de auto monitoramento do indivíduo no seu cotidiano; carros atualmente são capazes de monitorar os hábitos de dirigir e sonolência, alertando os motoristas, por exemplo, se correm o risco de adormecer ao volante. Colchões específicos já monitoram os padrões de sono e temperatura corporal; as cadeiras podem detectar movimentos físicos e sapatos e roupas "inteligentes" podem registrar atividades e outros dados físicos (LUPTON, 2016, p. 105).

Residências "inteligentes" já usam sensores para monitorar os movimentos de seus usuários e os "medidores inteligentes" para rastrear o uso energético doméstico. Inclusive, o termo "cidades inteligentes" é frequentemente usado para definir dados captados por objetos inteligentes localizados em espaços públicos e usados para razões pessoais em áreas privadas; enquanto as "escolas inteligentes" se utilizam de análises preditivas de aprendizado para criar perfis de dados em alunos individuais em muitos países europeus, para atingir determinados fins educacionais. Destacados esses pontos, fica evidente que as tecnologias digitais como um todo estão em crescente expansão e fazem parte da rotina de milhões de pessoas diariamente, mesmo que estas não tenham consciência disso (LUPTON, 2015, p. 188). Tais tecnologias estão atreladas intimamente a construção social do indivíduo e de suas demais relações, sejam elas amorosas, profissionais, familiares, com o espaço e até mesmo com o ambiente.

CAPITALISMO DE DADOS E PRIVACIDADE

Atualmente podemos perceber que com o desenvolvimento das tecnologias que concedem novos rumos a vigilância, se instaurou a presença continua do que podemos chamar de capitalismo de vigilância, que na contemporaneidade traz consigo o "pecado original" de acumulação primitiva do capitalismo (ZUBOFF, 2019, p. 01). Tecnologias digitais integram sistemas de educação, de saúde e da mídia de massa, dentre outros. Nesse sentido, novas formas de investigação e armazenamento de dados são possíveis em razão dessa dinâmica integrada, cuja evolução fez surgir um novo entendimento acerca da economia (LUPTON, 2015, p. 188-189).

O capitalismo do século XXI encontrou uma nova matéria-prima massiva para se apropriar: dados (SRNICEK; DE SUTTER, 2016, p. 106).. Por meio de uma série de desenvolvimentos, a plataforma eletrônica tornou-se uma maneira cada vez mais dominante de organizar os negócios, monopolizando, extraindo, analisando, usando

e vendendo dados. Os modelos de negócios da era fordista eram capazes apenas rudimentarmente de extrair dados do processo de produção ou do uso do cliente. A era da produção enxuta modificou isso levemente, pois as cadeias de suprimentos globais 'just in time' exigiam dados sobre o status dos estoques e a localização dos suprimentos. No entanto, dados fora da empresa permaneciam quase impossíveis de obter; e, mesmo dentro da empresa, a maioria das atividades não foi registrada. A plataforma eletrônica, por outro lado, possui extração de dados incorporada ao seu DNA, como um modelo que permite que outros serviços, bens e tecnologias sejam construídos sobre ela, como um modelo que exige mais usuários para obter efeitos de rede, e como um meio digital que simplifica o registro e o armazenamento. Todas essas características tornam as plataformas um modelo central para extrair dados como matéria-prima a ser usada de várias maneiras. Os dados podem ser usados de várias maneiras para gerar receita. Para empresas como Google e Facebook, os dados são, principalmente, um recurso que pode ser usado para atrair anunciantes e outras partes interessadas. Para empresas como Rolls Royce e Uber, os dados estão no coração de vencer a concorrência: eles permitem que essas empresas ofereçam melhores produtos e serviços, controlem trabalhadores e otimizem seus algoritmos para um negócio mais competitivo.

Hoje, os dados moldam um cenário onde interessam a produção em massa ou aqueles com domínio econômico; geram alternativas, mas cada vez mais controversas, afinal é mobilizado estrategicamente dentro de parâmetros genéricos de política (por exemplo, contra mapeamento e cartografia crítica), ou estão sob a influência de fatores que fomentam lutas contemporâneas cruciais (por exemplo, contra discriminação por algoritmos) (BERALDO; MILAN, 2019, p. 03).

O ativismo de dados, em suas mais variadas manifestações, recentemente tem se tornado foco de estudos em ciências sociais críticas, que reconhecem a originalidade e a relevância das práticas de engajamento com a exportação de dados emergindo entre os cidadãos em geral (BERALDO; MILAN, 2019, p. 04). Vivendo em um contexto cuja as plataformas de mídia social se demonstram alternativas muito buscadas pelos usuários, como o Facebook e o Twitter, que enfatizam prerrogativas como o compartilhamento e a conexão, esses aplicativos se tornaram importantes recursos para usuários e empresas, a ponto de a não participação destas nesses meios não ser mais uma opção (KRAUSS; KROEZE; SCHYFF. 2018, p. 02).

