Segurança pública na era do Big Data: policiamento algorítmico, suas limitações operacionais e seus dilemas éticos

Daniel Edler

Resumo

Novas tecnologias de segurança têm transformado a rotina de forças policiais, trazendo mais eficácia para o serviço de investigação e permitindo ao policiamento ostensivo aumentar a eficiência no controle preventivo do crime. Avanços recentes na área de ciência de dados, além da disponibilidade de sistemas de processamento computacional mais baratos, permitem que departamentos de polícia aprimorem o serviço prestado à população, auxiliando as forças de segurança a "fazerem mais com menos". Contudo, essas inovações também criam desafios na prática policial. Além de apresentar aplicações recentes de *big data* no campo do policiamento e suas limitações operacionais, esse artigo debate os riscos da vigilância em massa e do aprofundamento de padrões discriminatórios nas estratégias de controle do crime.

Abstract

New security technologies have transformed the routine of police forces, making investigative work more effective and allowing visible policing to increase efficiency in preventive crime control. Recent advances in data science, in addition to the availability of cheaper computer pro-

cessing systems, allow police departments to improve the service provided to the population, helping security forces to "do more with less." However, these innovations also create challenges in police practice. In addition to presenting recent applications of big data in the field of policing and their operational limitations, this article discusses the risks of mass surveillance and the deepening of discriminatory patterns in crime control strategies.

1. Introdução

As vantagens de inovações tecnológicas no campo da segurança pública são colhidas todos os dias nas grandes cidades brasileiras. Por exemplo, até poucos anos atrás, sistemas de videomonitoramento tinham utilidade bastante restrita, oferecendo imagens de baixa resolução, o que limitava a polícia a análises superficiais sobre a dinâmica criminal. A dificuldade de armazenamento de dados também representava um desafio, já que novos registros eram muitas vezes gravados sobre fitas VHS utilizadas nos dias anteriores. Se a polícia não agisse rápido, perdia as evidências. Atualmente, não apenas as câmeras espalhadas pela paisagem urbana produzem imagens em alta resolução, como sistemas de processamento de vídeo em tempo real são capazes de gerar alertas para situações suspeitas e identificar indivíduos envolvidos em ações delituosas. Ou seja, as polícias militares podem responder mais rapidamente aos eventos criminais e as polícias civis são capazes arrolar evidências robustas em seus inquéritos enquanto economizam horas de serviço. Esses avanços se devem, em grande medida, à disponibilidade massiva de dados e à possibilidade de processamento algorítmico para a identificação de padrões criminais e eventos de interesse ao trabalho policial. Em outras palavras, as inovações descritas acima se devem ao advento do *big data*.

Big Data pode ser definido como a capacidade de coletar, armazenar, processar e analisar grandes volumes de dados, frequentemente em tempo real, a partir de fontes diversas e heterogêneas (MAYER-SCHÖNBERGER

& CUKIER, 2017). Sua principal característica está na combinação dos chamados cinco "Vs":

1. Volume: a escala dos dados coletados e disponibilizados para análise e processamento é cada vez maior, sendo medida não mais em *kilobytes* ou *megabytes*, mas, geralmente, em *petabytes* (10^15 bytes) e *exabytes* (10^18 bytes).
2. Velocidade: o processamento de dados ocorre em tempo real, o que permite a atualização de análises em poucos segundos, aumentando, por exemplo, a consciência situacional da polícia e sua capacidade de intervenção.
3. Variedade: os dados coletados podem ser estruturados (e.g., uma base de dados como nome e idade de indivíduos condenados pela justiça) e não-estruturados (e.g., vídeos produzidos por sistemas de monitoramento).
4. Veracidade: a maior disponibilidade de dados não vem necessariamente com maior certeza sobre sua qualidade e acurácia, sendo necessário avaliar a adequação dos dados à análise pretendida. Porém, o cruzamento de diferentes bases pode proporcionar ganhos de confiança sobre a informação analisada.
5. Valor: as vastas bases de dados tanto têm valor em si, formando um enorme mercado secundário de *data brokers*, como agregam enorme valor a processos de decisão nos setores público e privado.

Frente a esse cenário, entusiastas apontam que o *big data* deve revolucionar a maneira como trabalhamos, nos relacionamos e pensamos (DOMINGOS, 2015; FRY, 2019). Como descrevem Mayer-Schönberger e Cukier (2013, p. 132):

> Antigas certezas estão sendo questionadas. O *big data* requer nova discussão quanto ao caráter das tomadas de decisões... Uma visão de mundo que pensávamos estar relacionada com causas é desafiada pela preponderância das correlações. A posse do conhecimento, que já signi-

ficou o entendimento do passado, se transforma na capacidade de prever o futuro.

