CAXAMBU
43º ENCONTRO ANUAL DA ANPOCS
21 A 25 DE OUTUBRO DE 2019

POLICIAMENTO PREDITIVO, CONTROLE SOCIAL E DESIGUALDADES RACIAIS

Letícia Simões Gomes
doutoranda PPGS/USP
pesquisadora do NEV/USP
Financiamento: FAPESP
(Processo nº 2019/02612-0)

Minas Gerais
2019

Resumo: Este paper é parte de uma pesquisa de doutorado sobre as intersecções entre o uso de tecnologias e discriminação racial pela Polícia Militar do estado de São Paulo (PMESP). Visa-se avaliar a importância do uso da tecnologia — e se tal se enquadra enquanto policiamento preditivo — no policiamento dessa instituição. A partir da noção de racismo institucional, investiga-se como as tecnologias relacionadas ao policiamento podem impactar, em uma sociedade racialmente desigual, a reprodução dessas desigualdades raciais. Enquanto um estudo qualitativo, as fontes mobilizadas são bibliografia especializada e entrevistas com atores envolvidos. Os resultados preliminares indicam que o uso da tecnologias com funcionalidades preditivas pela PMESP aparece em duas situações diferentes da organização, ainda que ambas espacialmente referenciadas: i) contribuindo para a organização dos recursos policiais em áreas específicas/prioritárias por meio do georreferenciamento de registros de ocorrências criminais; e ii) fundamenta-se na introdução de tecnologias de análise de imagens para a identificação de situações suspeitas. O sistema Detecta entra nessa segunda modalidade; ainda que seja externo à Polícia Militar, possui uma interface e interatividade com a instituição. Analisando mais de perto a operacionalização do Detecta, põe-se em questão o uso das capacidades preditivas do sistema; seu uso restringe-se à expansão da malha de vigilância, mediada pela subjetividade dos atores por ele abrangidos. Nessas situações, ele parece reforçar as práticas de filtragem racial e de racialização do suspeito, contribuindo para a estigmatização de pessoas negras e suas comunidades.

Palavras-chave: Polícia Militar, racismo institucional, policiamento preditivo, controle social, filtragem racial.

Este *paper* é parte de uma pesquisa de doutorado em andamento que trata de políticas de segurança pública que utilizam da tecnologia como instrumento preditor da criminalidade e, por isso, como orientadora das práticas policiais em contextos de pronunciada desigualdade racial. Nos últimos anos, a literatura internacional tem chamado a atenção para a penetração de novas tecnologias nas práticas de policiamento e para como tal tendência pode reproduzir vieses raciais, apesar de estas serem anunciadas como potencialmente mitigantes dessas distorções.

No Brasil, verifica-se a existência de desproporções raciais em dados relativos a prisões em flagrante e vítimas de uso da força letal por policiais (SINHORETTO et al., 2014; CANO, 1997, 2004, 2010). Dentre a sociedade civil e os movimentos sociais, há uma percepção de viés racial na (má-)conduta policial (RAMOS, 2015; RAMOS; MUSUMECI, 2005; PORTO, 2001), que vem sendo internacionalmente identificada como um fator que compromete a legitimidade da polícia e confiança na mesma (WARREN; FARRELL, 2009). Entretanto, disparidades raciais não são necessariamente consequência de políticas ou agentes intencionalmente racistas – o conceito de racismo institucional[1] se coloca no intuito de perscrutar os mecanismos "racialmente neutros" cujas consequências são a produção de desigualdades raciais e discriminação racial na atividade institucional (no nosso caso, da polícia). A filtragem racial (*racial profiling*) é um desses mecanismos, nos quais o agente vigia mais, aborda mais e prende mais negros. Enquanto conceito, o foco está no agente e o que o leva a agir desta maneira. Há, contudo, outro ponto a ser considerado para a geração de resultados racialmente desproporcionais na atividade policial: seu aspecto institucional, ou seja, como a política pública – a despeito dos agentes que a implementam – reproduz vieses raciais. Indo além, como sua formulação, embora não aparente relação com raça, tem consequências raciais.

