ethic@
http://doi.org/10.5007/1677-2954.2025.e98091

A OFUSCAÇÃO COMO PRÁTICA DE RESISTÊNCIA AO CAPITALISMO DE VIGILÂNCIA DAS PLATAFORMAS DIGITAIS

THE OBFUSCATION AS A RESISTANCE PRACTICE TO THE SURVEILANCE CAPITALISM OF THE DIGITAL PLATFORMS

FELIPE DA VEIGA DIAS[1]
(ATITUS EDUCAÇÃO/Brasil)

LUAN BERTICELLI MOLOZZI[2]
(ATITUS EDUCAÇÃO/Brasil)

RESUMO

O presente trabalho procura entender as ferramentas de ofuscação como possível prática de resistência à forma atual do modelo de negócio das plataformas caracterizado como capitalismo de vigilância, que exerce poder por meio do controle da informação, moldando o comportamento e as subjetividades dos seus usuários enquanto lucra com a comercialização dos seus dados. Nesse contexto, a ofuscação como prática de resistência seria suficiente para a retomada da autonomia dos sujeitos sobre seus dados e sua privacidade? A pesquisa foi realizada utilizando de uma abordagem dedutiva, juntamente com a revisão bibliográfica em livros e artigos seminais sobre os assuntos e investiga, através de uma análise discursivo-argumentativa, a ofuscação como prática de resistência na retomada do controle dos dados pessoais dos seus usuários. Conclui-se que a ofuscação por si só não é suficiente para sanar os abusos cometidos pelo capitalismo de vigilância, sendo que o seu uso carece de orientação moral para finalidades protetivas, atenuando os danos causados (a direitos fundamentais), ampliando perspectivas sociais, culturais, políticas do ato de resistência, e subvertendo a ordem estabelecida ao retomar parte da autonomia dos sujeitos diante do poder exercido através do controle informacional.

Palavras-chave: Capitalismo de Vigilância; Ofuscação; Plataformas Digitais; Proteção de Dados; Resistência.

ABSTRACT

This work seeks to understand obfuscation tools as a possible practice of resistance to the current form of the platforms' business model characterized as surveillance capitalism, which exercises power through the control of information, shaping the behavior and subjectivities of its users while making profits. with the commercialization of your data. In this context, would obfuscation as a practice of resistance be sufficient to regain subjects' autonomy over their data and privacy? The research was carried out using a deductive approach, together with a bibliographical review of books and seminal articles on the subjects and

investigates, through a discursive-argumentative analysis, obfuscation as a practice of resistance in regaining control of users' personal data. It is concluded that obfuscation alone is not enough to remedy the abuses committed by surveillance capitalism, and its use lacks moral guidance for protective purposes, mitigating the damage caused (to fundamental rights), expanding social and cultural perspectives, policies of the act of resistance, and subverting the established order by retaking part of the subjects' autonomy in the face of the power exercised through informational control.
Keywords: Surveillance Capitalism; Obfuscation; Digital Platforms; Data Protection; Resistance.

Introdução

O atual modelo de negócio exercido pelas plataformas digitais, baseado no extrativismo massivo de dados pessoais dos seus usuários, transforma-se num capitalismo de vigilância, onde todas as interações humanas se tornam dados extremamente rentáveis para uma economia baseada em controle da informação. Ao controlar a informação, o capitalismo de vigilância é capaz de criar realidades paralelas, hiper individualizadas, confinando os sujeitos a esferas/bolhas informacionais que fragmentam a experiência coletiva e prendendo-os em um mito fundador de emancipação pelas plataformas digitais.

É pela lógica extrativista de dados exercida pelas plataformas, onde os sujeitos são transformados (ou mais precisamente, suas experiências são traduzidas em dados comportamentais) (Zuboff, 2021, p. 24) em matéria-prima de informações a serem vendidas para quem quer que esteja interessado, sem importar a destinação que será dada, que o capitalismo de vigilância exerce o seu poder assimétrico. Tal exercício força os usuários a usarem a sua privacidade como moeda de troca pelo uso dos bens e serviços ofertados, perdendo a autonomia nas suas relações sociais, de consumo e do próprio mundo real.

Essa nova forma de exercício de poder cria uma relação de subordinação dos usuários com as plataformas, uma vez que em um mundo cada vez mais conectado, torna-se impossível para o sujeito existir na sociedade moderna sem que ele tenha seus dados extraídos pelo capitalismo de vigilância. Seja nas relações pessoais intermediadas por redes sociais, nos hábitos de consumo em aplicativos ou, então, pelo simples exercício cívico do direito de votar, obriga-se a entrega dos dados às estruturas de poder do capitalismo de vigilância, para que se possa integrar a sociedade.

Diante dessa relação assimétrica e coercitiva, exercida por intermédio do controle sobre as informações, que coloca os sujeitos em situação de vulnerabilidade, esse trabalho analisa algumas das aplicabilidades,

implicações e os contextos em que as ferramentas de ofuscação podem servir como uma prática de resistência ao capitalismo de vigilância exercido pelas plataformas digitais. A partir dessa compreensão, buscamos responder à pergunta: as ferramentas de ofuscação, quando exercidas como ato de resistência, são suficientes para a retomada da autonomia dos sujeitos sobre os seus dados e a sua privacidade?

O artigo é dividido em três partes, a primeira conceituando as plataformas digitais e a forma como elas se transformam no capitalismo de vigilância pela lógica extrativista, que se apodera dos dados dos seus usuários. Na segunda parte, aborda-se como essa apropriação de dados pessoais dos sujeitos culmina em uma nova forma de exercício de poder sobre a informação, controlando as relações sociais, de consumo e a própria realidade dos usuários. Na última parte, aborda-se o uso de ferramentas de ofuscação como ato de resistência ao capitalismo de vigilância, entendendo as suas aplicações, implicações e os seus contextos, encontrando o seu papel na retomada da autonomia dos sujeitos sobre a sua própria privacidade.

O método elegido para abordagem é o dedutivo, tendo em vista a definição de concepções gerais e contextuais do ambiente social-tecnológico, para posteriormente realizar a observação das práticas de resistência, com ênfase na ofuscação. Ademais, empregou-se a técnica de pesquisa da documentação indireta com ênfase bibliográfica.

As plataformas digitais e o capitalismo de vigilância

Inicialmente, embora a pesquisa esteja centrada na visão acerca do capitalismo de vigilância, é valioso observar outros constructos conceituais contributivos com a abordagem proposta. Nesse sentido, encontra-se o conceito de capitalismo de plataforma, o qual alude à transformação do modelo de produção capitalista a um modelo baseado na extração, processamento e difusão dos dados obtidos por meio dos bens e serviços fornecidos pelas plataformas digitais (Morozov, 2018, p. 59). De uma forma geral, as plataformas digitais são infraestruturas que servem de elo entre usuários, consumidores, anunciantes, fornecedores e entidades dos mais variados tipos (Srnicek, 2017, p. 30).

Nesse sentido, a atuação das plataformas estaria centrada em uma espécie de "'extrativismo de dados' – em um paralelo direto com o extrativismo de recursos naturais que mantém as atividades de empresas de energia e dos produtores de commodities em todo o mundo" (Morozov, 2018, p. 171).

