POLICIAMENTO PREDITIVO NA ERA DA VIGILÂNCIA: A BUSCA DE UM MODELO CONSTITUCIONAL E DEMOCRÁTICO

Predictive policing in the surveillange age: the search for a constitutional and democratic model

Valter Shuenquener de Araujo
Universidade do Estado do Rio de Janeiro - UERJ, Rio de Janeiro, RJ, Brasil
Lattes: http://lattes.cnpq.br/8284713431239760 ORCID: https://orcid.org/0000-0003-1584-5340
E-mail: saraujo19@gmail.com

Júlio José Araujo Junior
Universidade do Estado do Rio de Janeiro - UERJ, Rio de Janeiro, RJ, Brasil
Lattes: http://lattes.cnpq.br/2244172481620032
E-mail: juliojaraujo@gmail.com

Lucca Fernandes de Albuquerque
Universidade do Estado do Rio de Janeiro - UERJ, Rio de Janeiro, RJ, Brasil
E-mail: lucca.albuquerque93@gmail.com

Trabalho enviado em 11 de janeiro de 2022 e aceito em 13 de fevereiro de 2022

RESUMO

Este artigo pretende abordar as potencialidades e os eventuais riscos na adoção de tecnologias em policiamento preditivo, além de avaliar as possibilidades de condução dos processos decisórios pela Administração Pública na definição do uso de Big Data em segurança pública. Em outras palavras, pretende-se responder à seguinte pergunta: quais os riscos e oportunidades que a coleta de um conjunto grande de dados, estabelecidos por algoritmos, sobre padrões de comportamento e entendimentos escondidos, oferece? Ao olhar para as experiências de outros países e os debates atualmente levados a cabo no Brasil, procuramos indicar alguns caminhos para uma discussão constitucionalmente adequada da matéria. A metodologia utilizada é a bibliográfica e o objetivo da pesquisa realizada é o de contribuir para o debate em torno da utilização da tecnologia para a tomada de decisões estatais.

Palavras-chaves: *Big data*; policiamento preditivo; direitos fundamentais; tecnologia; racismo.

ABSTRACT

This article aims to address the potential and possible risks in adopting technologies in predictive policing and to evaluate the possibilities of conducting decision-making processes by the Public Administration in defining the use of Big Data in public security. In other words, we intend to answer the following question: what are the risks and opportunities that the collection of a large set of data, established by algorithms, about behavior patterns and hidden understandings, offer? By looking at the experiences of other countries and the debates currently taking place in Brazil, we seek to indicate some paths for a constitutionally adequate discussion of the matter. The methodology adopted is bibliographic and the objective of the research carried out is to contribute to the debate concerning the use of technology for state decision-making.

Keywords: *Big data; predictive policing; fundamental rights; technology; racismo.*

INTRODUÇÃO

A efetivação de políticas de segurança pública tem despertado um grande interesse na sociedade brasileira nos últimos anos. Apesar da premência da discussão acerca de temas relacionados à desigualdade social - como políticas de inclusão, direitos sociais e liberdades -, o aumento de índices de violência em praticamente todas as capitais do Brasil acendeu discussões sobre a segurança que pareciam estar limitadas aos grandes centros urbanos.

Dada a ausência de respostas eficazes e a insuficiência de uma atuação policial que se dê apenas após a ocorrência dos fatos, os governos buscam soluções que não apenas reprimam práticas criminosas, mas também tenham a capacidade de prevenir novos ilícitos. Nesse contexto, a tecnologia tem emergido como uma possível aliada para que, mediante cruzamento de dados e informações, a polícia possa viabilizar serviços de inteligência e identificar práticas suspeitas e localidades e horários com crimes frequentes, além de utilizar técnicas como reconhecimento facial e monitoramento de redes. Fala-se assim em "policiamento preditivo", que consiste no uso de dados e algoritmos para efetuar análises e "predizer" a prática de crimes, iniciativa que já vem sendo adotada em outros países.

Vivemos, no entanto, uma era de vigilância constante, em que a experiência humana se torna uma matéria-prima para práticas comerciais por meio da obtenção de dados que ajudam não apenas a entender o perfil consumidor das pessoas, mas também a formatar o seu comportamento. Com isso, busca-se prever o que as pessoas farão hoje, amanhã e depois de amanhã. Esse capitalismo de vigilância, como cunhou Shoshana Zuboff, acumula conhecimento sobre nós, mas não para nós. A previsão de nossos comportamentos futuros é feita para o ganho de terceiros, e não nosso (2011, p. 11).