Com essas considerações em mente, observa-se um movimento em outros contextos nacionais de transformação no cenário do policiamento, com a introdução de novas tecnologias na elaboração de políticas de segurança pública, como o uso de *Big Data, Data Analytics* e *Data Science* na formulação de políticas de policiamento preditivo (*predictive policing*). Entretanto, no debate nacional sobre raça e segurança pública, esse movimento ainda é pouco explorado; contribuições sobre este tema são majoritariamente oriundas do

[1] "[existência de] mecanismos de discriminação inscritos na operação do sistema social e que funcionam, até certo ponto, à revelia dos indivíduos." (GUIMARÃES, 1999 apud SINHORETTO et al., 2014, p. 28).

contexto norte-americano. O conceito de filtragem racial, tanto na literatura norte-americana quanto na brasileira, está localizada no campo do policiamento direto, no contato do agente de segurança pública com o cidadão. Sucede, porém, que o desenvolvimento das próprias políticas de segurança pública em uma sociedade racialmente desigual – mesmo que cegas à raça (*colourblind)* e visando à redução da discricionariedade de onde se imagina provir o tratamento discriminatório – tem reproduzido viés racial ao concretizar-se (SELBST, 2017; FERGUSON, 2015). Essa discussão, inclusive pela incorporação de novas tecnologias ser ainda incipiente pelas forças policiais brasileiras, praticamente inexiste na literatura sociológica brasileira sobre policiamento. Todavia, o policiamento preditivo começa a acontecer no Brasil, e *big data* já é objeto de regulação recém-sancionada (Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018).

Este *paper*, então, propõe-se a discutir as relações entre desigualdades raciais e novas tecnologias de policiamento, parcial ou completamente implantadas pelo policiamento na capital paulista. Destarte, cabe caracterizar brevemente o uso de *big data* e novas formas de análise de dados integradas a ferramentas e políticas de segurança; na sequência, expõe-se sumariamente duas situações nas quais tecnologias com potencialidades preditivas são utilizadas pela Polícia Militar. Explora-se com um pouco mais de detalhe uma das tecnologias em particular, adotada pela Secretaria Estadual de Segurança Pública do estado de São Paulo: o sistema Detecta. Com isso, não se pretende implicar que esse é o único instrumento preditivo adotado pelo aparato de segurança estadual, mas que é aquele ao qual, nesta etapa da pesquisa, se teve acesso. Conclui-se o texto com algumas considerações sobre alguns achados de campo e próximos passos da pesquisa.

***

Como é de praxe entre grandes novidades muito expostas e discutidas nos meios de informação, *big data* não tem uma definição precisa, e os conceitos que o cercam (*data analytics*, *data science*, *metadata analytics, data mining,* entre tantos outros) também carecem de conceituação rigorosa. O que, afinal, é *big data* e por que esse fenômeno vem se tornando tão importante?

Uma definição bastante ilustrativa para o termo é de Berman (2013, apud FERGUSON, 2015, p. 352), que o define enquanto banco(s) de dados que possuem os "3Vs":

volume (grandes quantidades de dados), variedade (esses dados vêm em diferentes formatos e de diferentes fontes, incluindo bancos de dados tradicionais, imagens, documentos e registros complexos) e velocidade (o conteúdo desses dados está em constante transformação). Toda essa quantidade e heterogeneidade de dados necessitam de tecnologias específicas – inteligência artificial – para serem processados, interpretados e a partir deles se criarem padrões e modelos preditivos (COHEN, 2013, apud FERGUSON, 2015). De um ponto de vista sociológico, Mayer-Schönberger & Cukier (2013) definem *big data* como referente a "coisas que alguém consegue fazer em larga escala e que não pode ser feita em pequena escala, extrair novas epifanias ou criar novas formas de valor, de maneira a transformar mercados, organizações, a relação entre cidadãos e governos, entre outros" (apud RICHARDS; KING, 2014, p. 394, tradução livre).

