DOI: 10.1590/s0103-4014.2024.38110.004

Silenciamento sociotécnico e os limites do "poder instrumental"

Alcides Eduardo dos Reis Peron [I]
Anderson Röhe [II]

Introdução

Nos dias de hoje, a vigilância de dados tem se tornado uma das principais características das atividades governamentais, e se manifesta não somente em vigiar os indivíduos em outra escala (hipervigilância), mas como uma interação sociotécnica envolvendo classificação de risco e dispositivos preditivos. Esses sistemas direcionam esforços para a predição do crime e gestão de riscos, ao invés de promover atritos e confrontos desnecessários. Tais argumentos vão ao encontro da proposta atual de Shoshana Zuboff (2019), para quem as tecnologias de "datavigilância" possibilitam uma forma de poder não violenta focada em moldar comportamentos e decisões dos indivíduos. Diante disso, casos como a experiência atual da Polícia Metropolitana de Londres na implantação da Matriz de Violência de Gangues (GVM), usada para identificar e traçar o perfil das supostamente nominadas "gangues", tornam-se tanto o escopo deste artigo, quanto revelam uma realidade bem mais complexa.

Valendo-se das noções de violência simbólica e analisando os resultados duvidosos da implantação da GVM, este artigo explora, como método, os limites da ideia de poder instrumental. O objetivo é descrever como a violência é realizada por meio de um conjunto de práticas amplamente digitalizadas e como essas interações techno-mediadas pela tecnologia em fazer segurança interagem com os padrões locais de discriminação. E tem como referência, estudo de autores como David Lyon, Bruno Latour, dentre outros.

A hipervigilância (Zmoginski, 2019) – também conhecida como vigilância de dados – tornou-se uma questão de governar o cotidiano da população por meio de seus dados e informações pessoais, sustentando a estabilidade dos fluxos na cidade, atuando especialmente sobre desvios e distúrbios. Em especial em uma era pós-pandemia, dado o crescimento da vigilância sanitária. Ericsson e Haggerty (2002) sustentam que o policiamento se organiza como um polo de produção e comunicação de riscos, gerenciando outras instituições que passaram a ser incumbidas dessa mesma finalidade. A supervisão permanente da ordem cotidiana e do bem-estar dos cidadãos tornou-se o principal tom das práticas de segurança atuais (Dillon, 2004; Duffield, 2007). Nesse sentido, os departamentos de polícia estão investindo em tecnologias de vigilância, sistemas de gerenciamento de dados como resultado, sistemas preditivos e aplicações de

avaliação de risco. Especialmente câmeras inteligentes que cada vez mais fazem parte do arsenal policial. Nesse processo, tanto os sistemas de CFTV quanto as novas formas de monitoramento e sensoriamento de dados algorítmicos tornaram-se estratégias centrais para gerenciar riscos e identificar desvios.

Então, a vigilância pode ser empregada para diferentes propósitos: para deter a atividade criminosa,[1] a fim de produzir provas para fins investigativos e, ao se tornar onipresente, estabelece uma relação desequilibrada de poder. O primeiro a enquadrar a vigilância como uma tecnologia de poder foi Michel Foucault (1995). Em sua análise das instituições disciplinares, ele discute como a emergência de um regime escópico (e uma série de práticas disciplinares) obliterou a necessidade de registrar a violência sobre o corpo como ferramenta punitiva, ao invés de coerção moduladora. Enquanto a agressão física não é o principal eixo de normalização, a sociedade disciplinar é um ecossistema povoado de micro punições – sanções, penas, isolamentos, reprimendas – e uma atmosfera de ameaça iminente, que orquestra o funcionamento dos corpos, coagindo os indivíduos a se comportarem da forma desejada.

Embora os expoentes dos Estudos de Vigilância contemporâneos já tenham alertado como as práticas de vigilância podem assumir características violentas e discriminatórias (Lyon, 1994), análises recentes sobre o tecnicismo digital sustentam que a vigilância de dados articula uma forma de controle "inteligente", suave e não violenta (Zuboff, 2019). Particularmente, Zuboff parece convencida de que a vigilância possibilita formas de poder racionalizadas e brandas, nas quais o controle se estabelece sem recorrer à violência.

Práticas de perfilamento racial e avaliação de risco de determinados grupos, e a implantação de sistemas de reconhecimento facial tendenciosos nos Estados Unidos (Garvie et al., 2016), revelam, no entanto, como as técnicas de vigilância podem assumir formas nocivas e reproduzir a violência. Além disso, um olhar mais atento para as experiências de Londres na implantação de ferramentas preditivas de avaliação de risco, como a Gang Violence Matrix (GVM), revela como as práticas de criação de perfis algorítmicos podem incorporar viés discriminatório, perpetuando-o silenciosamente. Essa é uma ferramenta desenvolvida pela Polícia Metropolitana de Londres (MET) para traçar perfis das supostas nominadas gangues e prever comportamentos violentos coletando dados de várias fontes e atribuindo pontuações de "risco" aos indivíduos.

O conjunto de sistemas algorítmicos analisados por Zuboff, de fato, difere em vários aspectos do sistema GVM. No entanto, ambos se baseiam na captura e processamento de dados algorítmicos, visando, em última instância, interferir na vontade dos indivíduos, induzindo-os a consumir, ou regular seu comportamento por meio de ações policiais preventivas. Além disso, é incongruente supor que os sistemas que compõem o poder instrumental estão limitados ao âmbito comercial, e não se ramificam em sistemas de gestão e governança de segurança. Assim como Latour (1994), os autores deste artigo consideram que

as tecnologias não possuem uma ontologia fixa; seus significados, usos e conexões não se limitam a um fim predeterminado, mudando à medida que circulam e se estabelecem em outros contextos e hierarquias sociais. As multiplicidades de aparatos de coleta, processamento e modulação se espalham por diversos setores, tornando-se parte de um complexo aparato de governo de segurança. Como lembra Crawford (2021), os interesses das Big Techs e do Estado muitas vezes se cruzam, rompendo a linha divisória – se é que houve alguma – entre os sistemas comercial, social e policial.