A definição de *big data* pode ser relativamente simples, mas entender seu impacto na sociedade é bem mais controverso. Dois pontos levantados na descrição de Mayer-Schönberger e Cukier (2013) são centrais para a discussão: a produção de conhecimento a partir de correlações e a capacidade de previsão de fenômenos sociais.

No primeiro caso, alguns autores apontam que o *big data* induz novas abordagens epistemológicas sobre formas de conhecer o mundo (KITCHIN, 2014), o que, quando levado ao extremo, gera argumentos sobre o "fim da teoria", já que o "dilúvio de dados torna[ria] o método científico obsoleto" (ANDERSON, 2008). Nessa perspectiva, a profusão de dados nos permitiria abandonar a obsessão por compreender mecanismos causais e abraçar um conhecimento pautado exclusivamente na identificação de padrões (na natureza e na sociedade) e em suas mais variadas correlações (ZAVRŠNIK, 2018). O cruzamento de *exabytes* de dados sobre consumo e meteorologia, por exemplo, nos permitiria descobrir que indivíduos compram mais doces em dias de chuva. Essa correlação pode indicar que as condições climáticas causam variações na dieta da população, mas isso não é necessariamente verdade e nem relevante. O que importa para um gerente de mercado, digamos, é que ele deve ter um bom estoque de doces nos dias em que a previsão for de chuva.

No campo da segurança pública, o foco em correlações tem transformado a compreensão sobre o tipo de informação considerada relevante para o trabalho policial, o que leva à pressão pela expansão dos dados disponibilizados para as forças de segurança. Dito de outra forma, se antes serviços de inteligência e análise criminal focavam em diminuir o tamanho do palheiro para tornar mais eficiente a busca pela agulha, atualmente não se dispensa nada. Como podemos encontrar correlações surpreendentes entre variáveis que julgávamos distantes, qualquer dado é a priori importante para o combate ao crime. A busca

por suspeitos de lavagem de dinheiro pode obter avanços, por exemplo, pelo cruzamento de dados da Receita Federal, de empresas de cartões de crédito, instituições bancárias, redes sociais, buscadores na internet (e.g., Google), e serviços de compras online (e.g., Amazon). De modo semelhante, a coleta massiva de dados meteorológicos, de transporte e de interações nas redes sociais, somado ao uso de bases cartográficas com geolocalização de escolas, parques e hospitais, pode levar à descoberta de padrões criminais antes ignorados. Nessa nova forma de "conhecer" o crime, importam menos as causas do comportamento delituoso e mais as correlações que permitem a identificação de perfis ou locais de risco (WEISBURD, 2015).

E é justamente a lógica do risco que nos leva para o segundo ponto da definição de Mayer-Schönberger e Cukier (2013). Embora a experiência policial e os dados criminais já permitissem identificar determinados padrões, como concentração de roubos em áreas de grande circulação e em dias de pagamento, o cruzamento de novas bases de dados promete ir além na granularidade das informações fornecidas, permitindo a polícia a passar de estratégias preventivas e investigativas, para ações preditivas (EDLER & LOBATO, 2021). Por exemplo, ao cruzar dados de desempenho escolar, de serviços de assistência social e de saúde, algumas empresas prometem construir avaliações de risco sobre a chance de determinado jovem cometer crimes no futuro próximo (STATEWATCH, 2025). Assim sendo, o poder público pode acionar um conjunto de medidas que intervenham na situação desse jovem antes que o crime seja, de fato, cometido. Valendo-se de dados semelhantes, forças policiais têm buscado construir sistemas que avaliam também a chance de indivíduos integrarem redes criminais (DODD, 2018). Policiais, investigadores, promotores e juízes têm usado essa informação para auxiliar em processos de tomada de decisão, seja concentrando esforços na busca por mais evidências, seja alertando as patrulhas locais (RYBERG & ROBERTS, 2022).

Observando esse contexto, profissionais do sistema de justiça criminal e desenvolvedores de aplicações de *big data* para a segu-

rança pública argumentam que as inovações recentes representam a substituição do "faro policial" e da experiência construída na rotina de trabalho pelo conhecimento objetivo sobre a ação criminal que brotaria a partir dos dados, de modo que o policiamento das grandes cidades se tornaria mais preciso, eficaz e justo (BECK & MCCUE, 2009).

No entanto, essa "epistemologia empirista" e o entusiasmo em torno da possibilidade de prever e se antecipar ao crime se baseiam em uma série de premissas problemáticas (KITCHIN, 2014), entre elas: (1) a ideia de que as bases de dados usadas para alimentar os algoritmos são capazes de capturar e descrever todas as dimensões do fenômeno que buscam analisar; (2) o argumento de que o conhecimento surge puramente a partir dos dados, dispensando qualquer tipo de teoria social sobre o crime, de modo que os dados "falariam por si sós"; e (3) uma percepção de que os métodos de análise transcenderiam o conhecimento especializado, o que permitiria a qualquer um tirar conclusões acuradas a partir de *dashboards* de visualizações de dados. Essas premissas emprestam uma imagem de objetividade às soluções de *big data* empregadas por forças policiais, negligenciando o fato de que os dados são eles próprios produzidos por ferramentas políticas (i.e., decorrem do que queremos e conseguimos compilar) (BOWKER & STAR, 2000). Como resume Završnik (2018, p. 5), "estatísticas são produzidas por humanos e para humanos".