A vigilância e o acúmulo de dados sobre indivíduos e cidadãos não é um fato recente, tanto na esfera estatal (FOUCAULT, 1984) como na esfera econômica. Aponta-se como um diferencial do *big data* o fato de a quantidade e heterogeneidade de dados ser tamanha que sua manipulação é melhor executada por inteligência artificial, i.e., pelo desenvolvimento de sistemas capazes de analisá-los. Nesse sentido, o "mundo do *big data*" – no qual se integram diversas matrizes de dados que, cruzadas, nos dão informações bastante precisas sobre pessoas, lugares, preferências e comportamentos coletivos – possibilita a criação de modelos preditivos integrando variáveis que não seriam captadas a "olho nu". Informações são continuamente coletadas e seu uso gera consequências impensadas nas relações sociais.

Uma das esferas em que o *big data* vem sendo incorporado é justamente no Sistema de Justiça Criminal, mais especificamente pelo policiamento. O policiamento preditivo pode ser definido como uma "aplicação da modelagem por computadores a dados criminais passados para predizer atividade criminal futura" (BACHNER, apud JOH, 2014, p. 42, tradução livre), ou seja, "Policiamento preditivo é a fusão da 'tecnologia da informação…, teoria criminológica, [e] algoritmos preditivos'. Em outras palavras, é o 'uso de dados e análises para predizer o crime'" (SELBST, 2017, p. 114, tradução livre, notas omitidas). O uso de análises estatísticas e projeções para o trabalho policial tampouco é novidade. O que muda, aqui, é a expansão dessa lógica para uma situação com mais dados disponíveis e mais poder para analisá-los, o que tornaria tais policiamentos mais precisos, neutros e confiáveis.

Contudo, a neutralidade não se verifica: há muitos níveis a partir dos quais a inteligência artificial pode adquirir vieses e reproduzir discriminação. Dentre eles,

elencam-se: a) a discricionariedade do programador no desenvolvimento do *software* (o grau de precisão e generalização das variáveis, as conexões causais e exemplos dados à máquina no processo de *machine learning*) (SELBST, 2017, p. 131); b) a confiabilidade dos dados (dado que muitos vêm de *data brokers*, i.e., terceiros que compilam e comercializam informações, outros vêm de bancos de dados do governo) (MADDEN et. al, 2017); c) a natureza dos dados (como o banco sobre antecedentes criminais estão dentre os mais frequentes, assim como o de ocorrências) (SELBST, 2017; LUM; ISAAC, 2016); d) a manipulação dos dados (em quais categorias crimes são agrupados e qual a sua priorização (SELBST, 2017); e) a inserção dessas técnicas no processo de policiamento (se serve para alocação de recursos, para a formação de "listas de ameaças ("*threat lists*"), para investigação de suspeitos pré-identificados, etc.) (Idem).

Dentre esses pontos, um parênteses sobre os principais dados disponíveis. A modelagem desses *softwares* é bastante heterogênea em suas fontes, mas alguns dados relativos a bancos de dados do Estado estão quase sempre presentes, tais como fichas de antecedentes criminais, passagem pelo sistema carcerário, participação nos sistemas de assistência social, etc. No caso norte-americano, ao se considerar a histórica tendência de supervigilância dos pobres e da população negra (MADDEN et. al, 2017, p. 63-66; WACQUANT, 2007; BYFIELD, 2018), levanta-se questões sobre como a sua sobrerrepresentação nessas amostras pode levar a vieses.