Dessa forma, valendo-se das noções de violência simbólica, no que se descreve aqui como "silenciamento sociotécnico", e analisando os resultados dúbios da implantação do GVM em Londres, este artigo explora os limites da ideia de poder "instrumental". Assim, há uma abordagem multidisciplinar, que vai desde os Estudos de Vigilância à Ciência, Tecnologia e Sociedade (STS), para debater como a violência é realizada por meio de um conjunto de práticas amplamente digitalizadas (também conhecido como hipervigilância), e como esse fazer segurança tecnomediada, apesar da autoimagem de inocuidade e precisão, interage com os padrões locais de discriminação. Argumenta-se neste artigo que, por operarem à margem da percepção do sujeito, esses agenciamentos constituem um tecno silenciamento da violência – o que contribui para uma reprodução despercebida, porém nociva, das injustiças.

Nesse sentido, a primeira seção discute a transição entre vigilância (clássica) e vigilância de dados no contexto de aprimoramento do Big Data, apoiando-se especificamente nos argumentos sobre o poder inteligente e instrumental descritos na obra de Zuboff. Embora a autora não tenha abordado os sistemas policiais, sua tese sobre o poder não violento dos algoritmos pode ser questionada quando a transpomos para o espectro de segurança de vários países, dos Estados Unidos à China, independentemente de seus sistemas de governo. Portanto, a maneira como aquela autora qualifica essa forma de poder como não violenta, ao descrevê-la como invisível e supostamente imperceptível. Na seção seguinte, o poder instrumental é contrastado com a noção de violência simbólica, possibilitando uma crítica que coloca a invisibilidade da vigilância não como justificativa de sua brandura, mas como característica central para a promoção da violência. A ideia não é trazer informações novas e inovadoras sobre a Gang Matrix, mas usá-la como um estudo de caso que revela os contornos violentos do capitalismo de vigilância.

Os limites do poder instrumental

Em sua análise sobre poder, Michel Foucault (1995) descreve as técnicas e os dispositivos mobilizados por diferentes instituições para a administração dos indivíduos em seus ambientes. Fábricas, presídios, hospitais e instituições de ensino comporiam um conjunto de instituições disciplinares que exercem uma forma de poder descentralizado sobre os indivíduos e seus corpos, regidos por normas preestabelecidas, intensamente fiscalizadas e examinadas. O "poder

disciplinar" seria produtivo, como menciona Foucault (1995), visando apenas extrair o máximo de utilidade dos corpos, e para isso depende de sua vigilância permanente para produzir conhecimento, e estabelecer uma situação em que a certeza ou a incerteza da fiscalização produz um efeito de docilidade sobre os indivíduos. Isso não significa que Foucault considerasse esse modelo menos violento. Em sua perspectiva, o modelo panóptico "extrai" essa cooperação do corpo ao acomodar e normalizar uma multiplicidade de microagressões visíveis e coerção psicológica – uma forma de violência muito mais dispersa e indireta.

O modelo panóptico disciplinar, no entanto, é apenas uma expressão das formas de vigilância, e como aponta Deleuze (2017), é um modelo fechado circunscrito em instituições em crise atual, e talvez não represente as novas formas de vigilância e monitoramento que estavam por vir. Nesse sentido, Haggerty (2006) e Bigo (2006) apontaram para a insuficiência do modelo panóptico para explicar as práticas contemporâneas de vigilância, especialmente por ser estático, visível, limitado e não enquadrar como as tecnologias digitais e as câmeras inteligentes produzem novas formas de subjetivação que vão além da disciplinaridade. Em geral, a vigilância é descrita como a coleta, classificação e seleção sistemática de informações sobre indivíduos e contingentes populacionais para produzir ajustes comportamentais (Dandeker, 1990; Lyon, 1994; Wood, 2013).

David Lyon (2003), analisando as ramificações dos sistemas de coleta massiva de dados, e como eles se entrelaçam como prática cotidiana, mobilizada por diferentes agentes, descreve a vigilância como uma prática de "classificação social". O autor considera que a vigilância é, acima de tudo, uma técnica de manipulação de dados abstratos para a produção de perfis e classificação de riscos em um sistema líquido e em rede, com o objetivo de planejar, prever e prevenir (Lyon, 2003, p.13). E essa prática de triagem de vigilância é exercida não apenas por agentes que nos são estranhos e alheios ao nosso cotidiano, mas por nós mesmos. A vigilância é, portanto, uma atividade em que nos envolvemos em diversos contextos, seja para garantir segurança, ou comodidade, seja como uma possibilidade de lazer oferecida por aplicativos e redes sociais.

Os avanços tecnológicos nos campos informacional e comunicacional tornaram-se uma característica central no capitalismo contemporâneo e na gestão da segurança pública. Nesse sentido, "vigilância de dados" refere-se ao monitoramento sistemático de pessoas ou grupos de pessoas por meio de sistemas de dados pessoais, no intuito de regular ou governar seus comportamentos (Esposito, 2014). É muito mais onipresente e liberta as práticas de monitoramento do olhar humano – daí a expressão hipervigilância (Zmoginski, 2019) – que produz sugestões aos usuários, que vão desde uma compra online baseada em seu estado emocional até estratégias de abordagem policial em determinadas áreas onde crimes podem ocorrer (Lyon, 2003).

