RELAC
REVISTA LATINO-AMERICANA DE CRIMINOLOGIA

Algoritmos e segurança pública: controle e vigilância no policiamento baseado em dados

Algorithms and public security: control and surveillance in data-based policing

Algoritmos y seguridad pública: control y vigilancia basados en datos

Rafael de Deus Garcia[1]
Universidade de Brasília
orcid.org/0000-0001-7985-521X

Rogério Bontempo Cândido Gontijo[2]
Universidade de Brasília
https://orcid.org/0000-0002-7789-3295

Resumo

O presente texto aborda os novos padrões adotados pela segurança pública, em especial no que se refere ao uso de novas tecnologias de processamento de dados (machine learning e algoritmos). Assim, o artigo aborda a expansão no uso de dados no policiamento, de modo a traçar possíveis estratégias de aplicação, o contexto em que se coloca a segurança pública na contemporaneidade e as fragilidades tanto das tecnologias de Big Data como da origem dos dados que as alimentam e da intersecção de tudo isso no complexo policial-penal. O avanço tecnológico pode não significar necessariamente aumento de qualidade do trabalho policial, podendo haver, ao contrário, atualização de instrumentos preventivos/repressivos a partir da exploração de intimidades por meio do uso massivo de dados pessoais.

Palavras-chave

Algoritmos – dados – segurança pública – policiamento

Abstract

This text addresses the new standards adopted by public security, especially with regard to the use of new data processing technologies (machine learning and algorithms). Thus, the article aims to understand the expansion in the use of data in policing, in order to address the application strategies, the context in which public security is placed today and the problems concerning Big Data technologies and the origin of the data to be used, in the context of the police-criminal system. Technological advances may not necessarily mean an increase in the quality of police work. On the

contrary, we may face an update of preventive / repressive instruments, based on the exploitation of intimacies through the massive use of personal data.
Keywords
Algorithms – data – public security – policing

Resumen

Este texto aborda los nuevos estándares adoptados por la seguridad pública, especialmente en lo que respecta al uso de nuevas tecnologías de procesamiento de datos (aprendizaje automático y algoritmos). Así, el artículo aborda la expansión en el uso de datos en la vigilancia policial, con el fin de abordar las estrategias de aplicación, el contexto en el que se ubica la seguridad pública hoy y las debilidades tanto de las tecnologías Big Data como del origen de los datos que y la intersección de todo esto en el complejo policial–criminal. Los avances tecnológicos pueden no significar necesariamente un aumento en la calidad del trabajo policial. Por el contrario, podemos enfrentarnos a una actualización de los instrumentos preventivos / represivos, basados en la explotación de intimidades mediante el uso masivo de datos personales.
Palabras clave
Algoritmos – datos – seguridad pública – vigilancia.

Sumário

Introdução

Em 2013, o americano Eric L. Loomis foi sentenciado por um juiz que embasou sua decisão em um algoritmo privado e de código fechado (COMPAS) de avaliação de risco[3], que classificou Eric como alguém com alto risco para reincidir. O resultado final foi uma pena de 6 anos por crimes relativamente leves, no caso, dirigir um carro que foi utilizado em um tiroteio e "iludir um policial"[4].

Eric recorreu à Corte estadual para reverter a decisão, alegando que houve violação ao devido processo legal, uma vez que o algoritmo, por ser fechado e ter suas configurações internas secretas, não podia ser examinado. O Estado de Wisconsin venceu Eric na disputa e a Corte Suprema dos Estados Unidos se negou a julgar sua demanda[5].

A discussão sobre o uso de algoritmos no sentenciamento – e no sistema de justiça criminal como um todo – está em pleno vigor nos Estados Unidos da América[6], e a academia científica[7] tem levantado questões, por exemplo, sobre racismo estrutural integrado a esses sistemas. Sobre essa problemática, o COMPAS foi auditado pela

ProPublica[8], portal jornalístico investigativo e independente, identificando que a classificação de risco sobre negros era muito superior a de brancos.

Com isso, vale questionar sobre como são desenvolvidos esses programas de análise de risco, sendo que, para tanto, o artigo de J. C. Oleson (2011) nos dá boas pistas.

Adotando o ponto de partida da prevenção especial[9] (OLESON, 2011, p. 1333), o autor sumariza 17 variáveis a serem consideradas para embasar os testes de risco de reincidência comumente empregados. Em ordem de relevância, essas variáveis são: 1) contato com criminosos, com base na teoria criminológica da associação diferencial; 2) comportamentos antissociais, tais como falta de valores para o trabalho e educação; 3) personalidade antissocial, como impulsividade, falta de autocontrole e capacidade reduzida de empatia; 4) antecedentes criminais; 5) raça, que considera o percentual acentuado de pessoas negras no sistema de justiça criminal; 6) comportamento antissocial na infância e juventude; 7) criação familiar, o que inclui a análise da família do avaliado; 8) realização social, relativo ao status social, nível educacional e emprego; 9) conflitos interpessoais, o que se refere à amplitude de amizades e ambiente familiar conflituoso; 10) idade, que pressupõe a maior disposição à reincidência a jovens entre 16 e 20 anos; 11) uso abusivo de entorpecentes; 12) estrutura familiar; 13) funcionalidade intelectual, como QI, capacidade de leitura e dificuldade de aprendizagem; 14) criminalidade na família; 15) gênero, pesando mais para o masculino na reincidência; 16) histórico socioeconômico; e 17) aflições pessoais, como a presença de transtornos psicológicos e doenças psiquiátricas.

Quanto à dificuldade de implementação desses instrumentos, o autor aponta para "entraves legais", alegação de violações a direitos constitucionais, resistência judicial, questões filosóficas e, ainda, problemas logísticos na coleta dos dados (OLESON, 2011, p. 1368).

Ainda assim, apesar das dificuldades, Oleson parece mostrar entusiasmo, indicando pontos positivos como (a) solução para recursos escassos do judiciário; (b) servir de alternativa a uma série de elementos que a lei obriga aos juízes a considerar no momento da sentença que simplesmente não conseguem; e (c) superioridade no julgamento atuarial/empírico em relação a um julgamento sem critério ou baseado em intuição (OLESON, 2011, p. 1393–4).

Por fim, o autor indica que o futuro nos dá três alternativas (OLESON, 2011, p. 1395): 1) adotar as técnicas atuariais, com utilização ampla das variáveis; 2) adotar as técnicas atuariais, com restrição ou eliminação dos critérios não objetivos ou que venham a ferir bases legais e filosóficas; e 3) rejeitar as técnicas atuariais.

A utilização de algoritmos para análise de quem passa – ou pode passar – pelo sistema de justiça criminal (SJC) parece inevitável, de modo que a terceira alternativa apontada por Oleson pode ser de pronto descartada. A primeira alternativa, por sua vez, parece implicar na aceitação tácita de uma arbitrariedade demasiadamente arriscada, especialmente no que concerne à adequação de princípios constitucionais e até morais. Nos resta questionar quais as medidas a serem tomadas na adoção de técnicas atuariais no SJC, o que nos exige uma compreensão de quais os principais desafios a serem enfrentados, além do entendimento básico de como se operam as máquinas e, talvez mais importante, em que racionalidade elas serão utilizadas.

Vale notar que muitos dos critérios apontados por Oleson são sobrepostos entre si, são de difícil ou impossível mensuração objetiva e carecem de qualquer filtro sobre a consideração racial e de gênero no sistema de justiça criminal. O *input*, isto é, todos os dados necessários para a análise do risco de reincidência pelos programas, se referem a questões pessoais muito profundas, adentrando todas as dimensões da privacidade do indivíduo.

A consideração de elementos subjetivos e morais – como "sociabilidade", "personalidade", "criação familiar", "valores para o trabalho" – se unem a elementos tipicamente clínicos – como "transtornos psicológicos", "doenças psiquiátricas", "funcionalidade intelectual", "impulsividade" – marcando a passagem de fronteira entre o diagnóstico clínico com o prognóstico atuarial[10]. Para complementar, os selos do SJC também pesam na conta, como "antecedentes criminais" e "criminalidade na família". Em síntese, a lógica atuarial não desconsidera a união de etiquetas atribuídas a pessoas que são de ordem moral, médico–clínica e criminal.

Juízes e policiais, no momento da tomada de decisões, são autorizados a valer–se de elementos subjetivos, seja na configuração do que consiste uma conduta suspeita, na atribuição do crime de tráfico de drogas ou de porte para uso pessoal, na primeira fase da dosimetria de uma pena, no deferimento de um pedido de progressão de regime etc[11]. Ocorre que os elementos de informação disponíveis à pessoa tomadora de

decisão são reduzidos, localizados e individualizados, e dependem essencialmente de cálculo humano.

Suponhamos que um sujeito seja parado pela polícia em atitude suspeita e agentes checam seu nome em um banco de dados que consta, quando muito, suas passagens pela polícia, antecedentes criminais, se há mandado de prisão em aberto etc. E se esse trabalho for ampliado? Em vez de um acesso a uma base de dados simples, o nome do suspeito é colocado em um programa que avalia seu "índice de risco"?