Além disso, é interessante notar que a maior parte dessas tecnologias usa como base crimes patrimoniais e/ou ligados ao tráfico de entorpecentes, coincidentemente os tipos mais presentes nas bases de dados criminais. Outras tipologias, como estupro, tortura, crime de ódio, violência doméstica, não entram nesta contabilização. Nesse sentido, Joh (2014) apontou que esses sistemas não estão preparados para alguns tipos de ocorrência, pois muitos deles não obedecem a padrões territoriais. A natureza dos dados, então, é essencial: ao ensinar ao *software* o que é crime, recorre-se a uma gama duplamente restrita de dados: primeiro, ao ser um banco de dados de justiça criminal, filtra-se pelo sistema de registro oficial (há aqui um viés do que foi notificado enquanto tal, não correspondendo a uma amostra representativa nem universal dos delitos, cf. RATTON JR, 1996; ADORNO, 1993), que consolida vieses historicamente construídos na atividade policial. Segundo, recorta-se tal banco de dados para aqueles que são enquadráveis na construção de uma modelagem específica de *software*, focalizando ainda mais em crimes patrimoniais e/ou relacionados ao

tráfico. O sistema, então, tende a reproduzir padrões encontrados nessa seleção.

***

A partir do exposto acima, pode-se localizar nosso tema como a interação entre policiamento preditivo e desigualdade racial. Faz-se necessário, então, compreender o desenvolvimento do policiamento preditivo e sua articulação com a pré-existência de desigualdades substantivas entre grupos raciais. Nossos pressupostos, indicados pela literatura, são: a) há disparidades raciais no acesso ao direito à segurança no Brasil; b) políticas neutras podem reproduzir vieses encontrados nos contextos nais quais são introduzidas. Além da produção de vieses, os contextos culturais, sociais, econômicos e políticos também interferem na maneira pela qual a tecnologia vem a ser implementada e reinterpretada, que lugar passa a ocupar no mundo social pré-existente e quais sentidos passa a ter (LUPTON, 2015, p. 16).

No caso paulista, esses sistemas não colocam em prática todas as potencialidades preditivas. A partir da análise do sistema Detecta, argumenta-se que sua adoção parcial contribui para que posturas discriminatórias e segregacionistas se reproduzam. A introdução desse aparato de vigilância, ao invés de coibir práticas discricionárias baseadas no julgamento subjetivo, parece potencializá-los e legitimá-los por meio de montagens sociotécnicas, nas quais a subjetividade dos observadores é mediada por tecnologias e sistemas de vigilância.

No caso da PMESP, identificou-se por ora dois mecanismos que podem operar formas de policiamento preditivo. Nota-se que a adoção dessas tecnologias é bastante incipiente, ainda que seja parte dos projetos das gestões da Secretaria de Segurança Pública do estado. Destarte, há o Plano de Policiamento Inteligente (PPI). A principal atividade policial preventiva da PMESP é aquela estruturada ao redor da Radiopatrulha; para tanto, o patrulhamento das ruas é organizado via batalhões; a alocação desse efetivo se dá com a participação do Centro de Inteligência da Polícia Militar, o qual desenvolve o PPI, materializado na entrega semanal aos batalhões de um Cartão de Prioridade de Patrulhamento (CPP). Ele é uma "orientação sobre a atividade que o patrulheiro deverá exercer (tipo de crime, *modus operandi*, características de infratores, tipos de vítimas preferenciais, etc.)" (SÃO PAULO, 2005 apud RISSO, 2018). O PPI então se baliza pela análise das ocorrências criminais, estabelecendo tipos de ocorrências prioritárias para então traçar *hotspots*; a partir

disso, direciona-se o efetivo policial e demais recursos na intenção de se adiantar ao cometimento do delito.

O segundo instrumento identificado foi o Detecta. Adquirido pela primeira vez em 2014 pela Secretaria de Segurança Pública do estado, o Detecta foi um sistema da Microsoft inspirado na experiência do DAS (*Domain Awareness System*)[2], fruto da parceria da empresa com o departamento de polícia de Nova York, cujo objetivo era o rastreamento de suspeitos e compilação de dados. Originalmente projetado para identificação e prevenção de ataques terroristas em solo norte-americano, o Detecta foi adquirido em função da promessa de ser um sistema de vigilância que permite a identificação automatizada de criminosos e que sincroniza várias fontes de dados para melhorar a atividade policial.