A miríade de dispositivos conectados, coletando e monitorando dados é tão complexa e difusa que só pode ser entendida como um conjunto de vigi-

lância (Haggerty; Ericsson, 2000). As montagens são marcadas por uma coleta difusa de diversos dados de diferentes sistemas e métodos, tais como câmeras, celulares e sensores biométricos, que posteriormente são coletados para perfis de produção e classificações de risco. Assim, a vigilância contemporânea não se exerce a partir de um núcleo central, ou de uma única forma, mas a partir de um conjunto de instrumentos que se conectam horizontalmente (ibidem, p.614).

Nesse contexto, Shoshana Zuboff defende o surgimento de um "capitalismo de vigilância" que não apenas extraia valor da comercialização de dados. Com base nessa forma de acumulação, ela define como um "poder instrumental", no qual conhecimentos estatísticos e preditivos coletados de indivíduos são mobilizados por grandes empresas de tecnologia para governar a tomada de decisões desses mesmos sujeitos. Baseia-se na autoautorização dos usuários, introduzindo uma compensação entre privacidade, previsibilidade e gerenciamento de riscos. Consequentemente, seria capaz de persuadir os indivíduos sem qualquer forma de violência (Zuboff, 2019, p.381).

A rigor, esse poder instrumental é capaz de modular desejos e racionalidades em larga escala, por meio de dispositivos, aplicativos e redes de coleta de dados (ibidem, p.396-7). O instrumentarismo reflete as características de sistemas algorítmicos preditivos e de perfilamento, capazes de "interpretar" um conjunto de dados e induzir comportamentos e sugestões às pessoas, sem recorrer a meios violentos.

De certa forma, Zuboff confunde a ausência de violência com a invisibilidade da violência – o que ela reconhece como condição para permitir que esse aparato intrusivo induza, silenciosamente, decisões e comportamentos. Assim, este artigo argumenta que a "suavidade" a qual Zuboff se refere para descrever essa forma de poder é apenas um efeito da alienação em relação à intromissão do processo de vigilância. O poder instrumental pode ser particularmente violento (por meios tanto diretos quanto indiretos) em aplicações securitárias. Nesse sentido, a violência não desaparece com o poder instrumental, mas apenas a sensação de ser agredido – privando os indivíduos dos efeitos, ou percepção da violência.

Embora Zuboff (2019) tenha se concentrado em discutir como as Big Techs monetizam dados e modulam escolhas individuais com base em redes sociais e aplicativos, essas técnicas têm sido notoriamente empregadas em outros campos, para diferentes finalidades, como o setor de segurança. Patrulhamento digital em mídias sociais, extração de dados de redes, processamento de dados de múltiplas-ordens, criação de perfis, fomento à análise preditiva de dados e classificação de risco são algumas das técnicas das Big Techs emuladas e apropriadas por empresas e forças de segurança. Por um lado, há um número crescente de projetos de cooperação entre empresas de dados e agências de segurança e inteligência, como apontam Bauman et al. (2015). Por outro lado, existem inúmeros projetos desenvolvidos entre Big Techs e empresas de dados e forças de segurança, como destacado por Crawford (2021), como a Palantir (que é

essencialmente uma empresa de dados), ao apoiar forças policiais nos Estados Unidos; e assim como o Project Maven, em que o Google e o Departamento de Defesa dos Estados Unidos cooperariam com a troca de dados para aplicação em iniciativas militares.

Nesse sentido, por mais que a Gang Matrix seja um empreendimento público-privado, não associado diretamente às Big Techs, sua lógica operacional é muito semelhante à dinâmica instrumentista de Zuboff, no sentido de coletar dados para perfilar indivíduos e modular seus comportamentos – uma prática que reproduz tanto a violência simbólica quanto a direta. Acima de tudo, como outras grandes empresas de tecnologia, a Gang Matrix visa a previsibilidade, a antecipação e a gestão de riscos, construindo uma atmosfera de governança branda do crime que ofusca práticas violentas profundas. Então, para que a perspectiva de Zuboff sobre a não letalidade do capitalismo de vigilância se sustente, a autora acaba subestimando ou ignorando esse conjunto de amplas relações do capitalismo de vigilância.

Violência simbólica e Silenciamento sociotécnico

Os estudos da violência são necessariamente multidisciplinares, no sentido de que podem se manifestar de múltiplas formas, seja física, psicológica, seja simbolicamente. Para Crettiez (2011, p.15-17), a violência se manifesta direta e indiretamente. A violência direta é um ato de coerção dolorosamente vivenciado, obrigando alguém a agir contra sua vontade. Nesse caso, manifesta-se como um exercício passional e contingente; como o uso racional do Estado por meio das forças de segurança, ou mesmo por outros grupos que, estrategicamente, desdobram a violência; e, finalmente, pode ser uma expressão identitária, afirmando vínculos entre os praticantes, ou negando-os a quem os sofre.

Por outro lado, Pierre Bourdieu (2011) – em sua análise dos sistemas simbólicos de poder, expressos através da arte, religião e linguagem – abordou uma forma de violência indireta. Em sua perspectiva, a violência simbólica é mediada por diversas instituições estatais e está no centro da produção de hierarquias no mundo social contemporâneo. Ele a definiu como instrumentos estruturados e estruturantes de comunicação e conhecimento em que "sistemas simbólicos" funcionam como instrumentos de imposição e legitimação da dominação de uma classe sobre outra (Bourdieu, 2011, p.7). Em sua abordagem, a violência é articulada em termos de dominação consentida e internalizada nos hábitos desses subordinados, moldando comportamentos e entendimentos (estruturas estruturadas) que fundamentam sua docilidade.