Pode–se argumentar que *softwares* de identificação de risco individual serão melhores do que o tirocínio policial[12]. Ao que tudo indica, no entanto, o tirocínio policial é um dos meios mediatos de produção dos dados que alimentam esses *softwares*, uma vez que representa uma das maiores portas de entrada para o SJC. Não podemos falar, portanto, de substituição, fazendo mais sentido utilizar termos como automatização ou aprofundamento.

A verdade é que não se pode subestimar a força de tirocínio policial na confecção do que consiste o perfil dominante de pessoas jurisdicionadas do SJC. Não pela sua eficácia real nem pelo seu rigor técnico, mas pela centralidade que possui na percepção policial sobre o que consiste ser o trabalho de polícia ostensiva. Isso porque o tirocínio policial tende a ser uma das principais fontes para produção de dados que serão utilizados nos *inputs* de máquinas atuariais.

A debilidade do controle externo da atividade policial, tanto do Ministério Público como do Judiciário, além da carência de balizas legais para precisão da fronteira da legalidade da atuação ostensiva, parece indicar um cenário em que a utilização de máquinas para suporte da polícia ostensiva não passará por crivos minimamente rigorosos. Nesse cenário do tirocínio policial como central na atividade policial está o problema das buscas e revistas pessoais.

Como coloca Gisela Aguiar:

> Essa execução da busca pessoal como medida de rotina do policiamento ostensivo formata um cenário de ilegalidades sistemáticas e prejuízos múltiplos. O uso generalizado e tendencialmente discriminatório da medida leva a violações cotidianas de direitos, reafirma estigmas conexos à suspeição policial (extrajurídica) e ainda pode reforçar a desconfiança mútua entre a sociedade e o aparato policial (AGUIAR, 2017, p. 272).

Com isso, falou-se da possível abrangência exacerbada dos *inputs* para cálculo automatizado e da potencialidade nociva de seu viés discriminatório. Além disso, falou-se da importância do tirocínio policial como possível fonte de dados para alimentar as máquinas e de como ele não será simplesmente substituído pela tomada de decisão automatizada, mas como são passíveis de integração mútua, servindo de atualização tecnológica das práticas policiais na definição de suspeitos e abordados.

Partindo dessas questões iniciais, o presente artigo busca compreender o problema da adesão de algoritmos e tecnologias de processamento de dados no âmbito da segurança pública. A metodologia utilizada foi a de revisão de bibliografia especializada, com foco na produção estrangeira sobre o tema devido à maior disseminação do debate nos Estados Unidos e Europa – em razão da implementação igualmente mais avançada dessas tecnologias nessas regiões.

O objetivo principal é responder às seguintes questões: como as tecnologias que operam sobre fluxo de dados pessoais podem assumir o papel de protagonismo crescente nas instituições penais, em especial, na polícia? Quais as principais problemáticas advindas dessa nova reconfiguração tecnológica da vigilância e do policiamento?

O primeiro tópico aborda as possíveis tendências de policiamento. A despeito do discurso de objetividade e neutralidade que a automatização de processos decisórios pode despertar, não se pode ignorar a fonte geradora dos dados que irão alimentar as máquinas. Além disso, há um jogo institucional a ser medido, no sentido de que uma política de segurança pública baseada em dados pode dinamizar e alterar o jogo de forças das instituições públicas e privadas que atuam direta ou indiretamente no sistema de justiça criminal.

No segundo tópico, trabalha-se com o conceito de sociedade de risco, e como a racionalidade orientadora da política criminal pode estar se aproximando ainda mais de uma lógica atuarial, mais focada não na prevenção criminal de crimes determinados e com vítimas, mas para vigilância, catalogação e perfilização de pessoas e grupos específicos.

No terceiro momento, o artigo busca explicações sistêmicas mais abrangentes para esse fenômeno, e como a exploração das intimidades no capitalismo de vigilância está no pano de fundo da nova configuração do sistema de justiça criminal.

1. Mudanças nas tendências de policiamento

Como colocam Ferguson e Logan, "hoje, o que prevalece como *zeitgeist* nos governos é a expansão dos bancos de dados, não de controle de qualidade ou de prestação de contas, e uma aceitação *blasé* de erro de dados e suas consequências negativas para os indivíduos" (FERGUSON e LOGAN, 2016, p. 543). No mesmo sentido, conforme Garland, vez que os crimes são encarados como acontecimentos "regulares, previsíveis, sistemáticos [...], recorre-se, hoje, às tecnologias de segurança e de supervisão, que guiam e mantêm as pessoas longe da tentação" (1999, p. 66). O avanço tecnológico, no entanto, por si só não pode ser compreendido como solução imediata para os problemas da criminalidade e da segurança pública, devendo ser tratado com sua devida complexidade.

Além disso, as instituições do sistema de justiça criminal tiveram suas prioridades alteradas nas últimas décadas, de modo que o controle do crime passa a ocupar novos campos e a ser pensado e executado mediante novas estratégias. Com essas mudanças, segundo Garland, "o Estado de justiça criminal está maior do que antes", vez que as agências e os sujeitos que o conformam transcenderam o espaço da soberania estatal. Dessa forma, o poder de polícia, atualmente, "ocupa um lugar relativamente menor no campo por causa do crescimento da segurança privada e das iniciativas comunitárias e comerciais organizadas" (2008, p. 374).

Assim, não se verifica uma substituição do "padrão crescentemente punitivo de sentenciamento", mas um movimento de simultaneidade entre este padrão e o estabelecimento de novas formas de controle e de policiamento. "O Estado, agora, opera numa economia mesclada de provisão de segurança e controle do crime e suas agências têm que se adaptar ao mercado de segurança privada que cresceu ao longo dos últimos trinta anos" (GARLAND, 2008, p. 374).

David Garland (2000) aponta para a emergência de dois modelos estratégicos no combate à criminalidade. Um modelo seria o da estratégia adaptativa (*adaptative strategy*) com enfoque em prevenção e parcerias preventivas (*preventive partnerships*), que se referem a uma série de arranjos de infraestruturas entre Estado e agências não estatais para aumentar segurança na comunidade a partir de diminuição de oportunidades criminais e expansão da consciência pessoal sobre o crime (*crime-consciousness*) (GARLAND, 2000, p. 349).

Esse modelo de parcerias preventivas estaria em ambivalência com o modelo de segregação punitiva (*punitive segregation*), cuja estratégia está relacionada à ideologia da defesa social a partir da resposta punitiva ampliada e com severidade no cumprimento de penas, o que se associaria ao superencarceramento.

No entanto, talvez seja um equívoco dispor esses modelos em oposição entre si. Embora seja de fato uma leitura possível no começo do século XX, a ascensão tecnológica pode, sem muita dificuldade, compatibilizar os dois modelos, ou, no mínimo, colocar um à disposição do outro.

Em uma sociedade de informação com relativa centralidade no trânsito e acúmulo de dados pessoais, o modelo repressivo penal pode se associar ao modelo de parcerias preventivas de natureza tecnológico–informacional. Assim, apesar da ausência de respostas eficazes no combate à criminalidade pelo modelo repressivo, ele não só continua em expansão como pode encontrar um aliado para preencher as lacunas que poderiam indicar seu esgotamento: o modelo de parcerias preventivas.

Além disso, ao se perceber que o fenômeno *crime* tem sido visto muito mais como uma manifestação da normalidade social – ainda que o discurso da "lei e ordem" siga implicando a demonização e patologização de certos tipos criminalizados, como no caso da criminalização das classes políticas, por exemplo – o sistema de justiça criminal, especialmente no que se convenciona chamar de braço da "segurança pública", acaba por elaborar uma tendência de gestão dos riscos da criminalidade (GARLAND, 1999).

Por isso, é dito que "países do ocidente têm respondido ao aumento dos níveis de medo e insegurança por meio do crescente discurso da 'nova prevenção', dando lugar ao que vem sendo chamado de virada preventiva"[13] (LUCIANETTI, 2011, p. 260). Igualmente, "o policiamento ficou mais 'esperto' [...], mais disposto a trabalhar com a comunidade e enfatizar a prevenção. Tecnologias de informação e as novas técnicas gerenciais se combinaram para produzir maior controle de recursos e condutas mais dirigidas" (GARLAND, 2008, pp. 367–8).

Além disso, é válido pontuar que o desenvolvimento das tecnologias não se dá exclusivamente no setor público, existindo razoável permeabilidade com as inovações e práticas do setor da segurança privada. Segundo Cleber da Silva Lopes (2011), o setor da segurança privada é bastante heterogêneo, e abarca alto grau de informalidade e carência de fiscalização, além de considerável integração de agentes públicos em

atividades privadas. No mesmo sentido, grandes empresas, como redes de supermercado e bancos, utilizam de tecnologias para garantir a segurança de suas atividades, valendo–se de alarmes, sensores metálicos e câmeras de vigilância (LOPES, 2020, p 215), que, tão logo, poderão estar na dianteira de um processo de sofisticação tecnológica.