As plataformas digitais, em sua esmagadora maioria, referem-se a empresas com um valor de mercado extraordinário, cujo modelo de negócio aparenta ser nivelado e participativo, onde as pessoas interagem diretamente umas com as outras (Morozov, 2018, p. 59). Uma das características essenciais dessas plataformas é o que foi descrito por Srnicek (2017, p. 30) como "*network effect*" (ou efeito de rede), que representa, de forma literal, o potencial exponencial do modelo de negócio que sustenta essas plataformas, uma vez que, "quanto maior o número de usuários utilizando da plataforma, maior se torna o valor que essa plataforma terá para todos os outros" (Srnicek, 2017, p. 30, tradução nossa).

Esse efeito de rede faz com que as pessoas, ao escolherem uma plataforma para socializar, prefiram aquela em que a maior parte de seus amigos e familiares estejam presentes, tornando-a cada vez mais valiosa (Srnicek, 2017, p. 30), inclusive para o próprio mercado. Apesar de muitos usuários serem estimulados pelas plataformas digitais a performar as suas identidades no ambiente on-line, ou até mesmo capitalizar sobre o seu poder de influência, em alguns contextos sociais, como o verificado por David Nemer (2021) na Favela Território do Bem, em Vitória, Espirito santo, mais do que simplesmente socializar, aquelas pessoas buscam um espaço seguro para se comunicar, fazendo com que o uso destas plataformas de mídia social se torne muito "menos sobre performar identidade ou fazer novos amigos, e mais sobre reforçar conexões sociais existentes" (Nemer, 2021, p. 129-130).

Porém, mesmo que sirvam (segundo seus criadores) para o reforço das conexões existentes, a socialização promovida pelas plataformas, por meio de uma via extrativista de mercado, visa fundamentalmente atrair cada vez mais usuários (manipulação encontra-se embutida na essência do negócio das plataformas sociais) (Fischer, 2023, p. 37), cujos dados serão extraídos para serem usados das mais diversas formas. Como bem aponta Cesarino, este padrão mercadológico inverte a construção dos laços sociais, os quais deixam de ser formados em estruturas preexistentes como as escolas, igrejas e comunidades, passando a se formar a partir de relações puramente algorítmicas (Cesarino, 2022, p. 75).

O que antes era uma promessa emancipatória (Zuboff, 2021, p. 87), de uma internet intrinsecamente democratizante, que abalaria as estruturas de poder, passa a se tornar um "domínio feudal, nitidamente partilhado entre as empresas de tecnologia e os serviços de inteligência" (Morozov, 2018, p. 14-15). Apesar da ideia emancipatória das redes permanecer no imaginário do senso comum, não é porque o poder exercido sobre as massas não é mais o antigo modelo de produção capitalista que a população

está mais emancipada (Morozov, 2018, p. 178). Portanto, a retórica da liberdade democratizante do universo on-line e suas recentes plataformas oculta um funcionamento dominado por poucas corporações e uma distribuição desigual de informações/conteúdos (Loveluck, 2018, p. 206), cuja operacionalidade é viabilizada por ações humano-algorítmicas.

> Aqui também se pode detectar certa lógica em jogo – uma lógica do que chamo de "emancipação predatória". O paradoxo no cerne desse modelo é que nos tornamos cada vez mais enredados nas redes políticas e econômicas tramadas por essas empresas, mesmo quando cumprem um conjunto de promessas emancipatórias anteriores. Elas de fato nos oferecem um pouco de liberdade, mas isso só se dá ao preço de uma escravidão maior (Morozov, 2018, p. 177).

Essa sensação de liberdade emancipatória é necessária para o sustento da chamada economia de dados, que precisa que os indivíduos se coloquem à sua disposição, participando voluntariamente de ambientes propícios à extração de dados. Tal funcionamento opera com base na negação, ou ausência de concepção dos usuários de sequer estarem sendo controlados-manipulados pelas plataformas, o que faz com que se sintam livres e soberanos sobre o conteúdo que consomem (Cesarino, 2022, p. 70-71).

O sentimento emancipatório está diretamente ligado com a premissa-chave do extrativismo de dados, que vê os usuários como estoques de informações valiosas ou, conforme leciona Zuboff (2021, p. 18-19), produtores de superávit comportamental para comercialização em mercados futuros. Posto isso, as empresas de tecnologia concebem as mais diversas formas para fazer com que as pessoas abdiquem dos seus dados, ou que pelo menos os compartilhem voluntariamente (Morozov, 2022, p. 171).

> Nesse modelo de internet, os usuários vão perdendo o controle daquilo que aparece para si e de como eles mesmos aparecem para outros. Essas decisões vão sendo delegadas para os algoritmos e os usuários passam a uma posição cada vez mais passiva (Cesarino, 2022, p. 75).

As plataformas lucram ao turvar essa distinção entre a privacidade e a publicidade, armazenando dados que os usuários acreditam serem restritos apenas aos seus contatos, amigos e familiares. Independente do grau de publicidade que o usuário atribuiu a esses dados nas configurações disponibilizadas pela plataforma, a cada vez que ele "publica" algo para a

sua rede, antes dos seus contatos, é a plataforma digital que recebe tais conteúdos (Assange *et al*. 2013, p. 60).

As empresas de tecnologia dedicadas à mineração de dados buscam conhecer da forma mais exaustiva possível os comportamentos da população (Navarro, 2023, p. 126), o que faz com que todas as interações humanas intermediadas pelas plataformas se tornem pegadas digitais, que não só identificam os indivíduos como, também, quando somadas, conjugadas e processadas com metadados[3], criam uma espécie de "silhueta digital", que será preenchida e atualizada por cada nova interação realizada (Bruzzone, 2021, p. 43-44).

São poucas as corporações que possuem a capacidade técnica e estrutural de agregar, minerar e analisar essas enormes quantias de dados, alinhando-os a projetos sofisticados de máquinas de aprendizado e modelos preditivos direcionados à exploração de tecnologias de inteligência artificial[4] que são voltadas à agregação de valor a serviços, modelo que é descrito com precisão pelo que vem a ser conhecido como "capitalismo de vigilância" (Morozov; Bria, 2019, p. 180).

> Talvez seja inerente à tecnologia o surgimento de empresas cujo lucro reside principalmente na acumulação de nossos dados pessoais obtidos por meio da vigilância. Seguindo métodos semelhantes ao capitalismo industrial, atualmente, o nosso comportamento se transforma em mercadoria, outorgando às empresas e ao poder público um novo poder: prever e influenciar o nosso comportamento. Esse modelo de capitalismo, conhecido como capitalismo de vigilância, emerge diretamente da informação obtida através dos nossos dados (Navarro, 2023, p. 126, tradução nossa).

Assim, quando se fala em capitalismo de vigilância, se refere ao que Zuboff (2021, p. 15) define como uma mutação do capitalismo e de uma nova ordem econômica global, que se apropria da experiência humana como matéria-prima, destituindo a soberania dos indivíduos sobre os seus dados e atribuindo-lhes uma lógica econômica parasítica, que serve de base para a economia de vigilância. Essa economia de vigilância modifica os comportamentos humanos e impõe uma nova ordem coletiva, reivindicando o domínio sobre a sociedade, concentrando ainda mais riqueza, conhecimento e poder nas mãos das grandes empresas de tecnologia.

> O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit

> comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de mercados de comportamentos futuros. Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro (Zuboff, 2021, p. 24).