Bourdieu entende que essa forma de violência produz desconexões ou rupturas identitárias e históricas, assim como impõe ritmos e formas de comportamento que esmagam subjetividades e levam os grupos a naturalizar uma vida de subjugação (Bourdieu, 2011). A violência simbólica está inserida em produções culturais, discursos, costumes e práticas que normalizam a agressão, a exclusão social, a marginalização, "estruturas de hábitos de maneiras que aca-

bam contribuindo para a reprodução da exclusão social, hierarquia e violência simbólica" (Schubert, 2018, p.251).

Han (2017), explorando as proposições de Bourdieu, busca destacar a questão principal dentro das formas indiretas e simbólicas de violência. Ele observa que, em geral, aqueles que debatem a violência indireta traçam suas perspectivas unindo poder e violência, o que significa que o simbolismo da violência seria resultado de uma tentativa socio hierárquica de dominação (Han, 2017, p.161). Assim como acredita que a invisibilidade dessas técnicas favorece sua perpetuação (ibidem, p.162-9).

Nesse sentido, nas obras de Bruno Latour (1994) fica claro como a construção de dispositivos sociotécnicos emaranha um processo de ocultação das relações de poder. Eles compõem silenciosamente o tecido social, modulando condutas e programas de ação, mas também foram moldados por essas interações em uma "teia sem costura". Latour entende que a invisibilidade dessa interação sociotécnica e o esfriamento das disputas sociais inerentes ao desenvolvimento e atuação das tecnologias resultam de um processo que ele chama de "caixa-preta" (Latour, 1994).

Em essência, a caixa-preta é responsável pelo desaparecimento das infraestruturas, pela opacidade dos algoritmos, pela cobertura de disputas sociais e decisões cruciais para o desenvolvimento de dispositivos técnicos, perpetuando essa agência despercebida dos "não humanos". Portanto, é uma forma de produzir invisibilidades dentro dos processos sociotécnicos, significando que práticas e decisões nocivas, omissões, negações e valores embutidos nas decisões e escolhas sobre o desenvolvimento de um dispositivo e seus usos, podem ser silenciados, borrados, tornados opacos por meio de processo técnico.

No campo da vigilância de dados, isso significa que os algoritmos desenvolvidos para avaliar riscos, prever, identificar alvos ou perfis também são dispositivos de caixa preta, intencionalmente tornados opacos para silenciar seu entrelaçamento sociotécnico. Enquanto O'Neil (2016) sustenta que o algoritmo não seria apenas opaco para "sumos sacerdotes", matemáticos e cientistas da computação, Brayne (2021) argumenta que algoritmos preditivos são opacos e ininteligíveis até mesmo para seus usuários – como os policiais que progressivamente são submetidos a sugestões automatizadas realizadas por sistemas preditivos que ignoram sua experiência e as separam dos processos decisórios.

Tanto Scannel (2016) quanto Brayne (2021) concordam que algoritmos são elementos moldados pelos mundos sociais em que foram criados, e pessoas situadas em contextos sociais, organizacionais e institucionais preexistentes decidem quais dados serão coletados e analisados, sobre quem e com que finalidade, afetando assim o desempenho dos sistemas. Isso reverbera no que Ruha Benjamin (2019) escreve sobre a branquitude na era digital, destacando a fragilidade das discussões sobre "robôs racistas", pois desloca a análise sobre onde o racismo de fato estaria localizado: nas negações, ausências e silenciamento manifesto

durante os processos de tomada de decisão e desenvolvimento de algoritmos e aplicações.

A agência e os efeitos sociais dos sistemas algorítmicos são muitas vezes negligenciados para reproduzir a violência simbólica devido à sua "invisibilidade" dentro do tecido social. É um duplo silenciamento, primeiramente manifestado na aparência de neutralidade dos algoritmos, em que a "lavagem técnica" apaga suas interações humanas; e, em segundo lugar, um silenciamento que obscurece os critérios pelos quais os indivíduos são perfilados e enquadrados como suspeitos, deslocando práticas discriminatórias e nocivas ao longo de uma ampla e amorfa infraestrutura de vigilância.

Risco e violência preditiva

Há um consenso crescente sobre como os sistemas de vigilância de dados podem intensificar a reprodução de preconceitos, discriminação e segregação em aplicações policiais (Ferguson, 2017; Benjamin, 2019; Brayne, 2021; Crawford, 2021). Por exemplo, sistemas de policiamento preditivo e inferências algorítmicas sobre risco podem ser responsáveis por dotar como prejudiciais as práticas de policiamento.

A busca pela predição remonta ao contexto norte-americano de combate ao crime e deriva das práticas policiais (desde as táticas reativas às preventivas e "proativas") entre as décadas de 1980 e 1990, especialmente em Nova York. Influenciadas por modelos de criminologia ambiental, as forças policiais passaram tanto a introduzir sistemas de vigilância e monitoramento, como câmeras e o Compstat (para monitorar e classificar dados geolocalizados sobre crimes e ocorrências), quanto adotar técnicas de gestão de segurança – tais como a política de Tolerância Zero em Nova York – como técnicas de endurecimento criminal e aplicação da lei. Anos depois, sistemas como *PredPol* implantados pela Polícia de Los Angeles estão reformulando as práticas policiais para predição, criação de perfis e gerenciamento de risco.