A forma como se dará o fluxo de informação e de inovações entre o setor público e privado ainda é bastante incerta. A questão precípua, no entanto, é a natureza da coleta e da produção dos dados a serem utilizados para treinar a alimentar as máquinas.

Nesse sentido, é possível apontar que o modelo de parcerias preventivas, inseridas no âmbito tecnológico–informacional, não vai substituir o modelo de segregação punitiva e de encarceramento, mas, ao contrário, pode contribuir para engrandecimento das agências penais de controle. Isso afeta em especial a Polícia Militar, que, mais do que as demais forças policiais, têm à disposição um maior volume de dados operacionalizáveis, inclusive no momento da coleta e produção.

Powell (1990) nos apresenta distinções importantes sobre os modelos de organização, permitindo–nos progredir na análise da gestão da informação no âmbito da segurança pública. Há organização do tipo burocrática, hierárquica e de *network*. Dentre as mais importantes diferenças, pode–se destacar: enquanto na relação de mercado, a plataforma normativa está baseada em contratos e direitos autorais, e na hierárquica está na relação vertical de emprego, na de *network* está a de força complementar, destacando–se a forma de comunicação relacional. Se o tom das relações de mercado é pela suspeição e desconfiança, na hierárquica prevalece a formalidade, e na de *network* a de troca de benefícios, aberta e mais flexível. As diferenças podem ser pontuadas também quanto aos métodos de resolução de conflitos. Na organização de mercado o método é o negocial, na hierárquica é o formal–administrativo, e na de *network* o método é pela norma de reciprocidade, na preocupação de manutenção da reputação (POWELL, 1990, p. 303).

No modo organizacional de network, a alocação de recursos e a divisão de certas responsabilidades e benefícios não ocorrem por meio de relações formais contratuais ou de dependência funcional, mas por trocas discretas e não administrativas, de relações recíprocas e preferenciais, de ganho mútuo. Elas estão mais

relacionadas com a reputação e confiança conquistadas do que em uma relação fria determinada por um contrato específico. O vínculo criado se dá mais no âmbito pessoal do que formal, mais no da reputação e confiança do que no de obrigação contratual. Assim, quando o objetivo é, por exemplo, uma informação específica, o modo *network* prevalece, pois, sem formalidades e a partir de relações de mútuo interesse, é mais provável que dele venha uma informação segura e de fonte confiável. O modo *network* também prevalece quando a troca é de um bem ou valor não mensurável (ou de difícil medida) por preços, como *know–how*, um conhecimento específico sobre modos de produção, conhecimento de determinados serviços etc (POWELL, 1990, p. 303).

As polícias, incluindo–se órgãos internos como o setor de inteligência, podem funcionar bem na lógica de *network*, com gestão informal de informações, especialmente para reconhecimento de suspeitos. Embora a tecnocracia nos dê uma ideia de giro mecânico da lógica burocrática, a despeito – e por causa – da inovação tecnológica, na fase anterior ao flagrante, onde quase não há burocracia nem procedimento a ser seguido, o que impera é o dinamismo e a troca livre de informações, também baseada em *network* e confiança seletiva. Assim, a manutenção da condição estática da burocracia judicial é dependente dessa flexibilidade maximizada no ponto determinador da política criminal produzida na base. Como isso se opera?

Frequentemente, uma ação policial determinada, inclusive aquelas que resultam em morte, é justificada pelo argumento "repressão ao tráfico local", "área conhecida como ponto de vendas" etc. (FARIA, 2015, p. 77) (MISSE et al, 2015, p. 52). Havendo morte, há uma produção serial burocrática de enquadramento dos eventos ocorridos por meio de documentos como "autos de resistência" e "laudos periciais", passando pela normalidade institucional.

Segundo Maria Gorete de Jesus (2018), a compreensão de ordem e desordem pública passa por termos como "drogas", "medo", "desestabilidade familiar", "impunidade", "prisão" como sinônimo de "punição", "inibição", "retribuição", "descrença na Justiça" etc., o que compõe o léxico discursivo da "racionalidade penal moderna" (RPM) (PIRES, 2004), apta a justificar o agir policial e sua validação perante o Judiciário (DE JESUS, 2018, p. 187). A autora aponta ainda como a atuação policial na rua é "traduzida" à burocracia judicial, que, com ela, passa a estabelecer o status quo de combate à criminalidade. A autora indica também que termos como "fé pública", "*in*

dubio pro societate", "verdade real", servem enquanto categorias técnicas que "validam" judicialmente a política criminal de drogas.

Dessa forma, com essa lógica aliada ao funcionamento da instituição policial, é preciso manter abertos ao máximo os espaços passíveis de vácuo e opacidade, na medida em que o policiamento mais tecnológico pode aperfeiçoar–se e tornar a segregação menos escancarada e mais técnica. As novas tecnologias, a despeito de sua pretensa neutralidade, devem, portanto, ser aplicadas da forma mais transparente possível. Ainda que os métodos de policiamento tenham se diversificado, as políticas de vigilância estão em ampla expansão (GARLAND, 2008), e isso implica um descontrole institucional que já começa a deixar marcas e ditar os rumos para o futuro do controle.

Muitas vezes, porém, o debate vem na forma de eficiência vs. privacidade e essa forma de disposição já implica uma antinomia existente em seus formuladores. Partir dessa dicotomia parece até inevitável e, mesmo que se tente evitá–la, é inegável que ela já permeia a gramática comum do tema segurança pública. A própria Cathy O'Neil diz que o campo do direito e da política institucional possuem claramente uma orientação pró–justiça (*fairness*), valores juridicamente dispostos que se sobrepõem à eficiência punitiva (2016, p. 82), cuja lógica contraria a das *weapons of math destruction*, que tendem à eficiência.

Para Michael Rich, quanto maior acurácia se busca nos resultados de um algoritmo, mais ele ganha em complexidade e, portanto, perde em compreensibilidade humana, até mesmo para as próprias pessoas que o programaram (RICH, 2016, p. 886, 923). Por outro lado, no mesmo sentido, quanto mais fácil for auditar e interpretar o funcionamento de um algoritmo, mais ele apresenta a tendência de ser falho. Assim, a sociedade pode arcar com os custos de se exigir algoritmos interpretáveis, porém, o custo político de crimes não resolvidos ou criminosos não capturados tende a balança para o lado da aceitação da chamada *black box*, ou caixa preta[14] (RICH, 2016, p. 886). Ademais, "a tendência nas arenas da justiça criminal em direção ao sigilo nas estratégias de investigação da polícia sugere que os *algoritmos de automatização na definição da suspeição* provavelmente não serão transparentes ou interpretáveis"[15] (RICH, 2016, 911–2).

Em sentido diverso, para Zednik "opacidade é o coração do problema da caixa preta" (2019, p. 01). Em regra, as pessoas tendem a confiar menos e a conceder menos

controle a máquinas não compreendidas em seu funcionamento, e desenvolvedores podem encontrar mais dificuldades em corrigir problemas e em melhorar o sistema. Porém, o autor aponta que é sim possível garantir compreensibilidade a algoritmos complexos, mas que isso depende de um giro na formulação das perguntas a serem feitas. Zednik distingue "questões de que" (*what-questions*) e "questões de por que" (*why-questions*). Segundo o autor, enquanto se busca responder quais dados foram utilizados, qual o processo do sistema, quais são os *inputs* e *outputs*, pode-se afastar do mais importante: por que se chega em determinado resultado, e como interpretar as etapas em seu contexto e seus atributos.

Similar é a proposição de Coglianese e Lehr (2019), apontando a diferença entre transparência de aquário (*fishbowl transparancy*) e transparência fundamentada ou motivada (*reasoned transparency*). A primeira está associada à habilidade de o povo "olhar para dentro" do governo, bem como de adquirir informações sobre o que agentes têm feito. Em outras palavras, a transparência de aquário está mais associada à questão da publicidade e do acesso à informação. Por sua vez, "a transparência fundamentada enfatiza a utilidade das informações – isto é, se o governo revela por que agiu de determinada maneira. Enfatiza a importância de o governo explicar suas ações apresentando suas motivações"[16] (COGLIANESE e LEHR, 2019, p. 21).

Na medida em que algoritmos se referem a questões técnicas complicadíssimas e volume de dados enorme, transparência em inteligência artificial (IA) tem muito mais sentido quando relacionada à fundamentação, especialmente em matéria de segurança pública. É mais importante que o Estado, nas suas decisões, consiga justificar suas ações (COGLIANESE e LEHR, 2019). Não é que acesso a dados e a informação não seja também relevante, mas a transparência de aquário tende a significar muito pouco no que efetivamente significa transparência em processos decisórios baseados em IA quanto ao poder público. Em síntese, em matéria de segurança pública, transparência de aquário deve ser compreendida como complementar à transparência motivada.