Os usuários são classificados, categorizados e pontuados em diversos modelos algorítmicos com base em suas preferências e padrões, abastecendo campanhas publicitárias predatórias que vendem promessas falsas ou exageradas (O'neil, 2020, p. 68). Esses anúncios miram especialmente pessoas vulneráveis, carentes ou até mesmo ignorantes, pois sabem que a sua "vulnerabilidade vale ouro" (O'neil, 2020, p. 69-70).

Dessa forma, não se pode mais denominar os usuários das plataformas digitais como "clientes" do capitalismo de vigilância, uma vez que eles se tornam "objeto de operação de uma extração de matéria-prima tecnologicamente avançada e da qual é cada vez mais impossível de escapar. Os verdadeiros clientes do capitalismo de vigilância são as empresas que negociam nos mercados de comportamento futuro" (Zuboff, 2021, p. 28).

O modelo extrativista, que se sustenta na categorização dos dados como uma espécie de commodities, ao ponto de comumente serem considerados como "o novo petróleo", não se restringe unicamente ao lucro, conforme aponta Bruzzone (2021, p. 45): "talvez mais que petróleo, pois não se trata apenas de dinheiro: o acesso a dados e o entendimento sobre o que fazer com eles é a nova forma do poder".

Essa nova forma de poder do capitalismo de vigilância age por meio de assimetrias nunca antes vistas, ligadas diretamente ao conhecimento e ao poder que dele resultam. As *Big Techs* sabem tudo sobre seus usuários e acumulam conhecimento sobre eles através de todas as interações que as plataformas intermedeiam, sendo capazes até mesmo de predizer e direcionar o comportamento futuro desses usuários, gerando ganhos para agentes externos, mas nunca para o próprio sujeito (Zuboff, 2021, p. 29).

> Um problema fundamental dos sistemas de coleta e análise de dados pessoais é a sua assimetria, ou melhor, duas assimetrias. A primeira, a assimetria de poder: raramente podemos escolher se queremos ou não ser monitorados, o que

> acontece com os nossos dados e o que acontece conosco por causa dessas informações. Temos pouco ou nenhum poder sobre quando somos vigiados em contextos inadequados e as informações são compartilhadas de forma inadequada com pessoas inadequadas. A segunda assimetria é igualmente importante, a assimetria epistêmica: raramente estamos completamente conscientes da vigilância e não sabemos o que será feito com os dados produzidos por ela, nem para onde e o que pode ser feito com essas informações (Brunton; Nissenbaum, 2011, p. 5, tradução nossa).

Esse imperativo econômico do capitalismo de vigilância, que reduz o mundo, a individualidade e o corpo ao permanente status de objeto (Zuboff, 2019, p. 316), se torna perigoso, uma vez que as plataformas digitais passam a ter não apenas o potencial de determinar o comportamento dos seus usuários, alterando o seu humor conforme as postagens selecionadas pelo algoritmo (O'neil, 2020, p. 172), mas também a capacidade de fragilizar a democracia ao influenciar os votos a partir dos dados vendidos para políticos, que os utilizam para direcionar as mais diversas propagandas políticas, alienando potenciais eleitores, validando a sua opinião com vieses de confirmação específicos (O'neil, 2020, p. 175-180).

Assim, o poder exercido pelo capitalismo contemporâneo, que aspira ao saber total, não é alcançado mediante uma narração ideológica, mas por uma pura operação algorítmica (Han, 2022, p. 20). Significa dizer que este regime guiado pela informação-dados possui a capacidade de influenciar os comportamentos em um nível abaixo do limiar da consciência, de forma que "se apodera das camadas pré-reflexivas, pulsionais, emotivas, do comportamento antepostas às ações conscientes" (Han, 2022, p. 23).

Portanto, neste modelo de dados-informações ocorre a apropriação de "técnicas de poder neoliberais. Em oposição às técnicas do poder do regime disciplinar, não trabalham com a coação e interdições, mas com estímulos positivos". Há impulsão à produtividade do dito "capital humano" em se autopromover (Dardot; Laval, 2016, p. 229-231) fazendo uso de sua liberdade (devidamente conduzida), de modo que em lugar de repressões se tem a inserção de regimes de poder "*smart*, que não dá ordens, mas sussurra, que não comanda, mas que *nudge*, quer dizer, que dá um toque com meios sutis para controlar o comportamento" (Han, 2022, p. 17).

Um estudo conduzido em cooperação pelo próprio Facebook durante as eleições norte-americanas de 2010, revela como o imperativo econômico e a lógica extrativista das plataformas digitais transcende o digital ao converter o poder informacional em controle comportamental. Ao exibir um banner indicando quais "amigos" teriam votado, elevou em 0,39% a taxa de comparecimento do grupo exposto, mobilizando cerca de 60.000 votos

diretos e, em uma espécie de efeito dominó, outros 340.000 votos, número expressivamente superior à margem de 537 votos que definiu a vitória de George W. Bush na Flórida em 2000 – e, consequentemente, a corrida presidencial (Zittrain, 2014).

Em outro estudo conduzido por Kramer, Guillory e Hancock (2014) no Facebook, expôs, em grande escala, a capacidade das plataformas digitais influenciarem o estado emocional dos seus usuários. Ao manipular de forma discreta o algoritmo do *feed* de 689.003 perfis, suprimindo publicações positivas e/ou negativas, foi possível observar que pequenas variações na exibição de palavras é suficiente para repercutir de forma significativa no humor exibido pelos próprios usuários em suas postagens subsequentes (Kramer; Guillory; Hancock, 2014).

O controle algorítmico, imperceptível e aparentemente insignificante, permite que as plataformas digitais não se limitem a prever preferências, mas que com isso possam influenciar, ou controlar, tanto estados emocionais de seus usuários, quanto seus atos, influenciando concretamente até mesmo o exercício cívico do voto, convertendo a intimidade psíquica e moral dos sujeitos submetidos ao capitalismo de vigilância.

Além disso, quando as interações sociais passam a ser intermediadas pelos algoritmos[5] das plataformas digitais, otimizados para a lógica capitalista da extração de dados, os usuários passam a viver em "mundos personalizados que confirmam seus enquadramentos individuais" (Cesarino, 2022, p. 75), reforçando a ideia de que "quem controla essas mediações controla o próprio acesso das pessoas ao real" (Cesarino, 2022, p. 46). Valioso, ainda, situar o crescimento de estudos que interligam ações concretas, algumas de cunho odioso, antidemocrático, violento ou genocida, ao estímulo, em grande parte fantasioso ou falso, ofertado pelas redes sociais (Fischer, 2023).

Ante o exposto, o controle algorítmico inconsciente dialoga com o fato de que a cognição humana não tem acesso à realidade a não ser através de mediações que, neste caso, são intermediadas pelos algoritmos das plataformas digitais e segmentam os usuários em mundos personalizados, que se conectam apenas parcialmente, resultando em realidades paralelas (Cesarino, 2022, p. 82). Tais segmentos formados se inclinam à radicalidade, tendo em vista que a métrica do engajamento impulsiona cada vez mais conteúdo de natureza odiosa-raivosa como regularidade (Fischer, 2023, p. 91), algo distante das comunidades livres e plurais prometidas pelas companhias tecnológicas.

O regime de informação e a sociedade do controle

A partir do denominador da vigilância capitalista baseada em dados e na produção de subjetividades, observam-se novos regimes de força. Han (2022) introduz a noção de "regime da informação" como "a forma de dominação na qual informações e seu processamento por algoritmos e inteligência artificial determinam decisivamente processos sociais, econômicos e políticos" (Han, 2022, p. 7). Esse regime de informação é acoplado ao desenvolvimento do capitalismo de vigilância e "degrada os seres humanos em gado, em animais de consumo e dados" (Han, 2022, p. 7).