As tecnologias preditivas tornaram-se imensamente populares nos Estados Unidos e, no restante do mundo, com a eclosão da "guerra global ao terror", caracterizada pela constante desdiferenciação entre crime e terrorismo que acaba justificando o uso de sistemas de vigilância altamente intrusivos (Bigo, 2001). Além disso, uma lógica mais perversa ganhou expressão no período, e informa esse *ethos*: o surgimento do "direito penal do inimigo". Trata-se de um conjunto de princípios que permitem ao indivíduo ser privado de suas garantias e direitos, para os quais não se aplicam regras punitivas (baseadas em fatos passados ou atos cometidos). Em vez disso, tem um viés prospectivo, no qual os riscos, ou potenciais ações futuras, são determinantes para sancionar um indivíduo antecipadamente (Jakobs; Meliá, 2012. Isso implica que os indivíduos podem ser julgados não apenas com base em um "perigo fático" (relativo ao ato cometido), deslocando a factualidade do ilícito, mas também de acordo com a periculosidade de sua personalidade.

Nesse contexto, as "predições" produzidas pelos sistemas de vigilância de dados assumem o *status* de verdade, convertendo padrões de relacionamento e dados desagregados em um risco potencial, suficiente para fazer emergir um "inimigo" que legitima sanções antecipatórias.

Aprofundando essa discussão, Amoore (2013) entende que o cálculo do risco infere um espectro de "futuros possíveis" com base em múltiplos elementos de dados do passado. Assim, os modelos de cálculo de risco preditivo permitem "agir com base no que não se sabe" (Amoore, 2013, p.57). Isso significa que o desconhecido e o incerto se tornam "certo" por meio de tecnologias de avaliação preditiva de risco, informando as estratégias presentes: baseado, assim, na incerteza" (ibidem, p.58).

Os sistemas preditivos, sejam baseados em estatísticas, sejam em perfilamento e classificação de risco, antecipam a culpa de seus alvos, criminalizando formas de vida e construção de identidade. Esses sistemas privam de inocência os indivíduos, ao julgar uma hipótese de periculosidade e suspeita codificada por sistemas algorítmicos. Nesse sentido, os sistemas preditivos viabilizam formas autoritárias de policiamento, mesmo que não sejam identificados vieses, antecipando culpas e possibilitando sanções baseadas em um "verniz técnico". Assim, os sistemas preditivos tendem a reforçar os processos discriminatórios e enfraquecer a relação entre polícia e sociedade (Lipton, 2019). Ademais, ao avaliar crimes futuros, a "predição" pode ser responsável por produzir crimes ou inimigos, em vez de preveni-los (Benjamin, 2019).

Ferguson (2017) explora a implantação de sistemas preditivos de classificação de risco (segmentação preditiva baseada em pessoas) em várias cidades dos Estados Unidos. Esses sistemas de vigilância de classificação social cruzam vários tipos de dados, antecedentes criminais ou conjuntos de dados de redes sociais, ao elaborar uma "lista de calor" sobre potenciais vítimas e suspeitos com risco de violência. Esses sistemas perfilam e atribuem uma pontuação aos indivíduos e fornecem uma justificativa para que os policiais visitem suspeitos (e indivíduos relacionados a eles), emitam advertências e, eventualmente, os processem. O autor observa que tem havido muitas controvérsias relacionadas à coleta de dados de redes sociais, ao fazer predições e atribuir pontuações de risco aos indivíduos. Há casos em que ações passadas de indivíduos e relacionamentos despercebidos são trazidos à tona para assombrar os perfilados – fazendo emergir um inimigo culpável. Consequentemente, as decisões moldadas por sistemas de classificação de risco podem ser injustas, atualizando permanentemente formas simbólicas de violência, como a discriminação.

Tanto sistemas de classificação de risco quanto sistemas preditivos compreendem novas infraestruturas de vigilância e monitoramento policial que articulam formas inconscientes e invisíveis de subjugação. Seus algoritmos opacos – geralmente treinados e fornecidos pelas redes sociais – reduzem os indivíduos a perfis, que se cruzam com categorias preconcebidas de suspeição, justificando policiamento, abordagens e humilhações desproporcionais.

Matriz da violência das gangues e a punição de estilos de vida e identidades

A discussão sobre gangues sempre esteve presente no imaginário social das classes médias britânicas. Nas décadas de 1970 e 1980, o termo gangue era usado para se referir a grupos ligados a movimentos anarquistas, punks e skinheads que dominavam a cena da contracultura britânica, e geralmente era um conceito sociológico que buscava descrevê-los como um fenômeno específico. No entanto, no final da década de 1990, com o crescimento das comunidades asiáticas e norte-africanas que vivem na cidade – as chamadas Black, Mixed, Asian, and other Minority Etnic (Bame) –, o conceito de "gangue" parece ter mudado. As gangues deixaram de ser descritas como um fenômeno sociológico específico, mas como um conceito policial usado para se referir às comunidades Bame formadas em torno da periferia, que se tornaram alvo de um processo de criminalização (Williams; Clarke, 2018).

Nesse contexto, as gangues integram o conjunto de pânicos morais[2] no Reino Unido, fazendo emergir um "outro" que precisa ser regulado, governado e sancionado pelo aparato de segurança policial (Williams; Clarke 2018). Essa alterização é uma forma de conectar códigos morais de inferioridade e diferença aos grupos Bame, promovendo a discriminação racial (ibidem). O termo potencializa uma "criminologia do outro" racializada – concentrada na demonização do criminoso, produzindo medo e apoiando a punição de determinados grupos.