Para discutir sobre o impacto de novas aplicações de *big data* no campo da segurança pública, esse artigo se divide em duas partes, além dessa introdução e de uma breve conclusão. Na próxima seção, apresento aplicações de *big data* que permitiram o desenvolvimento de duas tecnologias que têm sido alvo de largos investimentos pelas forças policiais, os sistemas de alerta para dinâmicas criminais e as ferramentas de policiamento preditivo. Em seguida, o artigo levanta alguns dos dilemas éticos que surgem ou se aprofundam com o uso de *big data* em ações de controle do crime, entre eles a automação de práticas discriminatórias e os riscos da vigilância intrusiva para a democracia.

2. Novas tecnologias e novas formas de policiamento

Nos últimos anos, diversas metrópoles brasileiras investiram na construção de centros de comando e controle, onde as forças policiais operam uma panóplia de sistemas de pronta-resposta e vigilância. Entre os dispositivos à disposição dos agentes estão câmeras que realizam cercamento eletrônico – capazes de identificar em tempo real placas de veículos e o rosto de indivíduos suspeitos – e softwares de mapeamento de ocorrências e análise criminal. Em conjunto, essas "soluções inteligentes" têm afetado estratégias de patrulhamento e ampliado os horizontes de políticas punitivas (PERON & ALVAREZ, 2021). Através de exemplos de casos concretos, esta seção aborda brevemente como o *big data* e a automação algorítmica têm prestado auxílio à atividade policial ao identificar áreas e alvos prioritários para o policiamento.[1]

Em 2014, o estado de São Paulo anunciou a implementação do *Detecta*, uma ferramenta de monitoramento que combinava circuitos de câmeras de vigilância, a busca em múltiplas bases de dados (incluindo registros de ocorrência, identificação civil, etc.) e a integração com os demais sistemas empregados pelas polícias do estado.[2] Inspirado no *Domain Awareness System* (DAS), plataforma de integração de dados, mapeamento criminal e videomonitoramento desenvolvido no departamento de polícia de Nova York, o *Detecta* tinha como objetivo principal disparar alertas automatizados para a polícia paulista ao identificar dinâmicas de interesse (EDLER et al., 2023).

1 Automação algorítmica se refere a sistemas capazes de realizar uma leitura da imagem em tempo real, identificando-a com padrões previamente classificados de interesse. A partir desse "reconhecimento" automatizado, um alerta é criado para anunciar a ocorrência de determinado evento para o usuário, como uma conduta suspeita praticada em um determinado perímetro de abrangência da câmera, a invasão desse perímetro, ou a identificação de objetos de interesse, como facas e armas de fogo.

2 Entre os múltiplos sistemas integrados ao *Detecta* estavam: Infocrim (1999), FotoCrim (2002), o COPOM Online (2002) e o Sistema Omega (2003).

Com a promessa de ser o "sistema nervoso" da polícia, o *Detecta* teve um custo aproximado de 28 milhões de reais.[3] O alto valor se justificava pela perspectiva de ganhos para a segurança pública, já que além de ser capaz de identificar veículos roubados e pessoas com pendências na justiça, o sistema permitia ainda o reconhecimento de "comportamentos suspeitos" que poderiam requerer atenção especial (e.g., indivíduos caminhando de capacete na calçada, motos com passageiros emparelhadas com carros, etc.). A expectativa era que, na medida em que mais crimes eram registrados pelas câmeras de segurança, o sistema se tornaria mais acurado para identificar as dinâmicas delituosas no estado, podendo reconhecer, por exemplo, abordagens suspeitas e a presença de armas de fogo. Além disso, a disseminação das câmeras no espaço urbano permitiria seguir o indivíduo suspeito durante sua movimentação, fornecendo informações preciosas para que a polícia realizasse a prisão. Como descreveu o então governador: "Antes, [o centro de operações] era um arquipélago isolado e agora integramos todos os bancos de dados das polícias civil, científica e militar. O sistema [*Detecta*] é um '*Big Data*' da polícia, extremamente eficiente" (SÃO PAULO, 2016).