Com o sistema do Google em atividade e a elaboração do Facebook no cenário online — da publicidade direcionada, o capitalismo de vigilância agrega uma nova lógica de acumulação onde suas diretrizes e suas proezas financeiras dominam a esfera virtual, de redes conectadas e isso desfigura grosseiramente o sonho anterior da tecnologia digital como uma força capacitante e emancipatória (ZUBOFF, 2019, p. 01). Hoje, esse capitalismo de vigilância não pode mais ser identificado pontualmente como uma empresa específica (como o era, até há algum tempo atrás, exclusividade Google, pioneira nessa forma de capitalização de dados), visto que tal lógica se ampliou, de forma com a qual o Vale do Silício se expandiu para diversos setores da economia e suas vastas opções de produtos e serviços (ZUBOFF, 2019, p. 01). Tanto o capitalismo como a vigilância não podem mais ser confundidos como pertencentes a uma corporação individual, afinal as tecnologias digitais atualmente podem assumir muitas formas e reproduzirem diversos reflexos, dependendo do seu norte social e econômico. Para Zuboff (2019, p. 01) a orientação econômica é a mestra, enquanto a tecnologia é a marionete.

A partir de uma mudança na lógica da economia global e no mercado global tecnológico, temos atualmente um ambiente de trabalho caracterizado por menos

segurança no emprego, salários estagnados e onde a natureza do trabalho se tornou mais intensa e idiossincrática; diversos empregadores acreditam que devem satisfazer a um imperativo do mercado que constantemente pressiona por maior produtividade, para que suas organizações continuem competitivas (CONNOLLY, 2017, p. 69). Logo, as tentativas de satisfazer tais demandas fomentam uma busca incessante por eficiência, e o surgimento de cotas de desempenho rigorosas. O capitalismo de vigilância não é o mesmo que algoritmos, sensores, inteligência de máquina ou plataformas, embora dependa de tudo isso para expressar sua vontade; logo o capitalismo de vigilância é de fato uma criação econômica e, portanto, está sujeito a contestação democrática, debate, revisão, restrição, supervisão e pode até ser ilegal em muitos casos (ZUBOFF, 2019).

De acordo com Lupton e Michael (2017, p. 254) os dados digitais estão começando a influenciar os conceitos das pessoas sobre si mesmas, seus corpos e até mesmo suas relações sociais; o uso de dados digitais pessoais em atividades de vigilância é um um tópico controverso, afinal a vigilância de dados é realizada tanto no nível pessoal quanto no interpessoal, envolvendo a autovigilância ou a heterovigilância, e esse fenômeno é conduzido, fomentado e co-optado por empresas, por instituições e agências de segurança e policiamento, por organizações de transporte, empregadores, instituições de ensino, etc. (LUPTON; MICHAEL, 2017, p. 255).

O Google se capitalizou, e Zuboff (2019, p. 02) enuncia que o seu sucesso se deriva da habilidade de prever o futuro, especificamente o futuro do comportamento humano; e, ainda, descobriu uma maneira de traduzir suas interações fora do mercado com os usuários em matéria-prima destinadas aos seus clientes reais: anunciantes (ZUBOFF, 2019, p. 03). Em outras palavras, metadados que eram gerados pelos usuários do motor de busca (tais como a quantidade de pessoas que realiza determinada pergunta na plataforma, horários de pico pelo uso, sexo, gênero, idade, raça dos usuários da plataforma, geoposicionamento, etc.), que até há pouco tempo eram tidas como resíduo das operações ou, no máximo, informações úteis para a própria Google aprimorar seu produto, passaram a ser uma verdadeira "mais-valia comportamental" (*behavioral surplus*), altamente valorizada pela Google para formar perfis de usuários e direcionar, de modo cada vez mais preciso, anúncios para potenciais consumidores.

A internet das coisas (IoT) tem ganhado um grande potencial de concretização (e, também, de coleta de dados onipresente e em tempo real): dispositivos vestíveis (*wearables*), tais como *smart watches*, *smart glasses*, etc. As empresas que têm feito sucesso com a fabricação e venda de *wearables* acreditam que o rastreamento por meio desses produtos sempre ativados será muito mais avançado em comparação com os smartphones atuais (TUROW, 2017, p. 320). Eles inevitavelmente farão parte da IoT, ambiente em que dispositivos como smartphones, sensores de roupas e relógios inteligentes se conectam para executar serviços para seus proprietários conforme estabelecido pelo varejista ou comerciante que criou o software de serviço. As informações geradas viajam instantaneamente para uma nuvem de dados para serem executadas em tempo real através de análises preditivas complexas, incorporando outras informações já armazenadas pertencentes ao indivíduo. O varejista ou comerciante pode então detectar mudanças nos hábitos e comportamentos do indivíduo, bem como nos arredores do indivíduo, e direcioná-los de acordo com os dados coletados. Esse processo será possível por meio de elementos de escuta passiva no vestível, além de dicas ativas. Os dispositivos vestíveis permitem que os varejistas reconheçam compradores individuais

imediatamente, para que anúncios, ofertas e programas de fidelidade sejam personalizados individualmente com mais precisão do que nunca.