A acurácia presumida no cálculo de algoritmos, bem como a naturalização do sigilo dos processos de tomada de decisão em matéria investigativa não parecem adequar-se bem aos princípios do Estado Democrático de Direito. Do contrário, um sistema aberto, que permitiria aos cidadãos avaliar e contribuir para a solução de erros em prol da sofisticação do sistema, parece mais adequado ao caráter democrático que

se busca. Além disso, o estudo (com o olhar voltado para políticas públicas) mostra o perigo da falta de transparência, na medida em que ela tem o efeito de esconder erros e fechar–se no tecnicismo inacessível, ganhando com isso confiabilidade de natureza mais emocional do que racional.

2. Segurança pública para uma sociedade de risco?

Segundo Ulrich Beck, em *Sociedade de risco*, na modernidade contemporânea – chamada por ele de "modernidade tardia" – ocorre uma mudança sistemática de produção e distribuição de riquezas para a lógica de distribuição de riscos. Isso se dá, segundo o autor, na medida em que o processo de modernização vem sendo marcado pela "*autêntica carência material*" da sociedade (BECK, 2011, p. 23).

No que concerne a essa modernização, Beck indica que se trata de um processo de reconfiguração da trama social a partir das novas tecnologias, das formas de trabalho, formas de poder e de concepção da realidade material (BECK, 2011, p. 23). Assim, "o processo de modernização torna–se '*reflexivo*', convertendo–se a si mesmo em tema e problema. [...] A promessa de segurança avança com os riscos e precisa ser [...] continuamente reforçada por meio de intervenções" (p. 24). Para o contexto criminal e para a segurança pública, essa noção é fundamental, vez que a sobrevivência do sistema se dá, muitas vezes, em razão dessa reflexividade entre as medidas necessárias para o controle do crime e o medo social que reforça a necessidade de sua aplicação cada vez mais profunda.

Nesse contexto, uma das teses de Beck sobre a sociedade de risco está ligada justamente ao *conhecimento*, que "adquire uma nova relevância política". Segundo ele, "o potencial político da sociedade de risco tem de se desdobrar e ser analisado numa sociologia e numa teoria do surgimento e da disseminação do *conhecimento sobre os riscos*" (BECK, 2011, p. 28). Conhecer os riscos, portanto, na sociedade atual é necessário do ponto de vista político para que eles sejam devidamente administrados e distribuídos.

Ademais, vale pontuar que nesse modelo de aliança capitalista–tecnológico da sociedade de risco, existe uma espécie de vácuo político diante da movimentação para resolução dos problemas advindos dos riscos. Tem–se, na verdade, "uma solidariedade ininteligível, correspondente à ininteligibilidade dos riscos, [de modo que] surge com

essa fissura um vácuo em termos de competência política e institucionalidade" (BECK, 2011, p. 58).

Entretanto, tal *vácuo* não significa inação do ponto de vista da resposta social aos riscos; o que não há é um projeto político concreto com fins preventivos e com a intenção de controlar e diminuir as ameaças sociais. Com efeito, desse vácuo floresce, como "contraprojeto normativo", o impulso pela segurança – conduzido pela solidarização social mediante o sentimento de medo. Assim, "o modelo da sociedade de risco marca, nesse sentido, uma época social na qual a *solidariedade por medo* emerge e torna–se uma força política" (BECK, 2011, p. 60).

Mediante essa orientação pelo medo e essa urgência por segurança que precisa se tornar concreta em meio ao vácuo político, surgem também os "bodes expiatórios" da sociedade de risco: comunistas, imigrantes, judeus, árabes, mulheres, traficantes, bandidos etc. As estratégias de ação nesse meio se conformam no sentido dos estigmas, isto é, elas "transformam os estereótipos sociais e os grupos por eles atingidos em verdadeiros 'pára–raios' para as ameaças que se mantêm invisíveis, inacessíveis à ação" (BECK, 2011, p. 93).

Tal tendência de segurança vigilante se dá num contexto em que a criminalidade violenta, o terrorismo e o tráfico de drogas inspiram medo e dão forma a um sentimento distópico, o que define, segundo Zaffaroni e Santos, "um modelo de *segurança sepulcral*". Nesse modelo, a segurança volta aos moldes medievais com "uma vigilância análoga à da infância e das mulheres no milênio da misoginia, através de uma tecnologia digital que conta com o acordo e a cooperação ativa dos próprios controlados" (ZAFFARONI; SANTOS, 2020, p. 132). Além da infantilização, a tendência da vigilância é também de se "feudalizar", já que as tecnologias empregadas no processo vigilância e controle da segurança estão ligadas a "uma rede de interesses que liga fortíssimas corporações transnacionais com polícias e agências (secretas) autonomizadas e corruptas" (ZAFFARONI; SANTOS, 2020, p. 133).

Outrossim, o conceito de risco tem origem nas companhias de seguro (ERICSON e HAGGERTY, 1997, p. 39), que não estão tão preocupadas com as fontes ou consequências morais das ações humanas, mas com a gestão de recursos a respeito das possibilidades que a elas se relacionam. Nesse sentido:

> Risco é uma invenção baseada em medos imaginados e em tecnologias imaginativas para se lidar com eles. (...). Transforma pessoas, suas organizações e seus ambientes em uma miríade de categorias e identidades para que fiquem mais gerenciáveis. Ele torna as pessoas e suas organizações mensuráveis em seus próprios sistemas de racionalidade internamente referenciadas, e não em termos de problemas e questões morais extrínsecas (ERICSON e HAGGERTY, 1997, p. 39).

As polícias, em uma sociedade de risco, no mesmo sentido, não estão preocupadas somente com as causas e consequências das ações imorais ou criminosas das pessoas, com o intuito de reprimi–las ou de neutralizá–las, mas também com a vigilância e antecipação dos riscos na sociedade com o intuito de melhor gerenciá–la.

O foco se dá sobre o conhecimento que permita a seleção dos limites daquilo que pode ser considerado um risco aceitável ou não na sociedade. Para Ericson e Haggerty, na sociedade de risco, o policiamento vai além das funções punitivas, repressivas e dissuasórias, sendo "também uma questão de vigilância, de se produzir conhecimento sobre as populações que seja útil para administrá–las" (ERICSON e HAGGERTY, 1997, p. 41).

A atividade policial não pode ser considerada apenas com base na diagramação organizacional padrão que lhe é atribuída. Ela não somente se restringe a responder às demandas individuais quanto à segurança pública, tampouco ao interesse coletivo de ordem pública, mas igualmente em relação às demandas institucionais de conhecimento dos riscos sociais.

> O policial produz e distribui comunicações, tecnologicamente mediadas e burocraticamente formatadas, para outras instituições de [gestão do] risco e, ao mesmo tempo, se aproveita do conhecimento já processado de outras instituições que o ajuda a cumprir as demandas de riscos da sua própria instituição (ERICSON e HAGGERTY, 1997, p. 45).

Com efeito, a polícia é parte de uma rede interinstitucional que determina e gerencia as políticas públicas de determinado campo. Por essa razão, é um equívoco afirmar que a polícia apenas atua sobre regras, procedimentos e modelos operacionais para fins exclusivos de ordem pública e contra o crime, pois que também atua determinando e contribuindo para o desenvolvimento de regras, tecnologias e modelos que transcendem a aparência da atividade policial, influenciando diretamente sobre outras instituições.

Na sociedade de risco, as instituições não se organizam com base em uma noção coesa de ordem, e a polícia tem se voltado mais para segurança geral, previsibilidade, perfilamento e vigilância do que propriamente para garantia da ordem e repressão individual. "O controle é mais bem simbolizado na manipulação do que na coerção, nos chips de computador do que nas barras da prisão, e nos filtros remotos e invisíveis do que nas algemas e camisas de força" (ERICSON e HAGGERTY, 1997, p. 41).

Nesse sentido, não parece ser na deficiência da política criminal ou na carência de resultados efetivos, ou ainda na ausência de justificativas racionais para o agir policial, que a "racionalidade penal moderna" (PIRES, 2004) encontra amparo para adesão das novas tecnologias. Ou seja, a inserção das tecnologias na política criminal não é fruto de uma demanda popular por justificativas de um poder que se vê abalado em sua legitimidade, mas justamente em uma resposta (ironicamente) automática à pretensão de uma burocracia estatal que se impõe como racional em detrimento da população, que crê haver na ação estatal medidas minimamente justificáveis, ainda que não expressadas. "A tecnologia orientada por dados oferece uma dupla vitória – faça mais com menos recursos e faça isso de maneira aparentemente objetiva e neutra" (FERGUSON, 2018, p. 12).

Sobre a adoção das tecnologias de dados na segurança pública e no controle e persecução criminal, Ferguson (2018, p. 12) aponta que, após inúmeros protestos a atrocidades cometidas por irresponsabilidades e abusos policiais contra vidas de pessoas negras nos Estados Unidos em várias cidades, o policiamento baseado em dados surgiu como resposta, sendo vendida como "objetivo", "neutro" e "livre de preconceitos". A nova tecnologia, então, passou a ser utilizada para justificar a velha atuação policial nas mesmas comunidades pobres. Entretanto, investigações sobre o uso dessas tecnologias tendem a encontrar viés preconceituoso (especialmente racial e territorial[17]) e grandes chances de violações aos direitos à privacidade nos sistemas de tratamento de dados por *Big Data*.