Nessa óptica, o poder disciplinar deixaria de ser exercido pela posse dos meios de produção industriais e passaria a ser exercido por meio do acesso aos dados utilizados para vigilância, controle e prognóstico dos comportamentos, delineando uma governamentalidade psicopolítica (Han, 2022, p. 7) ou tecnopolítica (Lama; Sanchez-Laulhe, 2020). Esse poder disciplinar é compreendido como aquele que "em vez de se apropriar e de retirar, tem como função maior 'adestrar'; ou sem dúvida adestrar para retirar e se apropriar ainda mais e melhor" (Foucault, 2014, p. 167).

Essa submissão causada pelo adestramento do poder disciplinar "fabrica" os indivíduos por meio de técnicas, criando uma noção de obediência e docilidade, transformando-os ao mesmo tempo em objetos e instrumentos de seu exercício (Foucault, 2014, p. 167), segundo Han, o poder disciplinar difere substancialmente daquele exercido pelo regime da informação, pois "o sujeito submisso do regime de informação não é nem dócil, nem obediente. Ao contrário, supõe-se livre, autêntico e criativo. Produz-se e se performa" (Han, 2022, p. 9).

Independente da perspectiva adotada, o fato é que o poder exercido pelo capitalismo de vigilância restringe os corpos e as suas individualidades ao permanente status de objeto, reduzindo os indivíduos a uma única dimensão de equivalência, como simples "ativos de informação que podem ser desagregados, reconstituídos, indexados, navegados, manipulados, analisados, reagregados, preditos, produtizados, comprados e vendidos – em qualquer lugar, a qualquer momento." (Zuboff, 2021, p. 316).

Observa-se assim que o poder disciplinar (atuante nos corpos individualizados), ou mesmo o biopoder (voltado ao gerenciamento da vida das populações), embora ainda sendo exercidos, deixam de ser priorizados no contexto da vigilância. Dessa forma, o biopoder deve ser reconhecido como noção indispensável ao desenvolvimento do capitalismo, "que só pôde ser garantido à custa da inserção controlada dos corpos no aparelho de

produção e por meio de um ajustamento dos fenômenos de população aos processos econômicos" (Foucault, 2023, p. 151 – 152).

No entanto, a atualidade exibe regimes de controle mais insidiosos e sofisticados nas relações de poder estabelecidas, atribuindo às tecnologias um papel especial nesse cenário. Com base nessa nova interlocução humano-máquina se alude a operacionalidade de uma governamentalidade tecnopolítica.

> Apregoa-se então que falar sobre tecnopolítica é realizar a leitura dos processos sociotécnicos que inter-relacionam a gestão da vida por meio de dispositivos tecnológicos, algoritmos, redes, os quais moldam subjetividades e são ao mesmo tempo transformados por elas. Tem-se assim um segundo elemento nevrálgico, haja vista que a importância da tecnopolítica encontra-se exatamente no ponto em que não apenas dá forma às tecnologias, como as mesmas também passam a compor ou a dar forma aos seres humanos (Dias, 2022, p. 138).

Ocorre que as concepções sobre o corpo estão sempre sujeitas às mudanças, criando diferentes formas de compreendê-lo, permitindo, inclusive, que se diga que a noção de corpo se determina pelos conhecimentos e linguagens disponíveis, bem como pelas maneiras práticas que o manuseiam. Dessa forma, é pela passagem da percepção do corpo-físico para o corpo-informação, em que o corpo humano passa por um processo de digitalização ou dataficação dos seus aspectos físicos e biométricos (Loureiro; Carneiro, 2020, p. 206), que se pode compreender a noção do capitalismo de informação a partir do controle dos corpos e uma nova produção de subjetividades.

Um bom exemplo de digitalização dos aspectos físicos e biométricos foi em 2008, quando o Tribunal Superior Eleitoral (TSE) deu início ao programa de recadastramento biométrico, com o objetivo de coletar esses dados para verificar a identidade dos indivíduos nas suas atividades eleitorais, fazendo com que a impressão digital passe a ser um requisito ao legítimo exercício do voto (Loureiro; Carneiro, 2020, p. 209).

Já em 2017, flexibilizando a finalidade eleitoral, foi aprovada a Lei 13.444/2017, conhecida como Lei de Identificação Civil Nacional, sancionada com o propósito de identificar o brasileiro em suas relações com a sociedade, com os órgãos, entidades governamentais e com os meios privados, permitindo ao Poder Público o acesso gratuito ao banco de dados do ICN, inclusive os dados biométricos da Justiça Eleitoral (Brasil, 2017).

Mais adiante na linha do tempo, em 2018, é sancionada a Lei Geral de Proteção de Dados (Lei 13.709/18), instrumento jurídico cuja premissa

central reside na tutela da privacidade e dos dados pessoais. No entanto, o seu artigo 4º, inciso III, determina que a legislação não será aplicada aos tratamentos de dados realizados para fins exclusivos de: "a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais" (Brasil, 2018).

> A quantificação e a computação obscurecem os processos sociais, e o uso de algoritmos e plataformas de propriedade privadas tornam o processo decisório incrivelmente opaco. As ferramentas tecnológicas de vigilância policial estão avançando muito mais rapidamente do que as leis que as regulam, resultando em uma incompatibilidade entre a lei escrita e a lei aplicada (Brayne, 2021, p. 17, tradução nossa).

Essa exceção à proteção dos dados escancara a submissão causada pelo poder, que se utiliza da lógica extrativista de dados do capitalismo de vigilância para quantificar os seus sujeitos, adestrando-os e tornando-os submissos aos modelos algorítmicos utilizados para maior controle e vigilância social (Morozov; Bria, 2019, p. 178). Esse controle exercido faz com que os indivíduos não tenham saída, situação em que pregar o simples autocontrole, entendido aqui como "recusa de compartilhamento de dados", diante de uma cultura extrativista, reduz um problema coletivo e político ao nível individual (Morozov, 2018, p. 183).

Uma das falácias retóricas da discussão sobre proteção ou privacidade de dados se dá pela ideia de que a recusa de submissão de informação às plataformas digitais é uma responsabilidade individual, sendo possível uma espécie de "*opt-out*". Ainda que facultativos em alguns casos, muitos desses sistemas implicam custos sociais e pessoais substanciais, tornando ilusória a noção de recusa voluntária (*opt-out*) (Brunton; Nissenbaum, 2011, p. 6).

Ademais, outro registro relevante é trazido por Véliz (2020, p. 12) ao comentar sobre a formação de perfis de usuários que não participam ou interagem nas plataformas, denominados de sombras. O perfil sombra do Facebook é o demonstrativo de que mesmo que alguém assuma a postura de resistência às práticas corporativas de governamentalização algorítmica, isso não costuma funcionar de forma tão simples e coloca em xeque a concepção de subverter as ferramentas de controle digital.

Posto isso, considera-se que o submisso se coloca nessa posição pois para ele é impossível desobedecer, uma vez que a razão da obediência do sujeito está na violência e nas relações de força a ele impostas, tornando as sanções imediatas e demasiadamente pesadas (Gros, 2018, p. 39). Até mesmo o uso de e-mail gratuito, redes sociais e ferramentas de busca podem parecer mais opcional do que necessário, mas abdicar do seu uso

significa abandonar uma significativa porção da vida social intermediada pelas plataformas digitais (Brunton; Nissenbaum, 2011, p. 6).