As tecnologias estão se expandido de acordo com a procura dos consumidores, e diversos aparelhos atraem o olhar dos usuários pela experiência personalizada que oferecem, como é o caso da assistente virtual do Google, ou até mesmo a Alexa da Amazon. Esses assistentes pessoais virtuais, de acordo com Zuboff (2019, p. 06), estão disfarçados de mecanismos de "personalização", e funcionam como cadeias de suprimentos complexas para a extração automática contínua da mais-valia comportamental da experiência humana. A possibilidades de atuação e a onipresença da Alexa que opera pelo comando de voz, produzem interfaces cada vez mais variadas com a experiência humana, que depois é alienada de sua fonte, traduzida em dados comportamentais e aplica-os em funcionalidades, que em tese, estão apenas sob o comando do usuário e só operam a partir de tal anuência. É de se imaginar que tais dispositivos, que hoje interligam diversos aparatos tecnológicos de uma residência e têm acesso a todos os dados do usuário – desde a lista telefônica e de e-mails, passando pelas suas preferências de filmes e séries na Netflix, até as músicas que integram sua playlist do Spotify —, causem interdependência entre este e suas funcionalidades, que parecem coletar dados até mesmo do ambiente, afinal tratamos de aparelhos que ficam conectados à energia e à internet ao 24 horas por dia (para operarem adequadamente) e com isso são capazes de captar até mesmo conversas entre os presentes no recinto.[1]

A onipresença de tais aparelhos também inaugurou casos exemplares. Tais assistentes virtuais estão sempre a captar o áudio ambiente para receber comandos e ajudar o usuário. E essa característica tornou tais aparatos muito úteis durante uma investigação acerca de um assassinato nos Estados Unidos, em que foi realizada a análise de áudios captados pelo Echo Dot Alexa na noite do crime em 2015.[2] Em contrapartida, tem-se que a controvérsia privacidade versus ubiquidade dos assistentes virtuais tem sido uma questão crítica da última décadas que, especialmente, se tornou muito proeminente para a tecnologia e a indústria modernas. A privacidade, reconhecida internacionalmente como direito humano, e constitucionalmente, por várias democracias, como direito fundamental, é desvalorizada em razão de questões como segurança nacional e administração eficaz das empresas (RAHMAN et al., 2019, p. 965).

Outro caso paradigmático de empresa que se vale primordialmente da vigilância de dados para seu funcionamento e lucratividade é a Uber (ROSENBLAT, 2018, p. 367-368). Intermediário entre passageiros e motoristas, seu sistema controla não apenas preços, salários e padrões de trabalho, mas também uma série de dados confidenciais no processo. As práticas de coleta de dados da Uber são aproveitadas de maneiras que podem atrair os consumidores, como cobrar a certos grupos de passageiros o que eles estão dispostos a pagar, em vez de um preço definido. Simultaneamente, o Uber é altamente visível entre os consumidores por causa de sua vasta popularidade. Às vezes, a maneira como a Uber usa seus dados é um sinal de que o papel da Uber como corretora pode ser abusivo, e não apenas lucrativo. Os preços iniciais pairam sobre essa linha fina, não porque é especificamente ruim cobrar aos passageiros mais do que o motorista é pago, mas porque viola como os motoristas entendem sua parceria e contrato legal com a empresa.

Para Cowls (2018, p. 145) o Direito à privacidade sempre esteve atrelado às tecnologias e suas habilidades em captar dados ou até mesmo informações de grande valia. Formas mais simples de tecnologia, como a datilografia, estão de fato longe de formas contemporâneas que são capazes de coletar e armazenar dados,

como as câmeras de segurança. Nesse sentido é muito pertinente nos questionarmos como a vigilância e a privacidade se relacionam. No senso comum, a vigilância é muitas vezes erroneamente vista como apenas o oposto da privacidade (MARX, 2016, p. 23); entretanto, ela implica na existência de algo que acessa dados pessoais (por meio de ferramentas de descoberta, regras ou configurações logísticas); enquanto que a privacidade, ao contrário, envolve um agente capaz de restringir o acesso a dados pessoais através dos mais variados aparatos complexos.

Mas é possível destacar que tanto a vigilância quanto a privacidade são fatores que envolvem esforços para controlar as informações (como descoberta ou proteção), e podem ser conectados de várias maneiras. A vigilância é capaz de invadir abusivamente a privacidade, mas também, pode ser um meio útil para proteger a privacidade (por exemplo, a identificação biométrica e trilhas de auditoria, câmeras de vídeo que filmam aqueles com acesso a dados sensíveis); e a privacidade por sua vez, também pode proteger a vigilância (por exemplo policiais disfarçados que usam identificações falsas, e encaminhamento de chamadas anônimas para proteger a identidade de testemunhas), assim como pode anular a mesma (por exemplo, criptografia, sussurros e disfarces). Assim, dependendo da maneira pela qual é usada, a vigilância pode afetar a presença de privacidade e/ou publicidade, dependendo do contexto e do papel desempenhado.

A conceituação de rastreamento automático emergiu recentemente nas discussões a partir da investigação de agentes de maneiras pelas quais as demais pessoas podem monitorar e registrar recursos específicos de suas vidas. O rastreamento automático também é conhecido como registro de vida, análises pessoais e informações pessoais (LUPTON, 2016, p. 102). Após a coleta de dados, as práticas de rastreamento automático normalmente incorporam tais informações primeiramente a organização interna, após a análise, e por fim a interpretação e utilização dos dados (através da produção de estatísticas ou gráficos e outras formas de visualização destes) para determinar como esses dados podem oferecer perspectivas para a vida do usuário. Nesta mesma lógica, com o advento de dispositivos móveis e portáteis, bem como softwares criados para destinações específicas tais detalhes mencionados podem ser mais facilmente coletados, analisados, pesquisados, agregados, visualizados e comparados com os dados de outras pessoas em uma velocidade expressiva (LUPTON, 2016, p. 102).