É somente em 2011, em razão dos tumultos em Londres, que começaram com o assassinato de Mark Duggan, um negro de 29 anos no bairro de Tottenham, que as autoridades começaram a apoiar o argumento de que a violência urbana estaria relacionada ao surgimento de gangues pervertendo a ordem social, algo que exigiria formas mais incisivas de controle e administração policial. No auge dessa crise, o prefeito de Londres Boris Johnson também retratou os tumultos como um fenômeno de gangues (Amnesty Internatonal, 2018, p.5).

Em 2012, o MET começa a aplicar uma tecnologia de monitoramento e controle chamada Matriz de Violência de Gangues. Na época, essa ferramenta era retratada como um software preditivo, capaz de identificar quais membros de gangues teriam maior probabilidade de cometer crimes violentos (Kelion, 2014).

Em suma, o MET o define como "uma ferramenta de inteligência que usamos para identificar e avaliar o risco de membros de gangues em Londres que estão envolvidos em violência de gangues", que também seria capaz de identificar os sujeitos de gangues mais violentos; ou seja, aqueles que correm o risco de fazer vítimas, e assim sugere métodos de intervenção (The Metropolitan Police, 2020). O sistema emprega algoritmos opacos para prever comportamentos e antecipar culpas, com base em sua interação nas redes sociais – vídeos que esses indivíduos "curtiram" e compartilharam, padrões de conexões e chats, interesses registrados nos aplicativos – antecedentes criminais[3] e múltiplas fontes de inteligência.

O uso dessa tecnologia, no entanto, pode ser muito mais difundido do

que o descrito, produzindo danos irreparáveis aos "presos" no GVM, seja porque a polícia os aborda com muito mais frequência, seja porque terceiros têm acesso a essas informações e dificultam sua movimentação em outros espaços sociais – como acesso à educação, emprego ou crédito bancário (Amnesty Internatonal, 2018; Williams, 2019).

Há também evidências de que o MET compartilha os dados da Matriz com outras agências, como as de educação, saúde e emprego (Amnesty Internatonal, 2018, p.21-2). Construindo, assim, cercas em torno do indivíduo que está preso no sistema, o que pode reforçar o *status* marginalizado do indivíduo. Todas essas abordagens e restrições não só constrangem a vida dos "nominais" – que não têm plena consciência dos aparatos que roubam sua liberdade – como também contribuem para a produção de traumas e estigmas, fazendo com que desenvolvam desconfiança na polícia (Williams, 2019).

Embora as autoridades afirmem que o GVM é adequado e proporcional, o policiamento dos estilos de vida, a ruptura das relações identitárias e a antecipação da culpa pela pontuação de risco – sem vínculos com ilegalidades – configuram uma atrocidade punitiva que desperta a lógica de uma "lei do inimigo". O risco, nesse sentido, é mais uma antecipação da culpa do que um dispositivo de "predição». Cria-se, assim, um precedente que autoriza o exercício sistemático da violência contra os estilos de vida, obrigando os indivíduos a despojarem-se de sua subjetividade em favor de um comportamento "adequado".

Conclusões

Este artigo buscou demonstrar como a lógica do capitalismo de vigilância, marcada pela coleta e tratamento de dados, pela modulação do comportamento dos indivíduos e pela busca de previsibilidade, se espalha para as práticas de segurança e reproduz formas de violência que escalam em direção a um Estado autoritário. Motivado por essa crítica, analisou como os aparatos de classificação e monitoramento de risco podem reforçar e subsidiar práticas violentas. Por mais "inteligente" e ubíqua que seja a vigilância de dados, ao contrário do que afirma Zuboff, aquela pode intensificar processos de exclusão e normalizar exercícios de força discricionários e desproporcionais.

O artigo sugere que os ruídos gerados pelas formas simbólicas de violência estão se tornando cada vez mais silenciados graças aos sistemas algorítmicos de classificação de risco. Ao enquadrar essas ferramentas como parte de um aparato de violência discreta, ao invés de aceitar a ideia de que o poder instrumental é uma forma de poder superior e cândido, este artigo sugere que a violência, a discriminação e a opressão são ocultadas e naturalizadas dentro da infraestrutura de vigilância capitalismo.

A GVM é um exemplo perfeito de como opera o silenciamento sociotécnico da violência, uma vez que, não advertido, sujeita os indivíduos Bame a constrangimentos. Seus resultados são a geração de mais insegurança na forma de violência simbólica, criminalizando identidades e modos de vida de grupos

vulneráveis. O aparecimento de regularidade nesses processos é, portanto, o efeito perseguido por esse silenciamento sociotécnico que, longe de eliminar a violência, a torna intrínseca a uma tecnicidade, e opaca a abordagens que ignoram a arquitetura sociotécnica do poder.

Notas

1 Apesar de extensos estudos retratarem essa prática como ferramenta ineficaz para essas tarefas, incluindo a violência policial (Piza et al., 2019).

2 Na definição de Stanley Cohen (1987), o pânico moral é um fenômeno recorrente em que as sociedades, por uma condição ou episódio, classificam uma pessoa ou um grupo como uma ameaça aos valores e interesses sociais. Esse assunto é estereotipado pela mídia e outros atores, construindo barreiras morais ao seu redor. Esses episódios produzem comoção social e auxiliam na composição de argumentos que justificam a restrição de direitos e liberdades de determinados grupos e a ampliação das técnicas policiais para o gerenciamento dos riscos a ela associados.

3 Os bancos de dados incluem o Crime Information Report System, o software de custódia NSPIS, o Crimint and Merlin, o Emerald Warrant Management System e os dados do Youth Justice Board (Allain, s.d.)