> Seus dados não são acumulados em circunstâncias neutras, sejam eles coletados por meio de uma vigilância a nível infraestrutural em que você precisa participar, ou formas as quais seja necessário preencher um formulário para receber serviços essenciais, ou termos de serviços onerosos que você deve consentir para usar um produto online que se tornou vital aos negócios. O contexto frequentemente apresenta um desequilíbrio de poder, seja entre indivíduos consumidores e as grandes corporações, ou cidadãos e governos. (Brunton; Nissenbaum, 2011, p. 5, tradução nossa).

Na verdade, é muito simples para um indivíduo obter a emancipação do capitalismo de vigilância, basta que leve uma vida isolada e não documentada como um imigrante trabalhador dos anos 1920, sem internet, sem telefones, sem seguro, sem ativos, atuando fora dos livros e sendo pago em espécie por um trabalho manual ilegal (Brunton; Nissenbaum, 2015, p. 85).

É preciso reconhecer que o sujeito submisso obedece não por escolha racional, mas porque o custo da desobediência se revela insustentável diante da violência simbólica e estrutural do sistema, "no fundo, a única razão para obedecer é a impossibilidade de desobedecer" (Gros, 2018, p. 40). Portanto, atrelar a responsabilidade pela proteção dos dados à uma escolha individual significa deixar a privacidade à mercê dos meios de regulação, ou então, de quaisquer meios ou atos de resistência que estiverem disponíveis e dentro das capacidades dos sujeitos (Bruntom; Nissenbaum, 2011, p. 6).

Assim, torna-se evidente que o extrativismo de dados ocorre em um contexto de relação assimétrica de poderes, onde além de o sujeito não ter o poder de escolher se será vigiado ou não, não sabe o que é feito com esses dados coletados e muito menos o que será feito com ele com base nas conclusões obtidas através dessas informações (Brunton; Nissenbaum, 2015, p. 49).

A ofuscação como ato de resistência

Dado que é inviável sustentar uma vida integralmente pautada por princípios, sob uma perspectiva prática, os indivíduos inevitavelmente se veem comprometidos em relações assimétricas cotidianamente, frequentemente sem o controle ou o consentimento que gostariam (Brunton; Nissenbaum, 2015, p. 55).

Atualmente, leva-se um estilo de vida que obriga partes significativas das populações a passarem cada vez mais tempo conectados às redes, espaço em que é ainda mais difícil de evitar o poder de vigilância (Navarro, 2023, p. 127), porém, ainda há maneiras de inserir práticas de resistência e de autonomia, armas dos mais fracos, no cotidiano (Brunton; Nissenbaum, 2015, p. 55). Lembrando que "o poder é um feixe de relações mais ou menos hierarquizadas, mais ou menos coordenadas, constantemente ameaçadas pela própria liberdade que procura domar e pelas formas de resistência que o atravessa" (Chignola, 2020, p. 29), de modo que as atuais articulações tecnopolíticas vêm dando origem a novas práticas de resistência.

O direito de resistência, embora não positivado expressamente, decorre de uma interpretação sistemática da Constituição Federal de 1988, especialmente no art. 5º, § 2º, e se apresenta como mecanismo de autodefesa social na salvaguarda dos direitos fundamentais e da ordem constitucional (Buzanello, 2001, p. 11).

> De outro lado, a construção constitucional elucida, de forma implícita, a materialidade da resistência. A materialidade se combina com os elementos constitucionais formais, como: os princípios da dignidade da pessoa humana e do pluralismo político, erguidos como fundamentos do Estado Democrático (art. 1°, III, V, CF); a abertura e a integração para dentro do ordenamento constitucional de outros direitos e garantias decorrentes do regime e dos princípios por ela adotados (art. 5º, § 2º, CF) (Buzanello, 2001, p. 21).

Ainda, recentemente, a Emenda Constitucional nº 115, de 2022, inseriu no artigo 5º da Constituição Federal Brasileira o inciso LXXIX, que assegura, nos termos da lei, o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais (Brasil, 2022). Por mais que seja um significativo passo na estruturação de princípios éticos e legais que possam servir para impedir a consolidação de formas perigosas de controle social, político e institucional, a simples positivação do direito na Constituição não é suficiente para fazê-lo efetivo.

Dessa forma, num contexto de capitalismo de vigilância, surgem táticas de resistência digital, projetos de defesa cujo objetivo é formar um vernáculo de resistência ao extrativismo de dados através do que vem a ser denominado "ofuscação". A ofuscação consiste na produção deliberada de dados enganosos, ambíguos ou simulados, com o objetivo de comprometer a confiabilidade das informações extraídas por sistemas de vigilância digital e, portanto, menos valiosas (Brunton; Nissenbaum, 2011, p. 2).

A escolha da palavra "ofuscação", além de apresentar certa obscuridade, também serve para diferenciar a prática dos outros métodos, especialmente os que se baseiam na exclusão, alteração e desaparecimento de dados (Brunton; Nissenbaum, 2015, p. 46). Apesar de ambas as táticas servirem a propósitos parecidos, a ofuscação se limita à adição de ruídos (Brunton; Nissenbaum, 2011, p. 14). Nesse sentido, a ofuscação também pode ser entendida como uma forma de camuflagem, uma vez que visa desaparecer, evitar, redirecionar, confundir e enganar a atenção dos mecanismos de vigilância e extração de dados.

Todas as práticas de ofuscação procuram se posicionar criticamente contra a coleta massiva de dados que sustenta o atual capitalismo de vigilância e as suas mazelas, procurando pontos cegos para neutralizar os seus impactos. Essas táticas de ofuscação, em sua maioria, geram "ruídos de fundo" sobre as atividades humanas intermediadas pelas plataformas digitais, distorcendo as informações obtidas e processadas pelo modelo extrativista das plataformas (Navarro, 2023, p. 130).

Existem muitas formas, métodos, motivos e meios para a aplicação de táticas de ofuscação, variedade intrinsecamente ligada ao caráter reativo da estratégia, que pode ser exercida tanto por um único indivíduo quanto por um grupo de pessoas que atua em conjunto (Brunton; Nissenbaum, 2011, p. 13).

É importante ressaltar que essas ferramentas de ofuscação não devem substituir os outros modelos de defesa de direitos (que incluem liberdade, privacidade, proteção de dados), como a implementação de leis, regulamentos, normas e convenções sociais, mas que podem servir como um complemento, uma vez que a sua finalidade é a mesma, a de preservar a autonomia e a privacidade dos usuários (Navarro, 2023, p. 130). Por isso registra-se (apesar da análise regulatória transcender o escopo deste estudo), o reconhecimento da importância dos debates jurídicos que almejam a proteção social e coletiva da população, mesmo que tais garantias e mecanismos institucionais não signifiquem a inviabilidade das organizações de resistência.

Primeiro, para compreender o conceito de ofuscação, é necessário entender a sua utilidade técnica na defesa e construção da privacidade, servindo como prática de resistência aos modelos de extração e análise de dados do capitalismo de vigilância. A privacidade se torna importante a partir do momento que se entende que aqueles que sabem sobre as vidas dos indivíduos, possuem poder sobre seus comportamentos e subjetividades. E quem possui poder sobre as pessoas, geralmente, pode negar acesso ao emprego, ao crédito, à moradia, à educação ou a qualquer

outro direito ligado ao exercício de uma vida digna (Brunton; Nissenbaum, 2015, p. 53).