Contudo, as promessas em torno dos ganhos operacionais proporcionados pelo *Detecta* não se confirmaram. Em poucos meses, uma auditoria do Tribunal de Contas do Estado (TCE) revelou que o sistema era pouco usado pela polícia, já que enfrentava dificuldades técnicas na integração com os demais sistemas da instituição (TCE, 2017). Além disso, os ganhos com alertas automatizados para atividades suspeitas foram em muito suplantados pelo problema dos "falsos positivos". O sistema gerava uma quantidade enorme de alertas que se mostravam infundados, o que sobrecarregava os operadores e, em muitos casos, atrapalhava a rotina de monitoramento urbano. Esse problema veio à público durante uma demonstração das funcionalidades do *Detecta* para jornalistas realizada pela secretaria de segurança. Na ocasião, o sistema gerou

3 Valor referente a contratos da PRODESP com a Microsoft e contratos da SSP para compra de equipamentos e prestação de serviços (TCE, 2017).

alerta para "veículo em situação suspeita" no caso de um carro supostamente estacionado em via expressa. Entretanto, após análise do operador, verificou-se que se tratava apenas da sombra de um poste na via (PAGNAN & BARBON, 2017). Segundo o TCE, disputas políticas pelo controle de dados entre as diferentes agências de segurança pública também impediram o fluxo de informações, o que limitou a capacidade de análise do sistema e gerou lentidão. Nesse cenário, o *Detecta* foi aos poucos caindo em desuso, sendo substituído, em 2024, pelo programa Muralha Paulista (PAGNAN, 2024).

As expectativas sobre os ganhos da automação algorítmica em dispositivos de vigilância são, em grande medida, reproduzidas nas análises acerca de ferramentas de policiamento preditivo. Segundo, Chris Sims, ex-comissário de polícia de West Midlands, no Reino Unido, a substituição do tirocínio policial por modelos matemáticos capazes de estimar a incidência futura de crimes e riscos de vitimização é a "a transformação mais radical que já aconteceu na polícia" (citado em DODD, 2014).

Até algumas décadas atrás, dificuldades técnicas se mostravam obstáculos formidáveis ao uso de mapas e abordagens estatísticas na análise criminal e na escolha de alocação de patrulhas (HAGGERTY, 2001). Em muitos países, dados criminais não eram coletados de forma sistemática e padronizada, o que dificultava análise com séries temporais mais amplas e com atenção às dinâmicas de microrregiões. Policiais trabalhavam, então, com bases incompletas e não dispunham de muitas formas para compensar o problema de subnotificação de crimes. Além disso, a produção de mapas requeria investimento de tempo, mão de obra e espaço (geralmente, paredes inteiras) para a visualização adequada da incidência criminal. No Brasil, até poucos anos, mapas de crimes eram representações em papel de áreas de atuação dos batalhões de polícia militar ou delegacias de polícia civil, onde crimes eram geolocalizados com alfinetes coloridos. Na medida em que mais crimes eram cometidos, a visualização de sua distribuição geográfica tornava-se confusa, dificultando a distinção de padrões e séries de eventos relacionados. A

análise de tendências também não era tarefa simples, já que mapas precisavam ser atualizados de tempos em tempos e informações sobre diferentes períodos só estavam disponíveis em fotos de arquivo (DE LIMA, 2005).

De fato, os sistemas modernos de análise criminal alteram radicalmente o cenário descrito acima. Atualmente, não apenas os registros de ocorrência são, em sua maioria, eletrônicos, o que alimenta automaticamente as bases de dados, mas as ferramentas de visualização são também mais adaptáveis às demandas da polícia, permitindo a seleção e análise de determinados territórios ou dinâmicas criminais. Indo além, os sistemas disponíveis no mercado são capazes de cruzar enormes volumes de dados, incluindo variáveis como: densidade populacional, dados censitários, localização de bares, escolas, parques, terrenos baldios, igrejas, áreas comerciais, pontos de ônibus, estações de metrô, tabelas de campeonatos esportivos, agenda de eventos empresariais e culturais, transações bancárias, uso de cartão de crédito, relatórios hospitalares, reservas de hotel, voos, pesquisas de internet, e-mails, redes sociais, ligações telefônicas e até fases da lua (ANDREJEVIC, 2017).

Se antes o policial identificava áreas de concentração de crimes e alocava as patrulhas de acordo, atualmente, a disponibilidade de dados mais granulares e avanços nas ferramentas de modelagem algorítmica permitem a identificação de novos padrões criminais, a ponto de muitos especialistas em segurança pública garantirem que suas dinâmicas futuras também podem ser decifradas. A promessa é que o policiamento ostensivo pode se antecipar a crimes específicos e em áreas específicas (e.g., roubos de celulares em determinada esquina e em determinada hora do dia), de modo que a simples presença policial serviria para dissuadir a ação delituosa. Assim, a polícia atuaria antes do crime, não com o objetivo de reprimir o criminoso, mas tornando o próprio cometimento do crime cada vez mais difícil.