Essa tecnologia organiza os dados de maneira georreferenciada. Entretanto, seu diferencial está na conjunção de reconhecimento de imagens com a construção de modelos estatísticos a partir da análise de grandes bancos de dados — predominantemente públicos. Por meio deles, deriva-se padrões criminais futuros, que serão incorporados no policiamento, aumentando a eficiência policial na guerra ao crime. Originário de concepções e parâmetros militaristas — que equivale a luta contra o crime à luta contra o terrorismo —, a implementação do DAS trouxe a acomodação de novos atores ao modelo de segurança pública, ao incorporar empresas e tecnologias oriundas do setor privado na esfera do provimento da segurança pública estatal.

Desta feita, a instalação do sistema Detecta não se deu conforme o planejado. Em 2016, um relatório do Tribunal de Contas do Estado de São Paulo diagnosticou que o sistema não funcionava adequadamente, as funções de predição estavam inoperantes e havia baixa integração de bancos de dados. Em pesquisa de campo apresentada por Perón, Simões-Gomes e Nery (2019), a razão apresentada para tanto foi incapacidade logística e de custos — dificuldades que seriam sanadas no médio prazo, com a incorporação de atores privados. Tal integração, no entanto, não indica o fracasso da iniciativa, mas a configuração determinante de uma simbiose entre os setores público e privado para a operacionalização dessa política. A análise desses novos elementos é essencial para a compreensão do funcionamento do sistema.

[2] *Situational awareness* é um termo derivado da jargão militar e pode ser entendido como um regime de vigilância do campo operacional, por meio do monitoramento de diversos elementos e informações que podem contribuir para a gestão operacional, tanto tática quanto estratégica. Essa noção deriva dos esforços militares de coletar e produzir dados massivos, a partir de fontes públicas e privadas, para predizer e agir contra ameaças terroristas.

Em sua dimensão pública, o Detecta tornou-se um sistema abrangente de integração de dados e câmeras, em que a aquisição e instalação de novos aparelhos foram delegadas à iniciativa privada. Constam no sistema as câmeras públicas municipais do Radar (que contam com leitor automatizado de placas de veículos), as City Câmeras, bem como uma malha de aparelhos privados de cidadãos que buscam a adesão — seja individualmente, seja por intermédio de associações, seja em negócios e empresas privadas.

Assim, vê-se que esses elementos a serem levados em consideração têm múltiplas filiações: desde projetos municipais (como o City Câmeras e o *app* SP+Segura), servidores públicos estaduais (Polícias Civil e Militar, Secretaria de Segurança Pública), a empresas nacionais ou transnacionais (como Microsoft, Genetec, Techvoz, Tacira e Aster) e usuários, associações e instituições (Sociedade de Amigos do Alto de Pinheiros e Universidade de São Paulo). Na leitura do setor privado (evidenciado na entrevista de um executivo da Microsoft), a integração e visualização dos dados pelo Estado seria dificultada pela falta de *expertise*, de recursos financeiros, bem como pela despadronização semântica entre as agências de segurança pública. Nesse sentido, a ideia central seria não só providenciar uma solução instantânea para a Secretaria Estadual de Segurança Pública, mas modificar a gestão e interação entre as agências de segurança, tanto as forças policiais, militares e civis, como o aparato judicial. Assim, seria possível constituir uma *situational awareness*, mediada por esses instrumentos de vigilância (apud PERÓN, SIMÕES-GOMES, NERY, 2019).

A expansão do sistema de câmeras estar vinculada à iniciativa privada conferiu uma distribuição espacial peculiar, enfatizando a cobertura em bairros paulistanos de classe média e alta, regiões de centros de finanças e negócios, bem como espaços públicos e privados de intensa circulação. Essa tendência, também denominada formação de 'perímetros de securitização' (PERÓN, SIMÕES-GOMES, NERY, 2019), divide a cidade entre zonas de visibilidade e invisibilidade, de coleta de imagens heterogênea e de níveis heterogêneos de participação comunitária, tanto nas divisões de custos como de responsabilidades para o provimento da segurança.