Um exemplo de ferramenta são os navegadores (*web-browsers*), instrumentos que intermediam o acesso a qualquer site da internet e são elementos chaves à frustração das estruturas de poder do capitalismo cibernético pelas práticas de ofuscação. O simples uso de uma extensão (*plugin*) gratuita dos navegadores Firefox e Chrome, o *TrackMeNot*, é suficiente para ofuscar os dados. Essa ferramenta funciona mandando solicitações chamarizes para as ferramentas de buscas como o Google, o Bing ou o Baidu, escondendo os verdadeiros interesses do usuário em uma espécie de "barulho" digital (Howe, 2015, p. 89).

Outro demonstrativo é a extensão *AdNauseam*, que ofusca os dados coletados pelas redes de publicidade e propaganda. O *plugin*, além de bloquear a exibição de anúncios ao usuário na superfície, ao fundo "clica" em todos, poluindo os perfis dos usuários e criando desconfiança entre os patrocinadores dos anúncios e as redes de publicidade que são "pagas por clicks" (Howe, 2015, p. 91).

Para além dos navegadores, outras estratégias de ofuscação emergiram do digital para a vida nas ruas. A *Facial Weaponization Suite*, elaborada por Zach Blas, insere-se como performance crítica ao intervencionismo algorítmico, utilizando máscaras construídas a partir de composições biométricas que confundem os sistemas de reconhecimento facial (Howe, 2015, p. 92).

Essas táticas de ofuscação podem ser categorizadas conforme os seus objetivos. Uma tática de ofuscação "*time-based*" é baseada em ganhar tempo, distraindo um sistema por um curto momento de tempo, como os "*decoys*" em aviões militares, usados para criar uma distração momentânea nos radares inimigos (Brunton; Nissenbaum, 2011, p. 8-9).

Existem também as táticas de ofuscação cooperativa que objetivam causar um efeito de rede, já abordado nesse texto, tornando-se mais efetiva na medida em que mais usuários a aderem. Um exemplo é a suposta história que, certa vez, na Dinamarca, durante a ocupação nazista, o rei e a população decidiram voluntariamente usar uma estrela amarela, fazendo com que fosse impossível distinguir os judeus dos não-judeus (Brunton; Nissenbaum, 2011 p. 9).

Outra forma é a ofuscação seletiva, que permite que determinados dados continuem sendo úteis e acessíveis apenas para quem interessa, preservando a privacidade dos seus usuários enquanto interfere nos métodos de análise. Tal prática é vislumbrada no *FaceCloak*, um *plugin* que esconde os dados publicados nas redes sociais, mostrando-os apenas aos

usuários que também possuam a extensão instalada (Brunton; Nissenbaum, 2011, p. 10-11).

Por fim, a tática de ofuscação por ambiguidade, cujo objetivo é transformar permanentemente os dados em informações imprecisas e inconfiáveis. Aqui retoma-se o instrumento já apresentado do *TrackMeNot*, que insere entradas de distrações em conjunto com a entrada original, confundindo os algoritmos de análise de dados que não conseguem identificar qual delas é a verdadeira.

Destarte, as ferramentas citadas são desenhadas para dificultar a mineração e agregação dos dados em perfis de usuários, tornando-os imprecisos ou duvidosos, diminuindo o valor dos dados coletados, protegendo não só os dados do usuário dessas ferramentas, mas também os que não fazem uso, uma vez que nenhum conteúdo passa a ser confiável em um banco de dados comprometido (Howe, 2015, p. 93-94).

Utilizar das ferramentas de ofuscação como práticas de resistência significa inverter a lógica de controle da realidade (Cesarino, 2022, p. 82), construindo uma figura irreal ao adversário que compila e processa os dados extraídos pelas plataformas digitais (Brunton; Nissenbaum, 2011, p. 13). Mais do que somente esconder uma mensagem, cobrir um discurso ou abafar um ato subversivo, a ofuscação dá a oportunidade de o sujeito recuperar e exercer a sua autonomia (Brunton; Nissenbaum, 2015, p. 59).

Dessa forma, se pode dizer que o uso da ofuscação geralmente almeja três objetivos que se interrelacionam: o primeiro deles é a proteção, minimizando os danos causados pela falta de privacidade; o segundo é a expressão, que visa amplificar as perspectivas sociais, culturais e políticas; e, por fim, a subversão, ao atuar em uma lógica de insurreição diante do controle exercido sobre os dados na economia da informação (Navarro, 2023, p. 128). Esse conjunto estratégico ofertado aos usuários se alinha a noção foucaultiana de resistência política, no sentido de combater as condições insuportáveis dispostas pelas relações de poder (Foucault, 2006, p. 46), atualmente regidas pelos parâmetros capitalistas e tecnopolíticos.

Logo, as diferentes ferramentas de ofuscação que emergem em um contexto de resistência dos usuários na retomada da autonomia sobre o controle dos seus dados não possuem um valor político ou ético em si, mas sim nas finalidades em que são empregadas.

Assim, o emprego desses instrumentos é alvo de debates sobre a sua ética e a sua moral, sendo necessário sopesar os seus contextos, aplicações e finalidades, por exemplo: se a vigilância e o contexto aos quais a ofuscação é aplicada forem moralmente problemáticos, a ofuscação pode ser justificada frente a práticas injustas de processamento de dados pessoais (Brunton; Nissenbaum, 2011, p. 15).

O debate moral aborda questões sobre desonestidade, desperdício, poluição, danos aos sistemas e o efeito carona dos usos das ferramentas de ofuscação. De uma forma ampla, é possível argumentar cada um desses pontos, partindo de um contexto e finalidade de aplicação cujo objetivo é resistir a um ato coercivo, abusivo ou ameaçador, momento que até mesmo um ato "desonesto" se torna legítimo e justificável (Brunton; Nissenbaum, 2015, p. 65).

Em abordagem correlata, abrangendo mais a complexidade do uso do anonimato para resistência, Andreatta e Sabariego (2024, p. 173) demarcam que mesmo sem desconstruir as previsões constitucionais em prol do posicionamento político, se viabiliza observar aspectos inerentes a uma sociedade do controle em que sem o anonimato determinadas resistências a movimentos autoritários seriam impossibilitadas. Isso significa que seja o anonimato ou a ofuscação nos atuais contextos assimétricos ou, por exemplo, de levantes antidemocráticos, seriam plenamente justificadas, a fim de possibilitar condições mínimas de resistência e livre exercício de direitos.

Outra crítica comum às táticas de ofuscação é a possibilidade de causar desperdícios, danos e poluição aos bancos de dados, uma vez que alguns deles podem ser úteis ao desenvolvimento de projetos benéficos à sociedade, como iniciativas para melhorar a eficiência de uma cadeia logística, realizar uma análise demográfica de saúde populacional ou avaliar o efeito de políticas públicas. O processamento desses dados extraídos guia as decisões algorítmicas sobre os indivíduos, e introduzir ruídos nesse sistema pode interferir com a criação de perfis que, eventualmente, podem prejudicar inocentes que não tiveram participação na ofuscação (Brunton; Nissenbaum, 2011, p. 16-17).