Os mais recentes avanços da tecnologia no ambiente de trabalho facilitaram a obtenção dessas eficiências buscadas e cada vez mais permitem aos empregadores obter informações mais detalhadas sobre o desempenho dos funcionários, incluindo seu próprio uso da tecnologia durante e após o horário de trabalho; entretanto tal proeza gera preocupações no que tange a privacidade dos funcionários. O ambiente de computação tecnologia integrada pode ser definido pela junção contínua de tecnologias na sociedade, e essa natureza transparente que alimenta cada vez mais preocupações com a privacidade, e com isso, em contrapartida, os funcionários estão cada vez mais conscientes das maneiras pelas quais o gerenciamento pode empregar essas tecnologias para monitorar suas interações de email e computador no local de trabalho (CONNOLLY, 2017, p. 70).

As crianças se tornam usuários muitas vezes instantâneos de práticas de auto rastreamento, implicando em preocupações acerca de sua privacidade por parte dos familiares. O direito à privacidade da criança é estabelecido internacionalmente, por sua vez, na Convenção das Nações Unidas sobre os Direitos da Criança, cujo art. 16 prevê a proteção do direito das crianças à privacidade, família, lar, correspondência, honra e reputação (LIEVENS; MILKAITE, 2018, p. 287).

O Comitê dos Direitos da Criança da ONU definiu ainda que esses direitos fundamentais citados são aplicáveis tanto no mundo "online" quanto no "offline" em 2014, o que inclui brinquedos digitais conectados e dispositivos de IoT (*internet of things*, "internet das coisas"). Leis nacionais podem regulamentar questões acerca de conteúdos impróprios para menores no ambiente virtual, assim com os pais podem definir permissões ou restrições para tais abordagens online; entretanto, persiste uma incerteza jurídica quanto dispositivos de IoT, que geralmente não são direcionados diretamente para crianças, mas coletam seus dados, tais como a Amazon Echo, Alexa, Siri (Apple) e demais assistentes domésticos inteligentes — que ficam no modo de espera para ajudar seus proprietários (LIEVENS; MILKAITE, 2018, p. 286-292).

Em contrapartida, o ambiente de trabalho, de acordo com Lupton também já se tornou um local importante de autorrastreamento forçado, onde incentivos servem de justificativa para tais práticas. Nesses moldes, tais tecnologias se direcionam para gratificação como um meio de motivar as pessoas a continuar em tais circunstâncias. Empreendimentos de acompanhamento de condicionamento físico e perda de peso, programas corporativos de bem-estar em que usuários recebem distintivos e outras recompensas e são incentivados a comparar seus dados com outros e a tentar um melhor desempenho são exemplos claros de tal fenômeno (LUPTON, 2016, p. 108-109).

A partir de tais exemplos é possível conceber a possibilidade de utilização indevida de tais dados legais coletados pelo próprio agente, pois cibercriminosos também já são capazes de identificar o valor comercial dessas informações, fazendo surgir, assim, ameaças à privacidade envolvidas no upload de dados pessoais de dispositivos de rastreamento automático ou mídias sociais e plataformas para a nuvem de computação (LUPTON, 2016, p. 111-112). Dessa forma, tais aparatos mencionados sugerem maneiras pelas quais informações sensíveis passam a ser redirecionadas para âmbitos relativos à economia global, o que implica obviamente em questões de privacidade e segurança de dados e também para os conceitos de identidade e cidadania. Assim, resta claro que o rastreamento automático digital é uma forma de vigilância de dados, ou uma forma de observação de pessoas que se utilizam tecnologias que por sua vez geram dados (LUPTON, 2016, p. 102).

Logo, os dados digitais produzidos pela vigilância pertencentes a indivíduos são constantemente gerados e as combinações de tais conjuntos de dados podem ser reunidos e são numerosos (LUPTON, 2016, p. 115). Esse uso de dados pessoais pode ocorrer sem que as pessoas tenham qualquer controle ou mesmo conhecimento de como tais informações são utilizadas e empregadas (LUPTON, 2016, p. 118). Por fim, as tecnologias digitais foram capazes de criar novas formas de relações políticas e uma nova forma de consumir e produzir conteúdo e resultados; por um lado contribuem para inovar as formas de se conduzir a sociologia, e sob outro viés é capaz de gerar uma forma diferente de sensibilidade sociológica (LUPTON, 2015, p. 189).

UTILIZAÇÃO DE DADOS POR PARTE DO ESTADO E EXPORTAÇÃO DE TECNOLOGIA CIBERNÉTICA

A sociedade de vigilância atual envolve não somente o setor privado como também o Estado e as relações entre os indivíduos, o que traz à tona um paradoxo: em um mundo em que a vigilância é vista concomitantemente como uma resposta a ameaças e uma ameaça por si só, a mesma é boa ou ruim, afinal (MARX, 2015, p. 733)? Em meio

a tais questionamentos, é necessário identificar quais são os reais conceitos imprescindíveis para capturar suas estruturas e processos básicos.