À primeira vista, a implementação desses sistemas na rotina policial parece proporcionar avanços essenciais para a segurança pública. Contudo, o que tem sido verificado é um pouco diferente. Em primei-

ro lugar, não há consenso sobre os impactos positivos de sistemas de policiamento preditivo. Enquanto alguns desenvolvedores defendem que seus produtos são responsáveis pela queda de índices criminais (MOHLER, 2015), grande parte dos analistas aponta que, para instituições policiais que já fazem mapeamento de crimes, o policiamento preditivo não é "uma revolução que vai mudar tudo… mas um ganho incremental" (HOLLYWOOD, 2012). Além disso, pesquisas sobre a implementação de novos sistemas de análise criminal junto às forças de segurança indicam que, entre a prancheta do desenvolvedor e o uso da tecnologia na rotina operacional, há uma série de processos que podem impedir que o objetivo final seja cumprido. Em geral, policiais contestam, resistem, desvirtuam e adaptam os múltiplos sistemas que buscam automatizar seu trabalho e designar as áreas prioritárias de patrulhamento (MANNING, 2011). Por fim, críticos apontam que esses sistemas sofrem com vieses nas bases de dados usadas para seu treinamento. Quando os crimes registrados no passado são a chave para entender sua incidência futura, o que os sistemas fazem é reproduzir o padrão anterior de policiamento. Desse modo, se a polícia costuma reprimir com mais ímpeto crimes em determinada área ou costuma realizar abordagens e prisões de determinado grupo populacional, o que o sistema de análise vai aprender é que é preciso aumentar ainda mais o controle sobre esses mesmos territórios e indivíduos.

Defensores de aplicações de *big data* no campo da segurança pública reconhecem essas limitações, mas apontam que, mesmo como as distorções nas bases de dados, a automatização algorítmica seria ainda melhor do que as alterativas existentes. Como apontam Mayer-Schönberger & Cukier (2013, p. 112):

> com o uso do *big data*, esperamos identificar pessoas específicas em vez de grupos, o que nos liberta do problema da "culpa por associação", no caso do "perfilamento". Num mundo de *big data*, alguém com um nome árabe, que paga em dinheiro por uma passagem só de ida de primeira classe, talvez não esteja mais sujeito a uma minuciosa investigação no ae-

> roporto se outros dados específicos determinarem improvável se tratar de um terrorista. Com o *big data*, podemos escapar da camisa de força das identidades grupais e substituí-las por previsões mais granuladas para cada pessoa. A promessa do *big data* é continuar com a mesma prática – "perfilando" –, mas aperfeiçoada, de forma menos discriminatória e mais individualizada.

As vantagens operacionais advindas de novas aplicações de *big data* não podem ser ignoradas, mas o que se viu com os exemplos acima é que precisamos entender os problemas que elas podem acarretar, especialmente no que tange à supervisão da ação policial e ao seu impacto em populações vulnerabilizadas. Na medida em que aumentam as capacidades das forças de segurança de vigiar e se antecipar a ações criminosas, aumentam também os riscos de usos indevidos das novas tecnologias. E é sobre esses desafios que a próxima seção vai se debruçar.

3. Dilemas éticos e desafios regulatórios no uso de *big data* no campo da segurança pública

Existe alguma forma justa de se atuar sobre um crime que não aconteceu? Quais são os dilemas éticos de realizar perfilamento de risco de reincidência criminal para manter determinada pessoa presa em regime fechado? Os ganhos na capacidade de vigilância e controle a partir de sistemas de reconhecimento facial e identificação de padrões de comportamentos suspeitos são proporcionais ao desafio da violência urbana? Como podemos garantir que essas ferramentas são usadas dentro de limites aceitáveis, evitando, por exemplo, o monitoramento de manifestações pacíficas, a vigilância de adversários políticos ou mesmo o uso dos sistemas de coleta de dados para fins privados (e.g., policiais que usam as câmeras para flagrar traições matrimoniais)? Quando pensamos nos ganhos operacionais das aplicações de *big data*, não podemos negligenciar que as novas ferramentas disponibilizadas para as forças de segurança expandem enormemente sua capacidade de controle, poden-

do interferir nas regras do jogo democrático e nas nossas percepções de liberdade e privacidade.