Tais críticas partem, não raro, da suposição de que há uma forma legítima e aceitável de exploração e análise de dados. Contudo, quando se demonstram práticas opressivas ou abusivas, a ofuscação se converte em um instrumento eticamente válido de resistência (Brunton; Nissenbaum, 2015, p. 65-67).

Talvez o debate mais importante esteja no efeito carona, em que um indivíduo protege a sua privacidade direcionando a atenção do adversário para um alvo que não ofuscou os seus dados. A situação cogitada segue a ideia de que você não precisa ser mais rápido que o predador, apenas mais rápido do que as outras presas (Brunton; Nissenbaum, 2011, p. 16).

A perspectiva supramencionada torna o debate extremamente relevante e levanta duas questões principais: o sistema de ofuscação que está sendo utilizado é gratuito e disponível para todos? As pessoas que não o utilizam podem ser prejudicadas pelo seu uso? Se a resposta para as

perguntas for "sim" e "não", respectivamente, como muitos dos sistemas aqui apresentados, não se compreende como um ato imoral e que deva ser condenado, no entanto, ainda que as respostas para as perguntas sejam contrárias, deverá existir espaço para o debate, que precisa apreciar caso a caso, conforme o seu contexto de aplicação (Brunton; Nissenbaum, 2015, p. 67-68).

Novamente de forma analógica se entende que "em um jogo de cartas marcadas, o mínimo que se pode fazer é não revelar sua mão", por isso anonimizar-se ou ofuscar-se "na rede não equivale apenas a escapar da bruta redução do sujeito a um produto ou à matéria, mas a criar uma outra forma de existência" (Andreatta; Sabariego, 2024, p. 171).

Quando os sujeitos são obrigados a renunciar as suas informações pessoais sem uma explicação razoável das suas finalidades para que possam fazer uso de um serviço quase obrigatório ao convívio social, resta demonstrada a desproporção dos valores pagos pelos serviços prestados em contrapartida ao potencial lucro das grandes empresas com os dados dos usuários, revelando o caráter exploratório e opressivo do extrativismo de dados (Brunton; Nissenbaum, 2015, p. 68).

Os indivíduos que fazem uso da ofuscação como uma prática de resistência operam de uma posição de vulnerabilidade, obrigados a aceitar escolhas que eles provavelmente recusariam, resultando numa relação de submissão. Nesta relação de submissão às *Big Techs*, a ofuscação não é mais um luxo daqueles preocupados com a sua privacidade, mas uma ação limítrofe de resistência em que, diante da constante vigilância e manipulação das nossas informações, torna-se uma forma legítima de desobediência (Brunton; Nissenbaum, 2011, p. 19).

Nessa perspectiva das práticas de ofuscação como um exercício do direito de resistência, é necessário ter uma noção clara de onde se quer chegar com o ato de ofuscar (Brunton; Nissenbaum, 2015, p. 86). Ofuscar os dados oferece a possibilidade de proteger pessoas do escrutínio do extrativismo de dados que alimentam os algoritmos do capitalismo de vigilância (Brunton; Nissenbaum, 2011, p. 19-20). Assim, a ofuscação se torna a possibilidade de refúgio quando os outros meios falham, servindo como uma força positiva para a cultura de dados contemporânea e representando valiosos recursos para a defesa da privacidade e autonomia de escolha humana.

Conclusão

Para responder se as ferramentas de ofuscação, quando inseridas em um contexto de resistência, são aptas a promover a retomada da autonomia

dos sujeitos sobre seus dados e sua privacidade, teve-se que compreender como as plataformas digitais sustentam o capitalismo de vigilância por meio da lógica mercadológica do extrativismo de dados. Soma-se a isso a necessária leitura da forma com que o controle sobre esses dados culmina em uma nova articulação de poder sobre dados-informações, que moldam as relações de consumo, as interações sociais e a própria percepção da realidade, cada vez mais segregada e individualizada.

O regime de forças disposto assume o controle sobre os dados obtidos por intermédio do capitalismo de vigilância, produzindo subjetividades adaptadas-normalizadas ao atual modelo. Isso se operacionaliza pela via do gerenciamento tecnopolítico, estabelecendo uma relação assimétrica (e insidiosa) de submissão, obrigando o usuário ao fornecimento de seus dados como moeda de troca às entidades de controle pelo simples exercício da sua vida em sociedade.

Essa transformação nas relações de poder pelo controle da informação-dados, criando uma falsa sensação de emancipação e autonomia, reforça o condicionamento "livre" dos indivíduos, subordinando-os a uma lógica extrativista do capitalismo de vigilância, que quantifica os sujeitos e os adestra, tornando-os submissos aos algoritmos de controle e vigilância social, impedindo que retomem a autonomia do controle sobre os seus próprios dados.

É nesse cenário que se insere o uso das ferramentas de ofuscação como prática reativa e estratégica de resistência frente ao capitalismo de vigilância e à governamentalidade tecnopolítica. Logo, os indivíduos acabam vitimados por esta relação assimétrica e, ao se manterem passivos, deixam a sua privacidade à mercê dos meios de regulação, que por muitas vezes demoram (ou simplesmente não agem) para impedir os abusos cometidos.

Tais ferramentas, quando empregadas como práticas de resistência (garantida constitucionalmente), almejando uma finalidade específica, clara e objetiva, mostram-se muito úteis no combate às estruturas de poder formadas a partir do controle dos dados e da informação. Embora representem respostas pontuais e reativas à dominação informacional do capitalismo de vigilância, as ferramentas de ofuscação não se mostram suficientes, por si sós, para sanar a complexidade do problema. Para que a ofuscação funcione, o seu uso precisa ser moralmente guiado à uma finalidade de proteção, minimizando os danos causados pela falta de privacidade; expressiva, ampliando as perspectivas sociais, culturais e políticas do ato de resistência; e subversiva, retomando a autonomia dos sujeitos diante do poder exercido através do controle informacional.

Importa frisar que este trabalho não se propõe a discutir, exaustivamente, a necessidade de regulação específica da matéria. O

enfoque recai sobre o uso da ofuscação como manifestação de resistência individual diante do poder informacional. Ainda que se reconheça a carência de regulação institucional, compreende-se que a resistência individual — aqui representada pela prática da ofuscação — constitui apenas um dos elementos de um espectro mais amplo de respostas possíveis ao poder informacional exercido pelas plataformas digitais.

Notas

[1] Pós-doutor em Ciências Criminais pela PUC/RS. Doutor em Direito pela Universidade de Santa Cruz do Sul (UNISC) com período de Doutorado Sanduíche na Universidad de Sevilla (Espanha). Professor do Programa de Pós-Graduação em Direito da Atitus Educação – Mestrado. Professor do curso de Direito da Atitus Educação – Passo Fundo – RS. Brasil. Coordenador do Grupo de Pesquisa "Criminologia, Violência e Controle". Advogado. Passo Fundo – Rio Grande do Sul – Brasil. Orcid: 0000-0001-8603-054X.

[2] Mestrando em Direito na Atitus Educação. Pós-graduando em LGPD, Privacidade e Proteção de Dados pela Universidade Candido Mendes. Pós-graduado em Advocacia Corporativa pela Fundação do Ministério Público. Graduado em Direito pela Universidade Regional Integrada do Alto Uruguai e das Missões. Advogado, Compliance Officer e Encarregado de Dados. Orcid: 0009-0004-7103-8185.