A utilização de dados por parte de agências governamentais, de segurança, comerciais e até mesmo criminais (para que tais informações obtidas pelo rastreamento automático possam ser mobilizados para seus próprios fins) são exemplos clássicos de monitoramento, que com o advento de novas formas de rastreio chega nas mãos da iniciativa privada ou até mesmo indivíduos ordinários, com apenas um smartphone nas mãos (LUPTON, 2016, p. 114). A vigilância como tal não é ontologicamente boa ou má, é o contexto e o comportamento que irão caracterizá-la de uma forma ou outra (MARX, 2015, p. 734) — e o mesmo pode ser dito para o conceito de privacidade. Contexto refere-se ao tipo de instituição e organização e seus objetivos, regras e expectativas; e comportamento refere-se ao tipo de comportamento esperado (seja com base na lei ou em expectativas culturais menos formais).

As diferenças nos contextos de vigilância que envolvem coerção (governo), assistência (pais e filhos), contratos (trabalho e consumo) e dados pessoais acessíveis e gratuitos (pessoais e privados em público) precisam ser consideradas — afinal, a vigilância se trata de um processo genérico característico de sistemas vivos com fronteiras de informações, e não algo restrito a governos, espionagem ou sigilo. E assim,

> A vigilância e a privacidade não estão necessariamente em oposição, e o último pode ser um meio de garantir o primeiro, assim como os controles de acesso à informação. Embora a atenção da mídia aos problemas associados à vigilância inadequada (principalmente pelo governo) esteja presente, também existem problemas associados à falha em usar a vigilância quando apropriado. O emergente campo interdisciplinar de estudos de vigilância analisa essas questões (MARX, 2015, p. 734).

Existe muito potencial para os algoritmos — ou seja, as programações utilizadas nesse amplo processo de vigilância a partir de dados — minarem os valores humanos considerados importantes, tanto para usuários finais quanto para titulares de dados (HAYES; VAN DE POEL; STEEN, 2020) — tais como a privacidade e a autonomia. Geralmente os algoritmos são construídos para aprimorar a autonomia humana com o objetivo final de promover seu florescimento; no entanto, quando há erros no processo de design, implementação e implantação, esse potencial é cada vez mais restrito. Não apenas esse potencial é limitado, mas uma falha na incorporação adequada de valores no processo de design para implantação pode ser ativamente prejudicial aos nossos valores e inibir ativamente o florescimento. Uma aceitação acrítica de algoritmos pode acabar com a autonomia, e o potencial de coleta e processamento de dados gratuitos pode prejudicar em muito a privacidade. Nesse sentido, também há de se destacar que os algoritmos são capazes de exacerbar ações discriminatórias contra minorias e outros grupos sociais (ainda que esta não seja a intenção direta do programador).

Todas essas implicações adversas representam problemas a serem abordados durante o design, implementação e implantação e não são desafios intransponíveis. Isso demonstra a importância do design sensível a valores (VSD) e a incorporação de valores no processo de design. O desafio de projetar algoritmos que maximizem sua contribuição para o florescimento humano no contexto de justiça e segurança sem causar danos não deve ser encarado de ânimo leve, mas as recompensas são potencialmente grandes. Vidas e propriedades podem ser protegidas se o design,

implementação e implantação de algoritmos puderem ser executados de maneira eficaz e ética. Esses desafios nem sempre serão possíveis de serem resolvidos com soluções matemáticas, pois alguns problemas requerem deliberação filosófica.

O ramo dos estudos acerca da vigilância foi aumentado significantemente a atenção da acadêmica após os eventos de 11/09/2001, mas tal tópico vem sendo interesse de estudiosos desde a década de 1950; e tal noção e dá em razão da maior consciência dos direitos humanos e dos abusos provocados pelo colonialismo, fascismo e comunismo bem como do comportamento antidemocrático mesmo em sociedades ditas democráticas (MARX, 2015, p. 734-735). Destaca-se que a vigilância particularmente na medida em que envolve Estados e organização, desempenha um papel significante nas relações sociais dos indivíduos em seu âmbito privado; tais aplicações se dão através de circunstâncias diferentes, e nesta sistemática é necessário entendermos que tal conceito se propaga em diferentes formas de poder.

O controle e a dominação classicamente são objetivos centrais para a vigilância humana no que tange a proteção ou entretenimento, e as autoridades derivadas de tal lógica e suas relações de poder estão relacionadas intimamente a habilidade dos agentes em coletar e usar dados, afinal as condições de acesso e de utilização de informações são elementos próprios e uma sociedade democrática (MARX, 2015, p. 735-736). De acordo com Lupton (2016, p. 102-103) as tecnologias de rastreamento automático digitalizadas promovem uma cultura de vigilância de dados; e deve-se fazer uma distinção entre o tipo de vigilância de dados do realizado para fins de auto rastreamento e outras formas usando tecnologias de monitoramento. Por exemplo, diversas atividades de vigilância de dados monitoram as pessoas de maneiras que elas desconhecem, como por exemplo câmeras de circuito interno fechado de televisão (CCTV), monitoramento através de sensor de movimentos de pessoas em espaços públicos, vigilância das agências de segurança nacional e até mesmo órgãos de policiamento que se utilizam de dados comerciais das empresas de internet.