No mesmo sentido, como aponta Byfield (2018), é um equívoco até mesmo supor que as novas tecnologias (mineração de dados e algoritmos) poderão ser utilizadas para se encontrar novos padrões na ocorrência de crimes e então contribuir para a tomada de decisão. O problema reside no fato de que os dados digitais utilizados

para se buscar novos padrões não são novos, mas os mesmos dados utilizados em padrões de policiamento anteriores, e é sabido que algumas comunidades são muito mais policiadas que outras. "Assim, a abordagem 'preditiva' do policiamento provavelmente servirá para se associar ainda mais negritude com criminalidade, novamente com o uso de ciência *junk*, semelhante ao que foi feito no final do século XIX" (BYFIELD, 2018, p. 11).

O ponto central, portanto, pode ser sintetizado da seguinte maneira: se os dados que alimentam as bases são coletados e produzidos mediante instituições policiais que levam em consideração e replicam estigmas criminais ligados à raça, por exemplo, as decisões sugeridas mediante o processamento e cruzamento de dados reproduzirão esses vieses, que serão usados para intensificar a atuação seletiva das forças governamentais nesse sentido, num ciclo vicioso.

Nesse mesmo sentido, Beck aponta que a racionalidade objetiva da ciência ao tentar compreender os riscos é, por si mesma, refutável, haja vista que as especulações e conjecturas científicas tem lastro baseado em "*asserções probabilísticas*". Dessa forma, "ao ocuparem–se com riscos civilizacionais, as ciências sempre acabaram por abandonar sua base de lógica experimental, contraindo um casamento polígamo com a economia, a política e a ética" (BECK, 2011, p. 35).

Percebe–se também que essa tendência continua seguindo os rumos e as bases do positivismo criminológico, na medida em que se segue classificando indivíduos conforme suas "possibilidades de tratamento e fatores de risco" (GARLAND, 2008, p. 369), ainda que hoje esse fenômeno tome forma por meio do emprego e outras tecnologias, como é o caso dos algoritmos e do *machine learning*.

Com isso, no que se refere à criminologia positivista e à ânsia do direito penal em tornar–se objetivamente aplicável – e, consequentemente, ser visto mais como ciência do que como técnica jurídica – Cristina Rauter aponta que, a despeito da pretensão de descompromisso ideológico e neutralidade dos "instrumentos científicos", essas técnicas "reproduzem todos os estereótipos e preconceitos, em suma, toda a ideologia que permeia a questão do crime, traduzindo–se em prática de repressão, controle e disciplinarização das parcelas mais pobres da população" (RAUTER, 2003, p. 87).

> A criminologia, como a mais utilitária das ciências humanas, não pode propor um 'tratamento' do delinquente sem enfatizar a necessidade de 'vigilância', ou não pode falar de reforma social sem defender a repressão policial, ligada ao chamado combate ao crime. Contraditório, impreciso, desordenado, o discurso da criminologia não deixa de ter, entretanto, para o Judiciário, a função de dotá–lo de uma racionalidade científica, de transformar a função repressiva numa função técnica, fruto da 'neutra' observação dos fatos individuais e sociais (RAUTER, 2003, p. 75).

Com isso, assim como a criminologia positivista foi (e continua sendo) peça essencial para a legitimação e consolidação do sistema penal moderno, hoje, a Justiça – em razão de suas contradições e inconsistências entre realidade empírica e garantias legislativas de direitos – segue em busca de "instrumentos" que fundamentem e deem lastro científico as suas medidas e a sua atuação.

Rouvroy e Berns (2018) dizem que "o propósito daquilo que chamamos *machine learning* é, em resumo, tornar diretamente possível a produção de hipóteses a partir dos próprios dados", fazendo com que, dessa forma, se possa extrair um saber objetivo "absoluto" acerca das interações que compõem a sociabilidade humana. Assim, "afastado de toda intervenção subjetiva (de toda formulação de hipótese, de toda triagem entre o que é pertinente e o que seria somente ruído, etc.) [...] as normas parecem emergir diretamente do próprio real" (ROUVROY & BERNS, 2018, p. 113).

Ocorre que, segundo os próprios autores, a forma como se dá o estabelecimento dos dados pelos algoritmos não ocorre de maneira meramente correlacional, sendo necessário "evitar que as decisões que produzam efeitos jurídicos em relação a pessoas ou que as afetem de maneira significativa sejam tomadas somente com base no único fundamento de um tratamento de dados automatizado" (ROUVROY & BERNS, 2018, p. 113–4).

Não se pode, portanto, trabalhar o presente tema de forma ingênua a ponto de se crer na neutralidade de tais tecnologias. Em verdade, para que funcionem e tenham sentido na situação determinada em que serão empregados, instrumentos de *machine learning* devem, primeiro, passar por etapas de alimentação, pré–processamento e também de treinamento, no caso da inteligência artificial. Por mais que pareçam objetivas, racionais e apartadas de "interações ideológicas", essas tecnologias são frutos de interação humana e são alimentadas por dados advindos da sociedade, de modo que a não reprodução de vieses depende de esforço positivo nesse sentido.

Como já havia sugerido Bruno Cardoso sobre os sistemas de vigilância por câmeras e seus controladores, "o olhar e a percepção humanos não são meras formalidades" (CARDOSO, 2010, p. 45). Todo o aparato tecnológico, por si só, não é capaz de atribuir sentido à multidão de informações que chegam às centrais. Assim, "colocar ênfase excessiva nas inovações tecnológicas da revolução digital é incorrer no mesmo erro de sobredeterminação técnica que os paranoicos e os apologistas da videovigilância" (CARDOSO, 2010, p. 45). Afinal de contas, embora os meios técnicos sejam elementos culturais e sociais que influenciam e moldam a cultura humana, se valendo de estrutura de troca, são fatores culturais que dizem o que será trocado (CARDOSO, 2010, p. 45).

Dessa forma, “se a polícia concentrar a atenção em certos grupos étnicos e bairros, é provável que os registros policiais sistematicamente representem excessivamente esses grupos e bairros” (LUM e ISAAC, 2016, p. 15). Isso ocorre porque tais programas se utilizam dos dados advindos da criminalização anterior de grupos sociais específicos, o que contribui para a perpetuação de lógicas discriminatórias – porém, no caso, sob o disfarce da imparcialidade técnica dos algoritmos.

Nesse mesmo sentido, P. Jeffrey Brantingham afirma que

> [...] se pessoas não brancas são detidas e presas desproporcionalmente por crimes de drogas em relação à prevalência real, e se essas prisões são a base para previsões, então as previsões levarão a prisões mais desproporcionais. Resultados desiguais crescerão e, não surpreendentemente, as prisões subsequentes serão consistentemente confirmadas pelas previsões[18] (2018, p. 474).

Ademais, para compreender o uso de tecnologias da informação no sistema de justiça criminal, é preciso, antes, olhar para as dinâmicas estruturais do próprio sistema. Isto porque, conforme Zuboff, “as tecnologias são construídas por funcionalidades específicas, mas o desenvolvimento e a expressão dessas funcionalidades são moldados pelas lógicas institucionais nas quais as tecnologias são projetadas, implementadas e usadas” (2018, p. 56).

3. Capitalismo de vigilância e o uso político das intimidades

Para Shoshana Zuboff, vive–se na contemporaneidade um “capitalismo de vigilância”, no qual, por meio da informação, procura–se prever e interferir nas

interações humanas a fim de aperfeiçoar processos de acumulação e de controle de capital (ZUBOFF, 2018).

No mundo do *Big Data*, a colaboração ativa das pessoas é fundamental, e há incentivos psicológicos muito fortes, nauseantes, como coloca Zuboff, para impedir a resistência. Além da conveniência permitida pelo consumo personalizado, a rastreabilidade permanente e a produção de dados aptos à mineração passam a ser naturalizadas no cotidiano – quando não enaltecidos (ZUBOFF, 2015, p. 84).

A acumulação de dados se insere como lubrificante na lógica capitalista de acumulação de bens, e a sociedade adere a vigilância como ingrediente de cultura, não perdendo sua vinculação com o mercado participativo ativo (ZUBOFF, 2015, p. 77). A possibilidade de mediação da segurança pública por meio de algoritmos alimentados por dados cria novas mentalidades e práticas de vigilância, fazendo superar o papel de espectador do cidadão, tornando–o ativo e consciente (LYON, 2018, p. 159).

O consumo se alinha à produção de dados pessoais, cuja emissão é tolerada em troca de conveniências como serviços personalizados. A conformidade é um desejo constante, e hoje ela não mais aquela do século XX em que um indivíduo se submete a um grupo ou à massa em detrimento de sua personalidade, dirigida pelo medo, compulsão ou desejo de pertencimento. "A conformidade agora desaparece na ordem mecânica das coisas e dos corpos, não por ação, mas por resultado, é efeito, não causa" (ZUBOFF, 2015, p. 82).