Não por acaso, muitas das aplicações descritas acima têm sido acompanhadas de críticas relevantes da parte de pesquisadores e membros da sociedade civil. Por um lado, alguns especialistas apontam que muitas das promessas que cercam as tecnologias não se cumprem no mundo real. A adoção de novos dispositivos tecnológicos é sempre mediada pelas diferentes percepções sobre seus efeitos, o que leva policiais a resistir ou se adaptar às novas ferramentas. Mesmo inovações aparentemente simples, como a troca de plataformas de despacho de viaturas, se provam, com frequência, problemáticas, já que policiais tendem a rejeitar mudanças que aumentam a supervisão sobre seu trabalho ou demandem o desenvolvimento de novas habilidades profissionais (MANNING, 2011). Por outro lado, organizações da sociedade civil têm apontado que o processo de automação algorítmica, se não for implementado a partir de mecanismos participativos, transparentes e auditáveis, tende a se tornar simplesmente uma "atualização *high-tech* para o velho e conhecido racismo que está na base do sistema de justiça criminal" (NUNES, 2019). Diversas pesquisas corroboram essa crítica, apontando que sistemas de monitoramento biométrico e de análise da distribuição espacial do crime, por exemplo, carregam vieses que causam erros de identificação de elementos suspeitos e distorções no mapeamento de áreas de risco (FERGUSON, 2017).

Mais especificamente, críticos têm levantado graves alertas para os riscos de aprofundamento dos padrões discriminatórios da ação policial. Sistemas de policiamento preditivo, por exemplo, automatizam formas de classificar, mensurar e visualizar o fenômeno criminal. Estes, portanto, codificam e reproduzem escolhas de patrulhamento, como áreas de baseamento, perfis de suspeitos a serem abordados e crimes prioritários que devem ser registrados e reprimidos. Como lembra Jefferson (2018, p. 2), "estatísticas criminais moldam os mapas de crimes futuros e…, de forma recíproca, os mapas legitimam as estatísticas", já que os policiais tendem a realizar as prisões em flagrante nas

áreas para as quais foram designados pelos sistemas preditivos. Ou seja, o uso de tecnologias preditivas empresta uma "autoridade algorítmica" à ação policial (GILLESPIE, 2014), negligenciando que as representações do crime carregam vieses de origem, como repressão desproporcional de populações marginalizadas, e que táticas de patrulhamento proativo guardam estreita relação com formas punitivas de governo (ZEDNER, 2007). Contudo, os problemas inerentes às análises criminais preditivas não precisam implicar necessariamente no seu abandono. Se elas trazem conhecimento sobre riscos de criminalização e vitimização, elas podem informar políticas públicas preventivas que não passem pela repressão policial antecipada. Como apontam Edler e Lobato (2021, p. 91):

> softwares preditivos poderiam apoiar a retomada de um debate mais amplo sobre as causas sociais do crime, ajudando a guiar investimentos em equipamentos públicos, assistência social, melhorias em serviços básicos e inserção de jovens no mercado de trabalho. Ao invés de contribuir para a criminalização de populações já marginalizadas, [a previsão de crimes] poderia então servir como um diagnóstico de onde o Estado tem sido incapaz de fomentar o desenvolvimento. Nesse sentido, áreas onde há maior risco de crimes não seriam os alvos de mais patrulhas, mas sim de mais atenção aos fatores subjacentes do crime, suas causas menos imediatas e, por isso, mais difíceis de solucionar.

No caso dos sistemas de monitoramento biométrico e alertas automatizados de comportamentos suspeitos, o desafio de reposicionar as soluções tecnológicas para fins não punitivos é mais difícil de contornar. Os investimentos recentes em videomonitoramento nas grandes cidades têm criado redes de vigilância que capturam informações privadas de todos os cidadãos. Embora, as forças de segurança aleguem que monitoram apenas indivíduos com pendências na justiça e suspeitos de envolvimento com crimes, nossa capacidade de supervisionar a atividade policial é extremamente limitada e as instituições atuam, muitas vezes, à revelia de decisões do Ministério Público e de determinações

legais (MENDONÇA, 2025). Além disso, pesquisas confirmam que o risco de vigilantismo não deve ser minimizado, tendo documentado casos de policiais que usam esses sistemas para fins voyeurísticos, para perseguir adversários políticos e, inclusive, para vender informações ao crime organizado (CARDOSO, 2015; EDLER & CEIA, 2023).

Enquanto os usos de ferramentas de monitoramento eram voltados ao serviço investigativo e ocorriam após autorizações judiciais, era possível limitá-los à obtenção de evidências e pistas que pudessem ajudar na resolução de crimes. Já o emprego da vigilância algorítmica no policiamento ostensivo e preventivo pode torná-la uma "ferramenta irresistível de opressão e uma máquina de destruição total de privacidade perfeitamente adequada para governos que exercem controle autoritário sem precedentes" (HARTZOG & SELINGER, 2018). De fato, a disseminação de câmeras de vigilância biométrica nas grandes cidades faz com que nossos hábitos, movimentações e interações possam ser documentados e catalogados sem qualquer esforço operacional. Basta fazer uma pesquisa em um banco de dados para ter acesso a todas as imagens em que determinado indivíduo aparece. Em questão de segundos, a polícia pode descobrir, por exemplo, todas as vezes em que uma pessoa foi a um bar, visitou amigos, chegou atrasada no trabalho, frequentou uma casa de prostituição, fumou na calçada, participou de reuniões dos alcóolicos anônimos ou se fantasiou de *Pikachu* no carnaval. Ou seja, a vigilância algorítmica carrega um potencial de controle ubíquo que pode transformar a natureza das interações sociais e constranger comportamentos individuais, sejam esses ilegais ou não.