Existem, obviamente, outras formas mais de vigilância de dados, como a triagem biométrica nos aeroportos; resta observarmos que sujeitos alvos dessa modalidade de vigilância de dados não possui acesso de fato às informações coletadas sobre si (LUPTON, 2016, p. 102). Há evidência de há um desconforto entre os membros do poder público sobre como seus dados pessoais são gerados e usados por outros agentes e agências de inteligência, afinal, os membros de instâncias públicas reconhecem por sua vez, o valor da bug data para bens públicos, como manutenção da segurança nacional, o controle do crime, promoção da saúde pública, melhoria da saúde e assim por diante. Entretanto, há a percepção também de que tais dados se tornam, comercialmente valiosos (LUPTON; MICHAEL, 2017, p. 256)

A partir de pesquisas de campo restou claro que quando muitos dos participantes tinham conhecimento das diversas maneiras pelas quais tecnologias de vigilância, dispositivos móveis, mecanismos de pesquisa e sites de mídia social coletam informações sobre as atividades das pessoas, entretanto, quando questionadas sobre qual formas tais tecnologias de vigilância operam as câmeras de filmagem de estabelecimentos públicos, instituições governamentais e até mesmo sistemas bancários foram citados. Nestes casos a vigilância até parece óbvia, entretanto muitos excluem de tal lista as atividades de empresas comerciais como Google e Facebook que realizam o rastreamento de dados pessoais dos usuários diariamente (LUPTON; MICHAEL, 2017, p. 261).

O potencial do big data cresce quase diariamente e, com isso, a tecnologia dele decorrente, de mapeamento de terroristas, agora pode ser usada para mapear

gangues, nos EUA (FERGUSON, 2017). Bancos de dados em larga escala de DNA, exames de íris, fotos e outras biometrias agora podem capturar exponencialmente mais dados pessoais. Todas essas técnicas de desenvolvimento incentivaram o interesse no policiamento de big data. Embora o objetivo subjacente de coletar, catalogar e usar dados sobre agentes criminosos seja tão antigo quanto o policiamento, as novas ferramentas tecnológicas tornam esse trabalho cada vez mais fácil e eficiente. Por sua vez, policiais e administradores estão cada vez mais interessados nas possibilidades de vigilância, e essa crença gerou entusiasmo, inovação e fé em um futuro orientado a dados.Cada um desses fatores aumenta o argumento de que o policiamento orientado por dados pode ajudar a virar a página em um momento de crise na aplicação da lei. Para os chefes de polícia, o policiamento de big data oferece uma fuga, um ponto de conversa para mudar a conversa do passado para o futuro. Para a comunidade, o big data oferece uma maneira mais objetiva de resolver o problema muito humano do policiamento tendencioso. Para a mídia, oferece inúmeras notícias dignas de zumbido sobre o policiamento futurista do *Minority Report*. E para os tecnólogos, ele oferece um novo mundo de oportunidade e inovação.

Desde os primeiros dias da guerra moderna na década de 1960, houve casos de uso doméstico de estratégias de contra-insurgência em solo americano. Mas desde o 11 de setembro a contra-insurgência atingiu um crescimento em termos de sua implantação sistemática e difundida em território nacional estadunidense. O paradigma foi refinado e sistematizado, tendo alcançado o estágio de domesticação completa e sistemática da contra-insurgência contra uma população local, onde não há insurgência real ou minoria ativa. Essa nova etapa é o que Harcourt (2018, p. 315-316) chama de "A Contra-Revolução", um paradigma de governar os próprios cidadãos em território nacional, modelado na guerra de contra-insurgência colonial, apesar da ausência de qualquer levante doméstico. Seu objetivo não é contra uma minoria rebelde — já que algo do tipo não existe real e significativamente nos EUA — , mas cria a ilusão de uma minoria ativa que pode ser implantada para atingir grupos e comunidades específicos e governar toda a população estadunidense com base em um modelo de guerra contra-insurgência.

A contra-revolução é uma nova e diferente arte de governar (HARCOURT, 2018, p. 319-320). Ele forma um todo coerente com um aparato de segurança composto por Casa Branca, Pentágono e funcionários da inteligência, membros de alto escalão do congresso, juízes, líderes de segurança e Internet, divisões de inteligência da polícia, empresas de mídia social, Vale do Silício executivos e corporações multinacionais. Essa rede, que colabora às vezes e compete com outras, exerce controle coletando e minerando nossos dados digitais. O controle de dados se tornou o principal campo de batalha e os dados, o principal recurso — talvez o recurso principal mais importante dos EUA atualmente.

Esse aparato de segurança busca aprender tudo sobre cada indivíduo, e os atrai através dos desejos, distrações e indulgências individuais. E executa um conjunto de instruções simples: vigilância total para obter conhecimento completo e perfeito, confinamento solitário, detenção juvenil, policiamento militarizado e bombas-robô para eliminar uma minoria radical — e tudo isso voltado para fazer a população americana se sentir segura e protegida para garantir que esta consuma, ao invés de simpatizar com os alvos.

A utilização da tecnologia cibernética normalmente implica em uma troca, assim como a exportação da tecnologia para países terceiros; desta forma a tecnologia de vigilância cibernética pode ser utilizada de maneira com que comprometa os direitos

humanos, especialmente o direito à privacidade e à liberdade de expressão (KANETAKE, 2019, p. 16). A exportação da tecnologia cibernética é capaz de trazer benefícios e malefícios quanto destinadas a países específicos; um exemplo é a exportação de um computador que é utilizado para interceptar comunicações online de âmbito privado. Tal artefato pode servir ao Estado, e assim agências de polícia podem detectar transações que são fraudulentas e prevenir o crime organizado; entretanto, por outro lado, este mesmo computador pode ser utilizado igualmente para suprimir a liberdade de expressão e o direito de privacidade daquele interceptado (KANETAKE, 2019, p. 02).