O presente trabalho pretende abordar as potencialidades e os eventuais riscos na adoção de tecnologias em policiamento preditivo, além de avaliar as possibilidades de condução dos processos decisórios pela Administração Pública na definição do uso de Big Data em segurança pública. Em outras palavras, pretende-se responder à seguinte pergunta: quais os riscos e oportunidades que a coleta de um conjunto grande de dados, estabelecidos por algoritmos, sobre padrões de comportamento e entendimentos escondidos, oferece? Ao olhar para as experiências de outros países e os debates atualmente levados a cabo no Brasil, procuramos indicar alguns caminhos para uma discussão constitucionalmente adequada da matéria.

À primeira vista, o policiamento preditivo oferece mais efetividade à atuação policial, pois disponibiliza informações que antes não estavam ao alcance dos órgãos de Estado. Por outro lado, há o risco de aprofundar o enviesamento da atividade policial e acarretar a violação de direitos fundamentais, como o direito à privacidade, e o viés racializante da programação de certos algoritmos.

O artigo está estruturado em três seções. A primeira descreverá as transformações por que o Direito Público vem passando em razão das novas tecnologias, o que provoca a ressignificação ou abandono de certos institutos, impondo-se novos *standards* jurídicos a uma realidade dinâmica. Na segunda, o tema da segurança pública é destacado, com ênfase na abordagem sobre o policiamento preditivo, em abordagem comparada. Por fim, ao apresentar a realidade brasileira e as iniciativas em curso no país, apresentamos alguns caminhos que consideramos constitucionalmente adequados para o êxito dos debates sobre a matéria, tendo em vista a existência de um anteprojeto de lei geral de proteção de dados no âmbito penal e na segurança pública.

1. AS NOVAS TECNOLOGIAS E AS TRANSFORMAÇÕES NA ADMINISTRAÇÃO PÚBLICA

A modernidade é marcada pelo constante advento de inovações disruptivas. Trata-se de eventos que causam uma "mudança abrupta de modelos e sistemas até então existentes em virtude de novas tecnologias" (ARAUJO, 2018, p. 1687) e transformam institutos e instituições consolidadas, legando à Administração uma reavaliação de seu papel na relação com os cidadãos. Nos últimos tempos, a frequência de inovações disruptivas aumenta e, constantemente, institutos e *standards* consolidados são modificados para acomodar as alterações por elas ocasionadas.

Em sentido estrito, o estudo das "inovações disruptivas" limita-se a tratar do seu impacto na administração de empresas e em mercados consolidados[1]. Verifica-se, no entanto, que essas inovações podem provocar verdadeiros "*desarranjos institucionais*" também na Administração Pública (BAPTISTA; KELLER, 2016, p. 127). Determinadas inovações conduzem à *regurgitação*[2]

[1] O tema foi cunhado em estudo seminal de Clayton Crristensen e Joseph Bower, *v.* (CHRISTENSEN, BOWEN, 1995).

[2] Aqui, o sentido empregado ao termo é o mesmo expresso no "manifesto antropofágico" de Oswald de Andrade: o artista, imerso em sua cultura nacional, deglutinaria influência externas (no caso, técnicas estrangeiras) e *regurgitaria* algo novo e superior (a estética modernista). Aqui, o intérprete, imerso nos institutos clássicos do

de institutos do Direito Administrativo e, ante a necessidade de seu *aggionarmento*[3] às modificações provocadas pelas inovações tecnológicas, induzem à reanálise de suas propriedades ou, em um fluxo inverso, demandam modificações nas próprias inovações tecnológicas que as acomodem às diretrizes desses institutos jurídicos.

O conceito de "discricionariedade" na análise de atributos de atos administrativos é um exemplo. A despeito das divergências doutrinárias em torno do conceito[4], as inovações disruptivas provocam forte impacto no exercício de atos de competência discricionária. Isso se dá especialmente pelo fato de que, em uma Administração Pública baseada na eficiência, os atos discricionários embasam-se em fatos e evidências que devem ser coletados e processados a fim de orientar o gestor público na tomada de decisão dentre as possíveis alternativas. Com o uso da tecnologia, abre-se um leque amplo de possibilidades e informações para a atuação administrativa.