4. Conclusão

"*Raw data is an oxymoron*" (GITELMAN, 2013)

Analisar os impactos políticos e sociais das múltiplas aplicações de *big data* para o campo de controle do crime é um importante antídoto ao otimismo exagerado que costuma cercar as inovações tecno-

lógicas na segurança pública. Assimilar de forma acrítica o discurso "tecno-solucionista" dos desenvolvedores de sistemas de vigilância biométrica ou policiamento preditivo (MOROZOV, 2013), por exemplo, pode levar não apenas a frustrações com seu real impacto na rotina policial, mas também pode esconder muitos de seus efeitos deletérios, como a adoção de padrões desiguais de policiamento em bairros pobres e um monitoramento mais intrusivo da população negra.

Lisa Gitelman (2013) nos lembra que não existem dados puros que refletem a realidade de determinado fenômeno social. Os dados não são recursos naturais, mas produções sociais, culturais e políticas que se moldam a partir de nossos valores e interesses. No campo da segurança pública e da justiça criminal, isso implica em uma série de desafios, como, por exemplo, como lidar com as cifras ocultas de crimes ou com a sobrerrepresentação de determinadas populações nas bases de suspeitos das polícias. Como vimos, o *big data* pode aumentar nossa compreensão sobre as dinâmicas criminais e melhorar a eficácia das forças de segurança, reduzindo a violência urbana. No entanto, o desenvolvimento de novas ferramentas deve vir acompanhado de regulação adequada, com mecanismos efetivos de supervisão e transparência.

Referências

ANDERSON, Chris. The End of Theory: The Data Deluge Makes the Scientific Method Obsolete. **Wired**, 23 de junho de 2008. Disponível em: https://www.wired.com/2008/06/pb-theory

ANDREJEVIC, Mark. To Pre-Empt A Thief. **International Journal of Communication**, v. 11, p. 879-896, 2017.

BECK, C., McCUE, C. Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession? **The Police Chief**, 26(11), p. 18-25, 2009.

BOWKER, G., STAR, S. **Sorting Things Out:** Classification and Its Consequences. Cambridge, MA: The MIT Press, 2000.

CARDOSO, B. **Todos os Olhos:** Videovigilâncias, Voyeurismo e (re)produção Imagética. Rio de Janeiro: Editora UFRJ, 2015.

DE LIMA, R. S. (2005) **Contando crimes e criminosos em São Paulo:** Uma sociologia das estatísticas produzidas e utilizadas entre 1871 e 2000. Tese de Doutorado, FFLCH/USP, 2005.

DODD, V. Police force spends £25m on switch to technology-led crime-fighting. **The Guardian**, 21 de julho de 2014. Disponível em: https://www.theguardian.com/uk-news/2014/jul/21/west-midlands-police-technology-led-crime-fighting

DODD, V. Met gangs matrix may be discriminatory, review finds. **The Guardian**, 21 de dezembro de 2018. Disponível em: https://www.theguardian.com/uk-news/2018/dec/21/metropolitan-police-gangs-matrix-review-london-mayor-discriminatory

DOMINGOS, P. **The Master Algorithm:** How the Quest for the Ultimate Learning Machine Will Remake Our World. New York, NY: Basic Books, 2015.

EDLER, D., Lobato, L. A política do policiamento preditivo: pressupostos criminológicos, técnicas algorítmicas e estratégias punitivas. **Revista Brasileira de Ciências Criminais**, 29(183), p. 57-98, 2021.

EDLER, D., CEIA, E. (eds.). *Tecnologia,* **Segurança e Direitos:** Os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Fundação Konrad Adenauer, 2023.

EDLER, D., SIMÕES-GOMES, L., PERON, A. **Nem uma "revolução digital", nem a distopia do controle total:** Os efeitos das inovações tecnológicas na polícia de São Paulo. Relatório de pesquisa, Instituto Igarapé e Universidade de Essex, 2023.

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

FRY, H. **Hello World:** Being Human in the Age of Algorithms. New York, NY: W. W. Norton & Company, 2019.

GILLESPIE, T. The Relevance of Algorithms. In: GILLESPIE, T., BOCZKOWSKI, P., FOOT, K. (eds.). **Media Technologies:** Essays on Communication, Materiality, and Society. Cambridge, MA: MIT Press, p. 167-194, 2014.

GITELMAN, L. (ed.). **"Raw data" is an oxymoron**. Cambridge, MA.: MIT Press, 2013.