Já existem várias diretrizes internacionais, incluindo os Princípios Orientadores da ONU para Empresas e Direitos Humanos, que esperam que as estas levem em conta os direitos humanos e realizem a devida diligência em direitos humanos. Propostas acerca do controle de exportação de dados com base em direitos instaurou um ambiente onde diversos setores sociais e interessados podem dialogar sobre até que ponto os direitos humanos podem ser acomodados na exportação de práticas de controle (KANETAKE, 2019, p. 16).

Logo após a Primavera Árabe, o clima político na União Européia (UE) acarretou reformas legislativas no que tange uma melhor gestão de riscos de direitos humanos das exportações de TICs; em 2015 o Parlamento Europeu repetidamente denunciou a necessidade de regulamentar a exportação de tecnologia cibernética sensível aos direitos humanos, e a proposta visa regulamentar a transferência transfronteiriça de itens que atendem a "propósitos civis e militares". Com a UE, a exportação de itens de uso duplo foi regida pelo Regulamento do Conselho, 428/2009, de 5 de maio de 2009, que faz parte integrante da política comercial comum da União Europeia (KANETAKE, 2019b, p. 156).

Em resposta ao apelo do Parlamento Europeu, a Comissão Europeia apresentou, em setembro de 2016, a proposta de reformular o atual regulamento de dupla utilização da União Europeia. Em suma, a proposta da Comissão coloca os direitos humanos como um dos pilares fundamentais da dupla utilização e controle de exportação de dados. O maior empecilho, entretanto, está no fato de que o controle de exportação se desenvolveu basicamente para amortecer riscos militares, principalmente o que envolve a proliferação de armas químicas, biológicas e nucleares.

Instrumentos legais para proteção de dados e da privacidade dos usuários são pensados pelas legislações ao redor do mundo, e devem possibilitar que os indivíduos tenham uma solução legalmente amparada para cada violação do seu direito à privacidade. Entre estes ainda discute-se a seguinte problemática: incluir ou não um direito a ser esquecido em tal rol; mais especificamente a conveniência de conceder um direito ao esquecimento, independentemente de qualquer violação da identidade informacional, conferindo assim aos indivíduos um a prerrogativa de apagar os traços de seu passado, de modo a impedir que outros possam acessá-lo e conhecê-lo (DURANTE; PAGALLO. 2014, p.28).

CONCLUSÃO

A sociedade se encontra interligada em suas mais diversas esferas em razão das tecnologias digitais que lhe servem de meio para a satisfação de suas mais diversas necessidades. E embora muitas vezes os usuários sejam conscientes dos riscos atinentes ao uso de tais aparatos, não compreendem a complexidade de tais permissões online que concedem e nem a destinação de seus dados pessoais. A

vigilância se trata de uma terminologia que não emergiu com a digitalização das tecnologias, mas se equipou com tal advento, se expandido através de tais meios. Não somente câmeras de segurança e de estabelecimentos são capazes de captar imagens e sons, afinal aplicativos e aparelhos móveis são os mais comuns entre os aparatos tecnológicos atualmente.

A evolução da vigilância tecnológica se vinculado ao processo de individualização e auto-responsabilização da economia capitalista, no qual é o usuário que produz os dados se sua própria vigilância, ficando sujeito ao processo de que seus dados são necessárias para melhorias aos sistemas — produzindo valor para os algoritmos. A vigilância configura uma situação constante, que cada vez mais evolui para além do paradigma do trabalho e da segurança pública para o núcleo da vida cotidiana, analisando e condicionando comportamentos— vinculada diretamente aos aplicativos de utilidade e redes sociais.

A busca por aumento de utilidade e pela satisfação de desejos, consequentemente, impulsiona uma lógica econômica de mercado por trás de tal ramo; e assim, o empreendedorismo se volta à venda e à produção de novas tecnologias que se adaptem às necessidades dos consumidores. O capitalismo que emerge de tal lógica apresenta diversos contrastes, e entre eles, a ameaça contra a privacidade dos agentes. São exploradas, assim, informações armazenadas em bancos de dados que servirão a vários propósitos — inclusive, a várias destinações relacionadas à política estatal.

Artigo recebido em 18/01/2020 e aprovado em 27/05/2020.

REFERÊNCIAS

BERALDO, Davide; MILAN, Stefania. From data politics to the contentious politics of data. **Big Data & Society,** v. 6, n. 2, p. 1-11, 2019. DOI: 10.1177/2053951719885967

CONNOLLY, Regina. Dataveillance in the Workplace: Privacy Threat or Market Imperative? In: INFORMATION RESOURCES MANAGEMENT ASSOCIATION (IRMA). **Biometrics:** Concepts, Methodologies, Tools, and Applications. S/l, 2017, p. 1382-1397. DOI: 10.4018/978-1-5225-0983-7.ch056.

COWLS, Josh. Privacy Risks and Responses in the Digital Age. In: ÖHMAN, Carl; WATSON, David (org.). **The 2018 Yearbook of the Digital Ethics Lab**. Oxford: Springer, 2018, p. 113-148.