Referências

ALLAIN, D. *Trident Gang Command*. (Slide Presentation) Metropolitan Police: Total Policing. S.d.

AMOORE, L. *The Politics of Possibility*: Risk and Security Beyond Probability. Durham, UK: Duke University Press, 2013.

AMNESTY INTERNATIONAL. *Trapped in the Matrix: Secrecy, Stigma, and bias in the MET's Gangs Database*. 2018. Disponível em: <https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnest y%20report.pdf>. Acesso em: 23 set. 2021.

BAUMAN, Z. et al. Após Snowden: repensando o impacto da vigilância. *Revista Eco-Pós*, v.18, n.2, p.8-5, 2015.

BENJAMIN, R. *Race after technology*: Abolicionist Tools for the New Jim Code. Cambridge, UK: Polity, 2019.

BIGO, D. Internal and External Security(es): The Möbius Ribbon. In: ALBERT, M.; JACOBSON, D.; LAPID, Y. (Ed.) *Identities, Borders, Orders*. Minneapolis: University of Minnesota Press, 2001. p.91-116.

_____. Security, exception, ban and surveillance**.** In: LYON, D. (Ed.) *Theorizing Surveillance*: The panopticon and beyond. Cullompton, Portland: Willan, 2006.

BOURDIEU, P. et al. *A miséria do mundo*. Petrópolis: Vozes, 1997.

BOURDIEU, P. *A economia das trocas simbólicas*. São Paulo: Perspectiva, 2011.

BRAYNE, S. *Predict and Surveil*: Data, Discretion, and the Future of Policing. Oxford, UK: Oxford University Press, 2021.

BROWNE, S. *Dark Matters*: On the Surveillance of Blackness. Duke University Press, 2015.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, n.81, p.1-15, 2018.

COHEN, S. *Folk Devils and Moral Panics*: The Creation of the Mods and Rockers. London; New York: Routledge, 1987.

CRAWFORD, K. *The Atlas of AI*: Power, Politics and the Planetary costs of Artificial Intelligence. New Haven; London: Yale University Press, 2021.

CRETTIEZ, X. *As formas da violência*. São Paulo: Edições Loyola, 2011.

DANDEKER, C. *Surveillance, power and modernity*. Cambridge, UK: Polity, 1990.

DELEUZE, G. Post-Scriptum das Sociedades de Controle. In: ___. *Conversações*. Rio de Janeiro: Editora 34, 2017.

DILLON, M. The Security of Governance. In: LARNER, W.; WALTERS, W. (Ed.) *Governamentality*: Governing International Spaces. London: Routledge, 2004. p.76-96.

DUFFIELD, M. *Development, security, and unending war*: Governing the World of Peoples. London: Polity, 2007.

ERICSON, R. HAGGERTY, K. The Policing of Risk. In: BAKER, T.; SIMON, J. (Ed.) *Embracing Risk*: The Changing Culture of Insurance and responsibility. Chicago: Chicago University Press, 2002.

ESPOSITI, S. When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society*, v.12, n.2, p.209-25, 2014. Doi: 10.24908/ss.v12i2.5113

FATSIS, L. Policing the beats: The criminalization of UK drill and grime music by the London Metropolitan Police. *The Sociological Review*, v.0, n.0, p.1-17, 2019. Doi: 10.1177/0038026119842480.

FERGUSON, A. *The Rise of Big Data Policing*: Surveillance, Race, and The Future of Law Enforcement. New York: New York University Press, 2017.

FOUCAULT, M. *Discipline and Punish*: The birth of the prison. New York: Vintage Books, 1995.

_____. *A história da sexualidade*: A vontade de saber. São Paulo: Paz e Terra, 2017.

GARVIE, C.; BEDOYA, A.; FRANKLE, J. *The Perpetual Line-up*: Unregulated Police Face Recognition in America. Center of Privacy & Technology. Georgetown University, 2016.

GAYLE, D. Rise in proportion of BAME suspects on Met's gangs matrix. *The Guardian*. May 29, 2018. Disponível em: <https://www.theguardian.com/uk-news/2018/may/29/rise-in- proportion-bame-suspects-met-police-gangs-matrix>. Acesso em: 8 fev. 2021.

HAGGERTY, K. Tear Down the Walls: On Demolishing the Panopticon. In: LYON, D. (Ed.) *Theorizing Surveillance*: The Panopticon and Beyond. Portland: Willian Publishing, 2006.

HAGGERTY, K.; ERICSON, R. The surveillant assemblage. *The British Journal of Sociology,* v.51, n.4, p.605-22, 2000. Doi:10.1080/00071310020015280.

HAN, B.-C. *Topologia da violência*. Petrópolis: Vozes, 2017.

JAKOBS, G.; CACIO MELIÁ, M. *Direito penal do inimigo*: noções e críticas. Porto Alegre: Livraria do Advogado, 2012, p.19-48.

KELION, L. London Police trial Gang violence "Predicting" Software". *BBC News* October 14, 2014. Disponível em: <https://www.bbc.com/news/technology-29824854> Acesso em: 15 out. 2020.

LATOUR, B. On Technical Mediation. *Common Knowledge*, v.3, n.2, p.29-64, 1994.

LIPTON, B. It's PredPol, and it's going to reduce crime: Agencies take algorithmic effectiveness on faith, with few checks in place. *MuckRock*, November 5, 2019. Disponível em: <https://www.muckrock.com/news/archives/2019/nov/05/predictive--policing-lacks- accuracy-tests/>. Acesso em: 5 out. 2020.

LYON, D. *The Electronic Eye*: The Rise of Surveillance Society. London: Polity Press, 1994.