HAGGERTY, K. **Making Crime Count**. Toronto: University of Toronto Press, 2001.

HARTZOG, W., SELINGER, E. Facial Recognition Is the Perfect Tool for Oppression. **Medium**, 02 de Agosto de 2018. Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

HOLLYWOOD, J. **Predictive Policing:** What It Is, What It Isn't, and Where It Can Be Useful. Arlington, Va: RAND Corporation and National Institute of Justice, 2012.

JEFFERSON, B. **Predict and Surveil:** Data, Discretion, and the Future of Policing. New York, NY: Oxford University Press, 2020.

KITCHIN, R. Big Data, new epistemologies and paradigm shifts. **Big Data & Society**, 1(1), p. 1-12, 2014.

MANNING, P. **The Technology of Policing:** Crime Mapping, Information Technology, and the Rationality of Crime Control. Nova York, NYU Press, 2011.

MENDONÇA, J. Minoria dos promotores acha que fiscalizar a polícia é prioridade do Ministério Público. Agência Pública, 29 de abril de 2025. Disponível em: https://apublica.org/2025/04/minoria-dos-promotores-acha-que-fiscalizar-a-policia-e-prioridade-do-ministerio-publico/

MOHLER, G., Short, M., MALINOWSKI, S., JOHNSON, M., TITA, G., BERTOZZI, A., BRANTINGHAM, J. (2015) Randomized Controlled Field Trials of Predictive Policing. **Journal of American Statistical Association**, 110(512), p. 1399-1411, 2015.

MOROZOV, E. **To Save Everything, Click Here:** Technology, Solutionism, and the Urge to Fix Problems that Don't Exist. London: Allen Lane, 2013.

NUNES, P. Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. **The Intercept**, 21 de novembro de 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/

PAGNAN, R. Tarcísio apaga marca tucana Detecta do sistema de busca das polícias de SP. *Folha de São Paulo*, 30 de julho de 2024. Disponível em: https://www1.folha.uol.com.br/cotidiano/2024/07/tarcisio-apaga-marca-tucana-detecta-do-sistema-de-busca-das-policias-de-sp.shtml

PAGNAN, R., BARBON, J. Alckmin vai relançar sistema que já custou R$ 30 milhões e não funciona. **Folha de São Paulo**, 30 de junho de 2017. Disponível em: https://www1.folha.uol.com.br/cotidiano/2017/06/1897306-alckmin-vai-relancar-sistema-que-ja-custou-r-30-milhoes-e-nao-funciona.shtml

PERON, A., ALVAREZ, M. O Governo da Segurança: Modelos Securitários Transnacionais e Tecnologias de Vigilância na cidade de São Paulo. **Lua Nova**, no. 114, p. 175-212, 2021.

RYBERG, J., ROBERTS, J.V. (eds.) Sentencing and Artificial Intelligence. New York, NY: Oxford University Press, 2022.

SÃO PAULO. Sistema Detecta ganha 97 novas câmeras de monitoramento. **Governo do Estado de São Paulo**, 19 de outubro de 2016. Disponível em: https://www.youtube.com/watch?v=EDyAm64qDgc&ab_channel=GovernodoEstadodeS%C3%A3oPaulo

STATEWATCH. UK: Ministry of Justice secretly developing 'murder prediction' system. **Statewatch**, 08 de abril de 2025. Disponível em: https://www.statewatch.org/

news/2025/april/uk-ministry-of-justice-secretly-developing-murder-prediction-system/

TCE. **Relatório de Fiscalização de Natureza Operacional Solução de Consciência Situacional – DAS Detecta**. Tribunal de Contas do Estado de São Paulo, 2017. Disponível em: https://www.tce.sp.gov.br/sites/default/files/portal/detecta.pdf

WEISBURD, D. The law of crime concentration and the criminology of place. **Criminology**, 53(2), p. 133-157, 2015.

ZAVRŠNIK, A. (ed.). **Big Data, Crime and Social Control**. Abingdon and New York: Routledge, 2018.

ZEDNER, L. Pre-crime and post-criminology? **Theoretical Criminology**, 11(2), p. 261-281, 2007.

Daniel Edler Duarte é pesquisador associado do Instituto de Ciências Sociais da Universidade do Estado do Rio de Janeiro (ICS-UERJ) e do Núcleo de Estudos da Violência da Universidade de São Paulo (NEV/USP), além de membro da Comissão de Segurança Pública da OAB/SP. Daniel já trabalhou em diversas instituições, incluindo: Universidade de Glasgow, Universidade de Southampton, PUC-Rio e na Fundação Getulio Vargas. Sua pesquisa atual se desdobra em três eixos principais: (1) novas tecnologias e práticas de vigilância; (2) policiamento de protestos; e (3) controvérsias públicas no campo da ciência e tecnologia. E-mail: danieledler@usp.br