CRAIG, Paul; SEÏLER Néna Roa. Empathetic Technology. In: TETTEGAH, Sharon Y; NOBLE, Safiya Umoja (org.). **Emotions and Technology:** Communication of Feelings for, with, and through Digital Media. London; San Diego; Cambridge; Oxford: Elsevier Academic Press, 2016, p. 55-81.

DE MUL, Jos. Database Identity: Personal and Cultural Identity in the age of Global Datafication. In: DE BEEN, Wouter; ARORA, Payal; HILDEBRANDT, Mireille (org.). **Crossroads in new media, identity and law:** the shape of diversity to come. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan, 2015, p. 97-118.

DURANTE, Massimo; PAGALLO, Ugo. Legal Memories and the Right to be forgotten. In: FLORIDI, Luciano. **Protection of Information and the Right to Privacy:** A New Equilibrium? Cham: Springer, 2014, p. 17-30.

FERGUSON, Andrew G.. **The rise of big data policing:** surveillance, race, and the future of law enforcement. New York : New York University Press, 2017.

HARCOURT, Bernard E. **The counterrevolution:** how our government went to war against its own citizens. New York: Basic Books, 2018.

HAYES, Paul; VAN DE POEL, Ibo; STEEN, Marc. Algorithms and values in justice and security. **AI & Society**, 2020. DOI: 10.1007/s00146-019-00932-9.

KANETAKE, Machiko. The EU's dual-use export control and human rights risks: the case of cyber surveillance technology. **Europe and the World:** A law review, v. 3, n. 1, p. 1-16, 2019. DOI: https://doi.org/10.14324/111.444.ewlj.2019.14.

KANETAKE, Machiko. The Eu's Export Control of Cyber Surveillance Technology: Human Rights Approaches. **Business and Human Rights Journal**, v. 4, n. 1, p. 155-162, 2019b. DOI: https://doi.org/10.1017/bhj.2018.18.

KRAUSS, Kristin; KROEZE, Jan; VAN DER SCHYFF, Karl. Facebook and Dataveillance: Demonstrating a Multimodal Discourse Analysis. **Twenty-fourth America's Conference on Information Systems.** New Orleans: Association for Information Systems, 2018, p. 1-10. Disponível em: https://aisel.aisnet.org/amcis2018/Philosophy/Presentations/1/. Acesso em: 18 jan 2020.

LIEVENS, Eva; MILKAITE, Ingrida. The Internet of Toys: Playing Games with Children's Data? In: MASCHERONI, Giovanna; HOLLOWAY, Donell (ed.). **The Internet of Toys;** Practices, Affordances and the Political Economy of Children's Smart Play. Cham: Palgrave Maxmillan, 2018, p. 385-306. DOI: 10.1007/978-3-030-10898-4_14.

LUPTON, Deborah. **Digital Sociology**. New York: Routledge Taylor & Francis Group, 2015.

LUPTON, Deborah. The Diverse Domains of Quantified Selves: self-tracking Modes and Dataveillance. **Economy and Society**, v. 45, n. 1, p. 101-122, 2016. DOI: 10.1080/03085147.2016.1143726.

LUPTON, Deborah. Data mattering and self-tracking: what can personal data do? **Continuum:** Journal of Media & Cultural Studies, 2019. DOI: 10.1080/10304312.2019.1691149.

LUPTON, Deborah. "It's made me a lot more aware": a new materialista analysis of health self-tracking. **Media International Australia,** v. 171, n. 1, p. 1-14, 2019. DOI: 10.1177/1329878X19844042.

LUPTON, Deborah; MICHAEL, Mike. 'Depends on Who's Got the Data': Public Understandings of Personal Digital Dataveillance. **Surveillance & Society,** v. 15, n. 2, p. 254-268, 2017.

LUPTON, Deborah; WILLIAMSON, Ben. The Datafied child: The dataveillance of children and implications for their rights. **New Media & Society**, v. 19, n. 5, p. 780-794, 2017.

MARX, Gary T. Surveillance Studies In: SMELSER, Neil J.; BALTES, Paul B. (eds.). **International Encyclopedia of the Social & Behavioral Sciences**, 2 ed., Oxford: Elsevier, 2015, p. 733–741.

MARX, Gary T. **Windows Into the Soul:** Surveillance and Society in na Age of High Technology. Chicago; London: The University of Chicago Press, 2016.

PETZOLD, Thomas. Human-algorithmic scaffolding In: DE BEEN, Wouter; ARORA, Payal; HILDEBRANDT, Mireille (org.). **Crossroads in new media, identity and the law:** the shape of diversity to come. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan, 2015, p. 156-176.

RAHMAN, Hanif Ur; REHMAN, Ateeq Ur; REHMAN, Izaz Ur; NAZIR, Shah; SHAH, Nazir. **Privacy and Security:** Limits of Personal Information to Minimize Loss of Privacy. Stockholm University, Stockholm, Sweden, 2019.

ROSENBLAT, Alex. **Uberland:** how algorithms are rewriting the rules of work. Oakland: University of California Press, 2018.

SRNICEK, Nick; DE SUTTER, Laurent. **Platform Capitalism.** Cambridge; Malden: Polity Press, 2016.

TUROW, Joseph. **The Aisles Have Eyes:** how retailers track your shopping, strip your privacy, and define your power. New Haven; London: Yale University Press, 2017.

ZUBOFF, Shoshana. **Surveillance Capitalism and the Challenge of Collective Action:** New Labor Form. New York: The Murphy Institute, 2019.