O setor privado, então, facilitou a organização sociotécnica dessas regiões, mediando a relação entre associações de moradores, indústrias de tecnologia de vigilância, o estado e o município. De uma parte, o setor auxilia na compra, provisão e instalação de câmeras, bem como no estabelecimento de canais de comunicação entre moradores, e promoção de eventuais treinamentos para identificação de problemas aos usuários. De outra parte, essas

provedoras de serviço garantem que as imagens geradas sejam integradas ao setor público, mediante a venda de *data analytics*.

Este mesmo trabalho de campo indicou que, dentre os agentes de segurança vinculados ao Detecta entrevistados, há a expectativa de que o sistema contribuiria para o aumento da eficiência e redução do tempo de resposta a chamados nessas áreas, bem como a identificação rápida de veículos (Ibidem). Haveria, pois, zonas na cidade de comunicação integrada e ágil, áreas essas em que o trabalho de abordagens, investigação e identificação de suspeitos pelas polícia seria facilitada. Tudo se dando no tempo presente, da vigilância continuada, porém não preditiva. Permanece então a dependência de interpretação e operacionalização humanas dessas informações.

Assim, em última instância, o Detecta se configura como um amálgama sociotécnico operacionalizado pelo olhar humano. Esse olhar subjetivo do agente de segurança e/ou do usuário atento tem relação com suas percepções, intuições e experiências prévias, derivadas de representações racializadas do suspeito (cf. SCHLITTLER, 2016; RAMOS; MUSUMECI, 2005).

No trabalho de campo descrito por Perón, Simões-Gomes e Nery (2019), há um caso bastante ilustrativo: a Universidade de São Paulo (USP). O *campus* Butantã foi um perímetro integrado ao Detecta no início de 2018, que permite o controle eletrônico do espaço a partir de um centro de monitoramento, integrado a câmeras e aplicativos. No aplicativo com interface para a comunidade universitária, há um 'botão de pânico' que pode ser acionado em caso de incidentes ou ocorrências. O alerta gerado é transmitido no centro de monitoramento, e a sua geolocalização ativa as câmeras dos arredores. Todavia, essa estrutura é mobilizada muito raramente. A rotina dos operadores do sistema se restringe ao monitoramento e observação das imagens gravadas e retransmitidas, que usam da sua experiência no ramo para diferenciar situações suspeitas. Situações essas que consistiam em jovens — negros — que não condiziam com o estereótipo do estudante universitário.

Os habitantes e circulantes habituais desses perímetros securitizados ganham proeminência nesse equipamento enquanto prosumidores[3] do sistema de vigilância. Ao

[3] Prosumidor é um aportuguesamento do termo *prosumer*, que consiste na fusão das capacidades de consumidor e produtor (*consumer* + *producer*) em uma mesma pessoa. Essa noção deriva da criação e expansão de plataformas *online* que permitem e encorajam seus usuários a contribuir e compartilhar conteúdo com outros em tempo real, chamando a atenção para as modificações nas formas de interação entre usuários por meio de tecnologias digitais (LUPTON, 2015, p. 10).

mesmo tempo em que produzem conteúdos e dados, eles consomem as informações extraídas do agregado desses dados. A possibilidade de sinalização de ocorrências e situações suspeitas ao poder público por meio dessas plataformas — como, no *app* SP+Segura, de cometimentos de delitos e infrações — alçam a percepção ordinária e destreinada ao status de dado registrado, que contribui para, de um lado, a desproporção numérica de dados contra suspeitos racializados, e de outro, a legitimação da figura do suspeito racializado e do indesejável.

A relação de prosumidor do sistema insere os usuários em um exercício ativo de vigilância e endereça o sentimento de insegurança e medo, apaziguando-o por meio de sua incorporação à atividade cotidiana. Sua utilização rotineira provê, assim, o *feedback* constante para a geração contínua de dados — os quais podem ser úteis no desenvolvimento da interface preditiva do *software*.