[3] Uma forma de entender os metadados é defini-los como "registros de atividades" realizadas pelos nossos dispositivos: a hora em que realiza a chamada, para quem e qual a sua duração, ou quanto tempo estamos vendo a televisão. Esse conceito também abarca tudo aquilo que os nossos dispositivos fazem de forma mecânica: contagem dos passos que damos, rastreamento da nossa geolocalização, ou nossos batimentos cardíacos enquanto dormimos. Esses dados, por si só, podem parecer inofensivos, mas devemos considerar que os metadados são gerados de forma automática, o que faz com que tenhamos mínimo controle sobre eles (Navarro, 2023, p. 127, tradução nossa).

[4] Acerca do tema da Inteligência artificial e suas correlações com a liberdade é importante referir o recente texto de Azambuja (2023, p. 521-525), o qual problematiza as consequências da algoritmização da vida e dos efeitos sociais e democráticos no Brasil e no mundo.

[5] Assim como Big Data o termo "algoritmo" possui um significado técnico e não técnico. Um algoritmo é tecnicamente formado por um conjunto específico de instruções, utilizadas para analisar dados e automatizar decisões. As pessoas frequentemente relacionam algoritmos à uma receita. Porém, hoje em dia, as pessoas tendem a usar o termo "algoritmo" como uma conotação geral de um processo pela qual os computadores tomam decisões e realizam previsões de forma automatizada sobre um conjunto de dados (Brayne, 2021, p. 13, tradução nossa).

Referências bibliográficas

ANDREATTA, S. M.; SABARIEGO, J. Anonimato: resistência tecnopolítica na rede. *Revista Quaestio Iuris*, v. 17, n. 2, p. 166-190, 2024.

ASSANGE, J *et al*. *Cypherpunks: liberdade e o futuro da internet*. Tradução: Cristina Yamagami. São Paulo: Boitempo, 2013.

AZAMBUJA, C. C. Tecnoliberdade: poder e política na era da Inteligência Artificial. *Ethic@ - An international Journal for Moral Philosophy*, v. 22, n. 2, p. 514-541, 2023.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Diário Oficial da União, Brasília, DF, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 11 dez. 2023.

BRASIL. *Lei nº 13.444, de 11 de maio de 2017*. Dispõe sobre a Identificação Civil Nacional (ICN). Diário Oficial da União, Brasília, DF, 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. Acesso em: 11 dez. 2023.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 dez. 2023.

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União, Brasília, DF, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 11 dez. 2023.

BRAYNE, S. *Predict and surveil: data, discretion, and the future of policing*. New York, NY: Oxford University Press, 2021.

BRUNTON, F.; NISSENBAUM, H. Vernacular resistance to data collection and analysis: a political theory of obfuscation. *First Monday*, [S. l.], v. 16, n. 5, 2011. DOI: 10.5210/fm.v16i5.3493. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/3493. Acesso em: 11 dec. 2023.

BRUNTON, F.; NISSENBAUM, H. *Obfuscation: a user's guide for privacy and protest*. Cambridge: The MIT Press. 2015.

BRUZZONE, A. *Ciberpopulismo: política e democracia no mundo digital*. São Paulo: Contexto, 2021.

BUZANELLO, J. C. Direito de resistência. *Sequência Estudos Jurídicos e Políticos*, v. 22, n. 42, p. 9–28, 2001. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/15391. Acesso em: 11 dez. 2023.

CESARINO, L. *O mundo do avesso: verdade e política na era digital*. São Paulo: Ubu, 2022.

CHIGNOLA, S. *Foucault além de Foucault: uma política da filosofia*. Porto Alegre: Criação Humana, 2020.

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

DEIVISON, F. *Colonialismo digital: por uma crítica hacker-fanoniana*. São Paulo: Boitempo, 2023.

DIAS, F. V. *Criminologia midiática e tecnopolítica*. São Paulo: Tirant lo Blach, 2022.

FISHER, M. *A máquina do caos: como as redes sociais reprogramaram nossa mente e nosso mundo*. São Paulo: Todavia, 2023.

FOUCAULT, M. *Ética, sexualidade, política*. Ditos e Escritos V. Org. Manoel Barros da Motta. Rio de Janeiro: Forense Universitária, 2006.

FOUCAULT, M. *História da sexualidade 1: vontade de saber*. 16 ed. São Paulo: Paz e Terra, 2023.

FOUCAULT, M. *Vigiar e punir: nascimento da prisão*. 42 ed. Petrópolis/RJ: Vozes, 2014.

GROS, F. *Desobedecer*. São Paulo: Ubu, 2018.

HAN, B. *Infocracia: digitalização e a crise da democracia*. Petrópolis, RJ: Vozes, 2022.

HOWE, D. C. Surveillance countermeasures: expressive privacy via obfuscation. IN: ANDERSEN, Christian; COX, Geoff. A peer-reviewed journal about: datafied research. *Digital Aesthetics Research Centre*, Aarhus University. v. 4, n. 1, 2015.

KRAMER, A. D. I.; GUILLORY, J. E.; HANCOCK, J. T. Experimental evidence of massive-scale emotional contagion through social networks. Washington, DC: *Proceedings of the National Academy of Sciences of the United States of America*, v. 111, n. 24, p. 8788-8790. 2014.

LAMA, J. P.; SANCHEZ-LAULHE, J. Consideraciones a favor de un uso más amplio del término tecnopolíticas: sobre la necesidad de la crítica y las políticas del conocimiento y las tecnologías. In: SABARIEGO, J.; AMARAL, A. J.; SALLES, E. B. C. *Algoritarismos*. São Paulo: Tirant lo Blach, 2020.

LOUREIRO, M. F. B.; CARNEIRO, J. V. V. Problematizando o direito à privacidade e à proteção de dados pessoais em face da vigilância biométrica. *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, v. 17, n. 2, p. 205-213, 2020.

LOVELUCK, B. *Redes, liberdades e controle: uma genealogia política da internet*. Petrópolis: Vozes, 2018.

MOROZOV, E. *To save everything, click here: the folly of technological solutionism*. New York: PublicAffair, 2013.

MOROZOV, E. *Big Tech: a ascensão dos dados e a morte da política*. Traduzido por Claudio Marcondes. São Paulo: Ubu Editora, 2018.

MOROZOV, E.; BRIA, F. *A cidade inteligente: tecnologias urbanas e democracia*. São Paulo: Ubu, 2019.

NAVARRO, F. S. Ofuscación: tácticas de resistencia frente al capitalismo de vigilancia. *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, v. 20, n. 1, p. 125–131, 12 ene, 2023.

NEMER, D. *Tecnologia do oprimido: desigualdade e o mundano digital nas favelas do Brasil*. Vitória: Milfontes, 2021.

O'NEIL, C. *Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça à democracia*. Santo André, SP: Rua do Sabão, 2020.

SRNICEK, N. *Platform capitalism*. Cambridge, UK; Malden, MA: Polity Press, 2017.

VÉLIZ, C. *Privacy is power*. Great Britain: Penguin Random House, 2020.

ZITTRAIN, J. *Facebook could decide an election without anyone ever finding out: the scary future of digital gerrymandering and how to prevent it*. Washington, DC: The New Republic. 2014.

ZUBOFF, S. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder*. New York: PublicAffair, 2021.

Recebido/*Received*: 05/01/2024
Aprovado/*Approved*: 21/06/2025
Publicado/*Published*: 18/07/2025