_____. *Surveillance as Social Sorting*: Privacy, Risk and Digital Discrimination. New York: Routledge, 2003.

O'NEIL, C. *Weapons of Math destruction*: How Big Data Increases Inequality. New York: Broadway Books, 2016.

PIZA, E.; WELSH, B; FARRINGTON, D.; THOMAS, A. CCTV surveillance for crime prevention. A 40-year systematic review with meta-analysis. *Criminology and Public Policy*, v.18, n.1, p.135-59, 2019.

SCANNEL, J. *What Can an Algorithm Do? DIS Magazine*. 2016, p.1-9. Disponível em: <http://dismagazine.com/discussion/72975/josh-scannell-what-can-an-algorithm-do/>. Acesso em: 20 nov. 2021.

SCHUBERT, D. Sofrimento e Violência Simbólica. In: GRENFELL, M. (Ed.) *Pierre Bourdieu: conceitos fundamentais*. Petrópolis: Vozes, 2018.

SHINER, M. et al. *The Colour of Injustice*: 'Race', drugs and law enforcement in England and Wales. Stopwatch; LSE; Release: Drugs, the Law & Human Rights, 2011.

THE METROPOLITAN Police. 2020. *Stop et Account: Self Defined Ethnicity*. Disponível em: <https://www.met.police.uk/sd/stats-and-data/met/stop-and-search--dashboard/>. Acesso em: 18 nov. 2020.

_____. *Gangs Violence Matrix*. 2021. Disponível em: <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/gangs-violence--matrix/>. Acesso em: 17 jul. 2021.

WILLIAMS, P. *Being Matrixed*: The (over)policing of Gang suspects in London. London: StopWatch, 2019.

WILLIAMS, P.; CLARKE, B. The Black Criminal Other as an Object of Social Control. *Social Sciences*, v.7, p.234-46, 2018. doi: https://doi.org/10.3390/socsci7110234

WOOD, D. M. Surveillance in the World City. In: DERUDDER, B. et al. (Ed.) *International Handbook of Globalization and World Cities*. Cheltenham. UK: Edward Elgar, 2013.

ZMOGINSKI, F. *A sociedade mais vigiada do mundo*: como a China usa o reconhecimento facial. UOL TILT. 2019. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do-mundo-como-a-china-usa--o-reconhecimento-facial.htm>. Acesso em: 22 out. 2022.

ZUBBOF, S. *The Age of Surveillance Capitalism*: The Fight for a Human Future at the New Frontier of Power. London: Profile Books, 2019.

RESUMO – Nos dias de hoje, a vigilância de dados tem se tornado uma das principais características das atividades governamentais, e se manifesta não somente em vigiar os indivíduos em outra escala (hipervigilância), mas como uma interação sociotécnica envolvendo classificação de risco e dispositivos preditivos. Esses sistemas direcionam esforços para a predição do crime e gestão de riscos, ao invés de promover atritos e confrontos desnecessários. Tais argumentos vão ao encontro da proposta atual de Shoshana Zuboff (2019), para quem as tecnologias de "datavigilância" possibilitam uma forma de poder não violenta focada em moldar comportamentos e decisões dos indivíduos. Diante disso, casos como a experiência atual da Polícia Metropolitana de Londres na implantação da Matriz de Violência de Gangues (GVM), usada para identificar e traçar o perfil das supostamente nominadas "gangues", tornam-se tanto o escopo deste artigo, quanto revelam uma realidade bem mais complexa.

PALAVRAS-CHAVE: Vigilância de dados, Poder instrumental, Violência simbólica, Silenciamento.

ABSTRACT – Dataveillance has become one of the main features of govern activities currently, and it manifests not only as the watching of individuals in another scale (hyperveillance) but as a sociotechnical interaction involving risk classification and predictive devices. These systems direct efforts into crime prevention and risk management, instead of promoting unnecessary friction, and confrontations. Such arguments are in line with the current proposition of Shoshana Zuboff (2019) for whom "dataveillance" technologies enable a nonviolent form of power focused on taming individuals' behaviors and decisions. In light of that, cases like the current experience of London's Metropolitan Police in deploying the Gang Violence Matrix (GVM), used to identify and profile alleged gang nominals both become the scope of this article and reveals a much more complex reality.

KEYWORDS: Dataveillance, Instrumentarian power, Symbolic violence, Sociotechnical Silencing.

Alcides Eduardo dos Reis Peron é graduado em Relações Internacionais e em Ciências Econômicas pela Faculdades de Campinas; mestre e doutor em Política Científica e Tecnológica pela Unicamp; pós-doutorado (Fapesp) em Sociologia pela USP. Professor e coordenador do Curso de Relações Internacionais da Fundação Escola de Comércio Álvares Penteado (Fecap). Pesquisador do Núcleo de Estudos da Violência (NEV-USP). @ – alcidesrperon@gmail.com / https://orcid.org/0000-0003-4537-2775.

Anderson Röhe é advogado graduado pela Universidade Federal Fluminense. Membro da Comissão Especial de Privacidade e Proteção de Dados da OAB-SP; especialista em Direito Digital pela UERJ e ITS Rio; mestre em Políticas Internacionais pela PUC-Rio; doutorando pelo TIDD da PUC-SP. @ – rohemeet20@gmail.com / https://orcid.org/0000-0002-3104-6365.

Recebido em 18.11.2022 e aceito em 2.1.2023.

[I] Fundação Escola de Comércio Álvares Penteado, São Paulo, Brasil.

[II] Pontifícia Universidade Católica, São Paulo, Brasil.