O peso e relevância desses dados passados, a serem usados em um processo de *machine learning*, tem o potencial de estabelecer um curso de ação — ou a predição de um evento — em detrimento de outro. Conforme argumentado por Esposito, "*[data] only become significant when processed and presented in a context, producing information. Information requires data, but data are not enough to have information*" (2017a, p. 4). Aqui, a produção da informação está vinculada à sua projeção do futuro e intervenção no presente, a partir das representações e imagens dele derivadas. A ressignificação, então, contribui para uma espécie de manufatura do futuro, já que o algoritmo visualiza o futuro existente pela intervenção algorítmica. A busca por padrões e intervenção na vida social com base em projeções feitas a partir de dados passados pode gerar uma espécie de exponencialidade das tendências identificadas — o que se denomina *overfitting* na computação e que basicamente deriva da uma cegueira dos algoritmos para outras possibilidades além daquelas identificadas nos eventos passados. A predição algorítmica, assim, vê o futuro como uma espécie de projeção do passado, mediada pelo presente. Como Byfield (2018, p. 11) coloca,

> *policing technologies have encouraged people to describe its capabilities as 'predictive', meaning that with the use of data mining, i.e. using algorithms to extract patterns from large amounts of data gathered in the daily work of policing, policing agencies think they can learn patterns in the occurrence of crime and use those patterns in decision-making to prevent crime and eliminate bias. One fallacy with this approach is that digital data being used in the predictive policing analysis is*

> *based on previous policing patterns. So the likely patterns you will get are really patterns about racialized forms of surveillance.*

A despeito dos padrões prévios de policiamento notados por Byfield, a implementação do caráter preditivo do sistema Detecta tem o potencial de incorporar as formas racializadas de suspeição dos usuários abrangidos nesses perímetros securitizados.

***

O debate público sobre a expansão do uso de dados digitais e *machine learning* para diversos âmbitos da vida social amiúde envolve considerações sobre um aumento da neutralidade e redução de discriminações derivadas das subjetividades dos atores. O uso de *big data*, então, é tratado como capaz de proporcionar de mais precisão, conferir potencialidades preditivas, as quais contribuem para o aumento da eficiência, segurança, geração de valor e gestão de recursos. "*[B]ig data sets are systems of knowledge (...) [they] are both the product of social and cultural processes and themselves act to configure elements of society and culture.*" (Lupton, 2015, p. 116). No entanto, a própria manipulação desses dados envolve escolhas e a agência de indivíduos — seja na seleção, tratamento e organização dos dados, como no desenvolvimento, treinamento e aplicação do *software*. Tais decisões não estão isentas de subjetividade ou das percepções dos indivíduos sobre o mundo social.

Para além dos vieses intrínsecos à produção e operacionalização originalmente idealizada dessas tecnologias, o contexto cultural, social, político e econômico no qual essas tecnologias são introduzidas também agem sobre as formas nas quais elas são reinterpretadas, que espaço assumem neste contexto e que usos se fazem delas. Como vimos, no caso da adoção do sistema Detecta, houve uma vasta expansão do sistema de vigilância, impulsionada pela iniciativa privada e acolhida pelo setor público. Tal conformação ampliou o espaço das empresas e da participação de usuários (individual ou associativamente) na interação com o sistema e os agentes de segurança pública, ainda que de forma heterogênea pelo perímetro urbano.

Contudo, por ora o Detecta parece não colocar em prática suas funcionalidades preditivas: seu uso restringe-se ao aumento da cobertura da malha de vigilância. Por meio dela, coletam-se dados mediados pela subjetividade dos atores contemplados pelo sistema.

Nessas situações, ele serve de intermediador de práticas de filtragem racial e de racialização do suspeito, contribuindo para a estigmatização de pessoas negras e suas comunidades.

Finaliza-se este *paper* apontando para o caráter ainda exploratório e processual da pesquisa. Até o momento, identificou-se nas atividades da Polícia Militar do estado de São Paulo duas modalidades de tecnologias digitais que poderiam incorporar análises de dados preditivas. Ressalta-se que a investigação está em andamento, e este é um resultado preliminar.