É o comportamento humano, com a exploração da vida privada, que passa a estar no centro do poder, e não mais a propriedade e os meios de produção (ZUBOFF, 2015, p. 82). Não é por acaso o tamanho das empresas de tecnologias e sua imensa penetrabilidade social. Cada pessoa pode seguir com suas próprias escolhas, mas elas já podem ser limitadas por quem tem o poder de adentrar cada aspecto do eu (ZUBOFF, 2015, p. 82).

Sofiya Noble traz mais luz aos perigos da adesão às novas tecnologias que exploram dados pessoais. Aponta que “há vários casos que demonstram como racismo e machismo são parte da arquitetura e linguagem da tecnologia, uma questão que precisa de atenção e remediação” (NOBLE, 2018, p. 21)[19].

A pesquisa de Noble tem por objeto alguns casos que ilustram como as plataformas baseadas em algoritmos não somente são alimentadas por dados já

enviesados como elas próprias passam a "fornecer informações deletérias sobre as pessoas, criando e normalizando isolamento estrutural e sistêmico, ou praticando redefinição digital, que de todo modo reforça relações sociais e econômicas opressivas" (NOBLE, 2018, p. 22)[20].

A autora identifica uma alteração na dinâmica das comunidades. Isso se deve ao fato de que a própria existência de uma pessoa, ou seu empreendimento e sua relação com as outras pessoas e comunidade, passa a ser definida e percebida pelo mundo na medida de quais e como os dados sobre elas são processados. A autora argumenta que "o ambiente político e econômico neoliberal lucrou tremendamente com a desinformação e descaracterização das comunidades, com uma variedade de consequências para os que dentre nós são mais desprovidos de privilégios e marginalizados"[21] (NOBLE, 2018, p. 187).

A discussão trazida por Noble é relevante porque evidencia a importância da interação e do julgamento humano na formulação e na utilização dos algoritmos. Falar em algoritmos de inteligência artificial, *machine learning* etc, é falar de automatização de processos decisórios. Além disso, é falar de automatização de processos decisórios a partir de dados pessoais produzidos no âmbito das intimidades, mas que transcendem o aspecto individual, se referindo também às diferentes coletividades que o mundo mediado por dados permite existir.

A matemática Cathy O'Neil sustenta que as ferramentas e técnicas de combate ao terrorismo estão sendo aderidas às políticas de policiamento a tal ponto que o modelo de abordagem e revista (*stops and frisks*) passará a ser compreendido como primitivo (2016, p. 86). No entanto, a autora sugere que essas mesmas abordagens, com foco especial nos comportamentos entendidos como antissociais, serão utilizados não como ferramenta para desvendar, especialmente pelo acaso, crimes, mas sim como fonte de dados para os sistemas informáticos de policiamento.

Se a fonte primária de dados – isto é, a origem do dado a ser computadorizado para então ser submetido à análise de uma máquina – parte majoritariamente do tirocínio do policial de rua que atua mediante seu "faro" ou "instinto", não é trivial o estudo do policiamento ostensivo.

Os sistemas de *mass surveillance* (vigilância em massa), como as tecnologias de reconhecimento facial, não necessariamente tornam a polícia mais atuante nas diversas

demandas de combate à criminalidade, mas definitivamente ampliam o seu poder de escolha sobre quais comportamentos deseja reprimir e, mais importante, catalogar.

Para O'Neil, os cientistas de dados da segurança pública estão transformando o *status quo* da ordem social, tal como compreendida pelo policiamento ostensivo, em modelos para os programas informáticos, naquilo que ela chama de *do–it–yourself WMD* (*weapons of math destruction*)[22] (O'NEIL, 2016, p. 79). Um dos pontos centrais dessa questão é que os sistemas são calibrados para se alcançar determinados objetivos: "cada modelo de combate à criminalidade demanda um certo tipo de dados na entrada, seguido por uma série de respostas, calibrados para alcançar seus respectivos objetivos"[23] (O'NEIL, 2016, p. 77). E a polícia que gera os dados elementares do que depois vai alimentar os bancos de dados usados nas tecnologias preditivas ou de decisão automatizada.

Desse modo, segundo O'Neil:

> Isso cria um ciclo de *feedback* pernicioso. O próprio policiamento gera novos dados, que justificam mais policiamento. E nossas prisões se enchem com centenas de milhares de pessoas consideradas culpadas de crimes sem vítimas. A maioria deles vem de bairros pobres e a maioria é negra ou hispânica. Portanto, mesmo que um modelo não faça distinção de cor, seu resultado não mostrará outra coisa além disso. Em nossas cidades amplamente segregadas, a geografia é um *proxy* [condicionante] altamente eficaz para a raça[24] (O'NEIL, 2016, p. 76).

Isso se explica em parte no fato de que os sistemas de vigilância em massa tendem para uma abordagem em volume populacional, com processamento de imensa quantidade de dados pessoais, diferentemente do que ocorre em uma investigação pontual de um fato criminoso já ocorrido, típico das polícias judiciárias. Em outras palavras, os sistemas de predição ou de identificação de suspeitos parecem estar mais inseridos na lógica de flagrante esperado[25] do que na lógica de investigação que sucede o fato incriminável. Assim, não é que a centralidade política das PMs em detrimento das polícias civis determina a política em segurança pública, mas o próprio modelo de policiamento que exsurge com as tecnologias parece pender mais para o lado do policiamento ostensivo.

A lógica é que, com a exploração das intimidades, as respostas e os panoramas preditivos sejam menos relacionados a juízos quanto à prática de crimes de homicídio, roubo ou qualquer outro crime com vítima definida, do que quanto à antecipação de

agentes do Estado a sujeitos que tenham praticado condutas referentes a atos preparatórios de crimes, condutas anti sociais associadas à criminalidade, comércio ilícito, crimes de associação etc, afinal, as tecnologias trabalham justamente sobre probabilidades e padrões a partir de perfis e categorias estabelecidas.

A vigilância nos moldes atuais "não consiste na velha *fichagem* policial", de modo que "o controle totalitário foi aperfeiçoado com alto grau de tecnologia de vigilância e manipulação, cuja sofisticação avança a passos largos" (ZAFFARONI e SANTOS, 2020, p. 131). Assim, o uso massivo de dados por serviços de inteligência e corporações multinacionais "rompe as fronteiras entre espionagem, guerra e controle da própria população" (ZAFFARONI e SANTOS, 2020, p. 134).

No mercado da segurança pública, portanto, a capitalização dos anseios sociais é fundamental para que sejam criadas respostas, ainda que ineficientes do ponto de vista estrutural, à criminalidade. O capitalismo de vigilância focaliza o medo social do criminoso e do terrorista, e oferece instrumentos para que se possa prever ou controlar o fenômeno criminal. Isso se dá, contudo, de modo a reforçar a seletividade do sistema punitivo – mediante a racionalização de dados racistas, por exemplo – e a ampliar a perda de direitos e garantias fundamentais.

Considerações finais

O paradigmático caso de Eric L. Loomis, sentenciado com auxílio de um sistema de avaliação de risco, é sem dúvida capaz de ilustrar o potencial discriminatório da utilização das novas tecnologias nos sistemas de justiça criminal. Porém, é apenas um retrato de desfecho, e, portanto, um retrato parcial e superficial do problema sobre o qual se erige. Assim como a decisão de um juiz somente se realiza após uma série de decisões anteriores de agentes da segurança, os cálculos baseados em dados para avaliação pessoal de risco na definição de uma pena dependem de um longo percurso de informações prévias geridas no contexto do policiamento, especialmente o ostensivo.

O policiamento baseado em dados tem o poder de ampliar a atuação policial no nível extra e pré–judicial. É possível a criação de um conjunto de medidas e práticas que deixam à disposição da política um complexo sistema de controle social com imensa capilaridade social. O controle judicial desse submundo de medidas e práticas fica

condicionado, antes, ao poder discricionário da decisão policial, que leva ao judiciário apenas o resultado da informação tratada, isto é, da seletividade estruturada na percepção dos estigmas do sistema penal.

A propósito, adotar a tese de que vivemos em uma sociedade de risco pode permitir a conclusão de que um policiamento baseado no risco seja justificável, e de que uma vigilância focada no processamento de dados seja o caminho de adaptação não somente natural, mas necessário para dar cabo das demandas crescentes por segurança e prevenção criminal. Isto é inclusive fortificado pela onda populista penal e pela ideia salvacionista apregoada às novas tecnologias. Logo, o terreno encontra-se fértil para que o medo crescente da população seja alimentado e utilizado como capital político para justificar e legitimar a ampliação do alcance do estado de polícia por meio, agora, desse novo "agente": o *Big Data*. Porém, partindo-se da epistemologia garantista, pensando-se um direito penal para fins de resguardo dos direitos fundamentais em detrimento da ampliação do Estado de Polícia, pensar o policiamento a partir do risco pode ser um caminho perverso em direção ao emergencialismo penal.

O emergencialismo penal – outrora justificado a partir da exploração discursiva do terrorismo, do crime organizado ou da guerra às drogas – pode passar a prescindir de justificativas explícitas e até mesmo implícitas. A razão para isso é de que o policiamento baseado em dados, em processos tecnológicos pouco ou nada transparentes (até mesmo para os próprios burocratas), em cima de informações (pouco ou nada confiáveis) produzidas e tratadas pelo Estado e empresas, no contexto de prevalência institucional das polícias militares no âmbito da segurança pública (inclusive em detrimento do próprio Judiciário) pode representar em si próprio a lógica emergencial, rifando ainda mais as possibilidades de resistência institucional.

Ferrajoli sustenta a tese de que o princípio da razão de Estado, em que há prevalência do emergencialismo em detrimento de um direito penal utilitário para fins de contenção e racionalização do poder punitivo, é incompatível com o Estado democrático de direito, uma vez que o subsistema penal de exceção condiciona as formas de justiça e orienta um processo penal concreto. Esse processo penal não é mais balizado pela legalidade jurisdicional, mas determinado pelo arbítrio policialesco, repressão política e de regressão neoabsolutista (FERRAJOLI, 2014, p. 751).

Isso talvez ajude a explicar a tendência de as tipificações legais se darem cada vez mais sobre condutas que atingem bens jurídicos abstratos, de caráter presumido, sem necessidade de uma direta lesão a algo ou alguém. A questão é que o direito penal e o sistema de justiça criminal estão mais preocupados com a gestão do risco do que exatamente com a proteção ou reparação de um bem jurídico específico.

Ou seja, em meio aos riscos contemporâneos e ao "caráter inseguro e arriscado das relações sociais e econômicas atuais", tem–se uma maior propensão ao controle, à "obsessão por monitorar pessoas temíveis, isolar populações perigosas e impor controles situacionais em contextos outrora abertos e fluidos" (GARLAND, 2008, pp. 414–5). O controle, então, toma novos contornos e novas amplitudes, de modo que, cada vez mais, passa a fazer parte do cotidiano a ideia de uma segurança diária, constante e sobre todos. O medo nos permite abrir mão de parcela dos direitos fundamentais, como é o caso do direito à privacidade, a fim de que nos sintamos mais seguros e a sociedade mais controlada.

Nesse sentido, um próspero mercado de serviços focados na promoção de formas de segurança surge para lidar com as demandas de controle, prevenção e previsão dos riscos sociais – "porque o velho Estado soberano pode prover punição mas não segurança, e isto se tornou visível para os atores econômicos que têm interesses reais no processo" (GARLAND, 2008, p. 423). Esse mercado se diversifica e se amplia na medida em que suas possibilidades e seu alcance podem ser aperfeiçoados pelas tecnologias de processamento de dados. É exatamente isso que vem ocorrendo, portanto, no cenário atual: uma expansão do controle e do estado de polícia por meio das tecnologias de vigilância e de algoritmos capazes de ressignificar quantidades massivas de informações.

Dessa forma, o sentimento de segurança social perante os riscos relacionados à criminalidade e à criminalização toma novas proporções, "tornando a aplicação da lei não mais um fim em si mesmo, mas meramente um meio para alcançar tal fim. Redução do medo, redução de perdas e danos e controle de custos se transformam em considerações proeminentes" (GARLAND, 2008, p. 371). Mais ou menos autoritária, essa cultura do controle invariavelmente vulnera direito e garantias dos cidadãos, enquanto propicia uma falsa resposta de cunho populista a questões sociais que têm reflexo na criminalidade, mas que só podem ser resolvidas mediante o desenvolvimento

de políticas estruturais e, de modo geral, a longo prazo. Ainda que haja ampla vigilância e predição de crimes, a ausência de justiça social não permite que uma radicalidade seja obtida, de modo que os problemas tendem somente a crescer, retroalimentando a dinâmica e as pulsões por essas mesmas políticas de segurança.

Notas

[1] Mestre e graduado em Direito na UnB. Foi professor substituto de direito penal e direito processual penal na Universidade Federal de Lavras (UFLA). Atualmente, leciona no UNIDESC, é doutorando no PPGD–UnB e pesquisador bolsista no IPEA. Lattes: http://lattes.cnpq.br/4789803970148615

[2] Graduando em Direito pela UnB. Membro do GCCrim/UnB, do Grupo Política Criminal/CEUB e do NPEPEP/USP. Lattes: http://lattes.cnpq.br/3487339835026289

[3] Tradução do termo em inglês: *risk assessment*. Se refere a ferramentas que avaliam risco em potencial de alguém, utilizando como dados o *status* socioeconômico, condição familiar, local de trabalho e de moradia, ficha criminal etc, como se verá logo a seguir.

[4] Sobre o caso, cf.: THE CONVERSATION. Beth Daley. **We use big data to sentence criminals. But can the algorithms really tell us what we need to know?** 05 jun 2017. <https://theconversation.com/we-use-big-data-to-sentence-criminals-but-can-the-algorithms-really-tell-us-what-we-need-to-know-77931> Acesso em 20 mar 2020.

[5] SCOTUS BLOG. Supreme Court of the USA < https://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/> Acesso em 20 mar 2020.

[6] Conferir, por exemplo, o caso *Iowa v. Guise*, especificamente o voto do juiz [Justice] Appel. <https://cases.justia.com/iowa/supreme-court/2018-17-0589.pdf?ts=1544798177> Acesso em: 24 mar 2020.

[7] Dentre outros, PEDRESCHI Et al, 2008; KAMIRAN; CALDERS, 2012; EUBANKS, 2015; NOBLE, 2018; O'NEIL, 2018; FERGUSON, 2017; BYFIELD, 2018.

[8] ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. **Machine Bias** – There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica: 23 maio 2016.: < https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> Acessado em: 25 jan 2021.

[9] Prevenção especial se refere a uma das funções da pena. Sendo especial e não geral, se refere à estratégia preventiva com foco e atuação sobre o indivíduo, não sobre a sociedade. Como indica Ferrajoli: "Contrariamente às teorias contratualistas e jusnaturalistas da época iluminista, que expressavam o apelo liberal e revolucionário da tutela do indivíduo contra o despotismo do velho Estado absolutista, referidas doutrinas [da prevenção especial] refletem as vocações autoritárias do novo e então consolidado Estado liberal e aquelas totalitárias dos regimes que emergerão da crise deste" (2014, p. 246).

[10] Cf. DIETER, 2012, p. 161.

[11] Na lei penal, nos referimos especialmente ao art. 59 do Código Penal, que autoriza o juízo a utilizar critérios eminentemente subjetivos para cálculo da pena–base de um condenado, ao art. 28, § 2º da Lei de Drogas (Lei nº 11.343/06), que no mesmo sentido prevê critérios abertos para definição da conduta de tráfico e de porte para uso pessoal, e também ao art. 244 do CPP, que permite a revista e busca pessoal quando agente policial tiver "fundada" suspeita.

[12] Sobre tirocínio policial, cf. DUARTE et al, 2014, p. 89.

[13] Tradução livre de: *Western countries have responded to increasing levels of fear and insecurity through the diffusion of 'new prevention ' approaches, giving place to what has been called the 'preventive turn'*.

[14] O conceito de *black box* se refere à dificuldade de se acessar ou se compreender o caminho do processo decisório efetuado pelas máquinas que processam dados pessoais.

[15] Tradução livre de: "Moreover, the tendency in criminal justice arenas toward secrecy in police investigative strategies suggests that ASAs [Automated Suspicion Algorithms] are unlikely to be transparent or interpretable". (RICH, 2016, 911–2).

[16] Tradução livre de: Reasoned transparency stresses the importance of government explaining its actions by giving reasons.

[17] Conferir nota de rodapé nº 5.

[18] Tradução nossa de: "[...] *if people of color are stopped and arrested disproportionately for drug crimes relative to actual prevalence, and if those arrests are the basis for forecasts, then predictions will lead to more disproportionate stops and arrests. Unequal outcomes will grow and, not surprisingly, subsequent arrests would be consistently confirmed by predictions*".

[19] Tradução livre de: "*there are several cases that demonstrate how racism and sexism are part of the architecture and language of technology, an issue that needs attention and remediation*".

[20] Tradução livre de: "*algorithms are serving up deleterious information about people, creating and normalizing structural and systemic isolation, or practicing digital redlining, all of which reinforce oppressive social and economic relations*".

[21] Tradução livre de: "*the neoliberal political and economic environment has profited tremendously from misinformation and mischaracterization of communities, with a range of consequences for the most disenfranchised and marginalized among us*".

[22] Em português: manuais *faça-você-mesmo* de armas de destruição matemática. Na tradução, perde-se o trocadilho proposto pela autora de *mass* (em massa) e *math* (matemática).

[23] Tradução livre de: "*each crime-fighting model calls for certain input data, followed by a series of responses, and each is calibrated to achieve an objective*".