Referências bibliográficas

ADORNO, S. A criminalidade urbana violenta no Brasil: um recorte temático. **BIB,** v. 35, n. 1, p. 3-24, 1993.

BYFIELD, N. P. Race science and surveillance: police as the new race scientists. **Social Identities**, v. 0, n. 0, p. 1–16, 2018.

CANO, I. **Letalidade da ação policial no Rio de Janeiro.** Rio de Janeiro: ISER, 1997.

_____. O perfil racial dos mortos pela polícia no Rio de Janeiro. Texto para o **Relatório de Desenvolvimento Humano 2004** – Capítulo Sistema de Justiça Criminal. Rio de Janeiro: CESeC e PNUD, 2004.

_____. Racial bias in police use of lethal force in Brazil. **Police Practice and Research: An International Journal**, v. 11, n.1, p. 31-43, 2010.

ESPOSITO, E. Algorithmic memory and the right to be forgotten on the web. **Big Data & Society**, v. 4, n. 1, p. 1-11, 2017.

FERGUSON, A. G. Big Data and Predictive Reasonable Suspicion. **University of Pennsylvannia Law Review**, v. 163, n. 2, 2015.

FOUCAULT, M. **Segurança, Território e População**. São Paulo: Ed. Martins, 1984.

JOH, E. E. Policing by numbers: Big data and the 4th Amendment. **Washington Law Review**, v. 89, 2014.

LUM, K.; ISAAC, W. To predict and serve? **Significance**, 2016.

LUPTON, D. **Digital Sociology**. New York: Routledge, 2015.

MADDEN, M. et al. Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. **Washington University Law Review**, v. 95, 2017.

PERÓN, A. E; SIMÕES-GOMES, L.; NERY, M. **Predictive Policing in governing the undesirable? The Detecta Surveillance System in São Paulo and the (in)security *dispositif***. Paper apresentado em Connected Life 2019: Data & Disorder. Londres: 2019.

PORTO, M. S. Violência e segurança: a morte como poder? In: **Violência policial: tolerância zero?** Goiânia: Ed. UFG, 2001.

RAMOS, P. **Relações raciais e violência: um balanço da produção teórica nacional e internacional dos últimos dez anos.** Paper apresentado no XVII Congresso Brasileiro de Sociologia. Porto Alegre: 2015.

RAMOS, S.; MUSUMECI, L. **Elemento suspeito: abordagem policial e discriminação na cidade do Rio de Janeiro.** Rio de Janeiro: Civilização Brasileira, 2005.

RATTON JR, J. L. **Violência e cultura no Brasil contemporâneo:** homicídios e políticas de segurança pública nas décadas de 80 e 90. Brasília: Cidade Gráfica e Editora, 1996.

RICHARDS, N. M.; KING, J. H. Big data ethics. **Wake Forest Law Review**, v. 393, 2014.

RISSO, M. I. **Da prevenção à incriminação: os múltiplos sentidos da abordagem policial**. Tese de Doutorado. São Paulo: Fundação Getúlio Vargas, 2018.

SELBST, A. D. Disparate impact in Big Data policing. **Georgia Law Review**, v. 52, 2017.

SCHLITTLER, M. C. **"Matar muito, prender mal" : a produção da desigualdade racial como efeito do policiamento ostensivo militarizado em SP.** Tese de Doutorado. São Carlos: UFSCar, 2016.

SINHORETTO, J.; *et al.* A filtragem racial na seleção policial de suspeitos: segurança pública e relações raciais. In: **Segurança Pública e Direitos Humanos: Temas Transversais**. Brasília: Ministério da Justiça, Secretaria Nacional de Segurança Pública (SENASP), 2014.

WACQUANT, L. **Punir os Pobres**. Rio de Janeiro: Ed. Revan, 2007.

WARREN, P. Y.; FARRELL, A. M. Y. The Environmental Context of Racial Profiling. **Annals of the American Academy of Political & Social Science**, v. 623, p. 52–63, 2009.