[24] Tradução livre de: "*This creates a pernicious feedback loop. The policing itself spawns new data, which justifies more policing. And our prisons fill up with hundreds of thousands of people found guilty of victimless crimes. Most of them come from impoverished neighborhoods, and most are black or Hispanic. So even if a model is color blind, the result of it is anything but. In our largely segregated cities, geography is a highly effective proxy for race*".

[25] Segundo Aury Lopes Jr., flagrante esperado "É o que ocorre na maioria das vezes em que a polícia, de posse de uma informação, se oculta e espera até que o delito esteja ocorrendo para realizar a prisão" (2020, p. 949). A oposição feita é com o modelo, mais tradicional, de investigação após o crime, em que as autoridades tomam ciência do crime, da vítima e de outros elementos somente após ele já ter acontecido.

Referências

AGUIAR WANDERLEY, Gisela. **Liberdade e suspeição no Estado de Direito**: o poder policial de abordar e revistar e o controle judicial de validade da busca pessoal. 2017. 290 f. Dissertação (Mestrado em Direito)—Universidade de Brasília, Brasília, 2017

BECK, Ulrich. **Sociedade de risco**: *rumo a uma outra modernidade*. Trad. Sebastião Nascimento, 2. ed. São Paulo: Editora 34, 2011.

BRANTINGHAM, P. Jeffrey. The Logic of Data Bias and Its Impact on Place-Based Predictive Policing. **Ohio State Journal of Criminal Law**. Vol. 15; 473-486, 2018.

BYFIELD, Natalie P. Race science and surveillance: police as the new race scientists. **Social Identities**. Jan., 2018. DOI: 10.1080/13504630.2017.1418599

CALDERS, Toon; CUSTERS, Bart. What Is Data Mining and How Does It Work? In: **Discrimination and Privacy in the Information Society Data Mining and Profiling in Large Databases**. Bart Custers, Toon Calders, Bart Schermer, and Tal Zarsky (Eds.). pp. 27-42, 2013.

CARDOSO, Bruno V. Olhares e mediações sociotécnicas: Videovigilâncias e videovoyeurismos. **Dilemas**: Revista de Estudos de Conflito e Controle Social – Vol. 3 – nº 10 – 2010 – pp. 33-50.

COGLIANESE, Cary; LEHR, David. Transparency and Algorithmic Governance. **Faculty Scholarship at Penn Law**, 2123. 2019.

DUARTE, Evandro C. Piza; MURARO, Mariel; SILVA, Marina Lacerda; DEUS GARCIA, Rafael de. Quem é o suspeito do crime de tráfico de drogas? Anotações sobre a dinâmica dos preconceitos raciais e sociais na definição das condutas de usuário e traficante pelos policiais militares nas cidades de Brasília, Curitiba e Salvador [p. 81–120]. In: FIGUEIREDO, Isabel Seixas de. (Org.). **Segurança pública e direitos humanos**: temas transversais, vol. 05. Brasília–DF, Ministério da Justiça (SENASP), 2014.

ERICSON, R e HAGGERTY, K. **Policing the Risk Society**. Oxford: Clarendon Press. 1997.

EUBANKS, Virginia. **Automating inequality**: How high–tech tools profile, police, and punish the poor. St. Martin's Press, New York. 2015.

FARIAS, Juliana. Fuzil, caneta e carimbo: notas sobre burocracia e tecnologias de governo. **Confluências, Revista Interdisciplinar de Sociologia e Direito**. Vol. 17, nº 3, pp. 75–91, 2015.

FERGUSON, A. G. How data–driven policing threatens human freedom. **The Economist**. 2018. Disponível em: <https://www.economist.com/open–future/2018/06/04/how–data–driven–policing–threatens–human–freedom>. Acessado em: 07/01/2020.

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

FERGUSON, A. G.; LOGAN, W. A. Policing Criminal Justice Data, In: **Minnesota Law Review** pp. 541–616, 2016.

FERRAJOLI, Luigi. **Direito e Razão – Teoria do Garantismo Penal**. 4ª ed. São Paulo, editora Revista dos Tribunais, 2014.

GARLAND, David. **A cultura do controle**: crime e ordem social na sociedade contemporânea. Rio de Janeiro: Revan, 2008.

GARLAND, David. As contradições da "sociedade punitiva": o caso britânico. **Rev. de Sociologia e Política**, Curitiba, nº 13, p. 59–80, nov. 1999.

GARLAND, David. The culture of high crime societies: some preconditions of recent "law and order" policies. **Brit. J. Criminol**. n. 40, pp. 347–375, 2000.

JESUS, Maria Gorete Marques de. **A verdade jurídica nos processos de tráfico de drogas.** Belo Horizonte: editora D'Plácido, 2018.

KAMIRAN, Faisal; CALDERS, Toon. Data preprocessing techniques for classification without discrimination. **Knowl Inf Syst** (2012) 33:1–33. Dez., 2011. DOI 10.1007/s10115–011–0463–8.

LOPES, Cleber da Silva. Como se vigia os vigilantes: o controle da Polícia Federal sobre a segurança privada. **Rev. Sociol. Polit.** vol.19 no.40 Curitiba, out., 2011. doi.org/10.1590/S0104–44782011000300008

LOPES, Cleber da Silva. O Poder de Revista da Segurança Privada: os fundamentos e limites das revistas realizadas em consumidores. **Revista Brasileira de Ciências Policiais.** Brasília, v. 11, n. 1, p. 203–226, jan/abr 2020.

LOPES JR., Aury. **Direito processual penal**. 17ª ed. – São Paulo: Saraiva Educação, 2020, (versão digital, 1937 p.).

LUCIANETTI, Livia. Crime prevention and community safety policies from a dynamic and comparative perspective: The cases of Rome and London. **Crime Prevention and Community Safety**. vol. 13, n. 4, pp. 260–272. 2011. doi:10.1057/cpcs.2011.13

LUM, Kristian; ISAAC, William. To predict and serve? **Significance Magazine**, pp. 14–19, October 2016.

LYON, David. Cultura da vigilância: envolvimento, exposição e ética na modernidade digital. In: **Tecnopolíticas da vigilância**: perspectivas da margem. Organização: Fernanda Bruno (et al.); trad. Heloísa Cardoso Mourão (et al.). 1. ed. São Paulo: Boitempo, 2018.

MISSE, Michel. O inquérito policial no Brasil: Resultados gerais de uma pesquisa. **Dilemas: Revista de Estudos de Conflito e Controle Social** – Vol. 3 – no 7 – pp. 35–50, jan/fev/mar 2010.

MISSE, Michel. O Papel do Inquérito Policial no Processo de incriminação no Brasil: algumas reflexões a partir de uma pesquisa. **Revista Sociedade e Estado** – Volume 26 Número 1. Pp. 15–27. Janeiro/Abril, 2011.

NOBLE, Safiya Umoja. **Algorithms of oppression**: how search engines reinforce racism. New York: New York University Press, 2018.

O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. 1ª ed. New York: Crown Publishers, 2016.

OLESON, J.C. Risk in Sentencing: Constitutionally Suspect Variables and Evidence–Based Sentencing [p. 1329 –1394]. 64 **SMU L. Rev.**, 2011.

PEDRESCHI, Dino; RUGGIERI, Salvatore; TURINI, Franco. Discrimination–aware Data Mining. In: KDD '08: **Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining**. p. 560–568, 2008. doi.org/10.1145/1401890.1401959.

PIRES, Álvaro. A Racionalidade penal moderna, público e os direitos humanos. In: **Novos Estudos.** São Paulo, n. 68, p. 39–60, mar. 2004.

POWELL, Walter. W. Neither Market nor Hierarchy: Networks forms of organization. **Organizational Behavior,** Vol. 12, pp. 295–336, 1990.

RAUTER, Cristina. **Criminologia e subjetividade no Brasil**. 2. ed. Rio de Janeiro: Revan, 2003.

RICH, Michael. Automated Suspicion Algorithms and the Fourth Amendment. **University of Pennsylvania Law Review.** Vol. 164: p. 871–929. 2016.

ROUVROY, Antoinette; BERNS, Thomas. Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individualização pela relação? In: **Tecnopolíticas da vigilância**: perspectivas da margem. Organização: Fernanda Bruno (et al.); trad. Heloísa Cardoso Mourão (et al.). 1. ed. São Paulo: Boitempo, pp. 107–139, 2018.

ZAFFARONI, Eugenio R.; SANTOS, Ílison Dias dos. **A nova crítica criminológica**: criminologia em tempos de totalitarismo financeiro. Trad. Rodrigo Murad do Prado. 1. ed. São Paulo: Tirant lo Blanch, 2020.

ZEDNIK, C. Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence**. Philos. Technol**. 2019. Disponível em: <https://doi.org/10.1007/s13347–019–00382–7>.

ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: **Tecnopolíticas da vigilância**: perspectivas da margem. Organização: Fernanda Bruno (et al.); trad. Heloísa Cardoso Mourão (et al.). 1. ed. São Paulo: Boitempo, pp. 17–67, 2018.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology** 30, 75–89. doi:10.1057/jit.2015.5, 2015.