A inteligência artificial tem disponibilizado ferramentas que antes eram inalcançáveis para organizar o conjunto de fatos e informações que subsidiarão a tomada de decisão. O cruzamento de dados e sistemas transcende um algoritmo regular, permitindo emular pensamentos e o próprio comportamento humano. Conforme observa Dmitrii Trubnikov (TRUBNIKOV, 2017), a inteligência artificial favorece a combinação das informações apreendidas e ajuda a prever comportamentos. Nesse contexto, a capacidade de disrupção da inteligência artificial pode ser potencializada ao associar-se ao *machine learning* e à utilização de *Big Data*, que armazenam e integram um conjunto de dados públicos, registros, informações em redes sociais, dados de câmeras e satélites, tornando-se fonte valiosa de informação.

Considerando que a capacidade de coleta e/ou processamento de dados de seres humanos é bem inferior à capacidade das máquinas e computadores, a atratividade dos sistemas de inteligência artificial é inegável. A incorporação de elementos de inteligência artificial, *machine learning* e *Big Data* em *softwares* permite uma capacidade de coleta e processamento de dados cujo potencial é

Direito Administrativo, deve absorver a influência das novas tecnologias e conceber institutos do Direito Administrativo revigorados e contemporizados. *V.* ANDRADE, 1928.

[3]Termo em italiano utilizado pela Igreja Católica no Segundo Concílio do Vaticano para simbolizar a necessidade de "adaptar melhor às necessidades de nosso tempo as instituições suscetíveis de mudanças"; V. Constituição *Sacrosanctum concilum*. Disponível em < http://www.vatican.va/archive/hist_councils/ii_vatican_council/documents/vat-ii_const_19631204_sacrosanctum-concilium_po.html > Acesso em 03 de novembro de 2020;

[4] Na concepção clássica, a discricionariedade corresponde à margem de liberdade conferida legalmente ao Administrador para proferir uma decisão ou fazer uma avaliação, segundo critérios de conveniência e oportunidade. Em contraponto a essa noção, Gustavo Binenbojm (2014) defende a ideia de "ato vinculado diretamente por princípio", que corresponde aos atos nos quais o administrador tem a "tarefa de escolher, dentre as opções jurídica e materialmente disponíveis, aquela que melhor concretiza os fins colimados pela norma de competência (constitucional, legal ou regulamentar".

infinito, limitando a intervenção humana. Em consequência, a compreensão sobre o exercício de ato de competência discricionária também é alterada: agora, o gestor pode atuar com base em informações coletadas e processadas por programas de computador. Se a marca do ato de competência discricionária seria a liberdade de conformação ao agente público, a coleta e processamento de dados feita previamente por algoritmos é capaz de restringi-la.

Do ponto de vista da efetividade do controle da própria Administração, a restrição da margem de conformação pode ser positiva, pois diminui a subjetividade na tomada de decisão. Afinal, o espaço de conformação agora pode ser delimitado e filtrado por sistemas de inteligência artificial que coletam, organizam e processam informações em larga escala para sua transformação em respostas (ARAUJO, p. 1687).

De pronto, é possível identificar uma maior eficiência na utilização dos algoritmos, pois eles permitem simultaneamente a redução de custos e a análise mais célere de dados, diminuindo as influências comportamentais relacionadas ao agente executor da atividade. Deve-se, porém, atentar que a ideia de neutralidade dos dados coletados não é totalmente verdadeira. Afinal, existe uma decisão prévia – feita por seres humanos - na definição dos dados que serão coletados e a estipulação de premissas que estabelecem como os dados devem ser utilizados e geridos. Com isso, todo o processo de coleta dos dados já terá sido desenhado a partir de uma prévia intervenção humana e discricionária.

Como consequência, a aplicação do conjunto de dados oferecidos pelas novas tecnologias pode aprofundar a arbitrariedade, mas desta vez sob a roupagem da objetividade e da neutralidade, inviabilizando ainda mais o controle de atos. Fatores e decisões que poderiam ser atribuídos a um excesso de discricionariedade do gestor desta vez seriam tratados sob a ótica da frieza dos números, com o fundamento de que os dados "não mentem".

Por essa razão, é fundamental compreender o campo de utilização dos dados e estabelecer mecanismos de sopesamento sobre os impactos que a tecnologia exercerá em direitos fundamentais. Da mesma forma, o controle da administração deverá atingir etapas precedentes à organização dos dados, de modo a impedir que a falta de transparência acarrete a violação de direitos, como o direito à privacidade, e a consolidação de práticas enviesadas e discriminatórias.

No âmbito da segurança pública, a questão ganha contornos ainda mais singulares, dado o risco de a tecnologia referendar a criminalização de grupos sociais específicos e a atuação seletiva sobre pessoas com base tão somente em suas características físicas e em seus modos de vida, hábitos e companhias.

2. A SEGURANÇA PÚBLICA E O POLICIAMENTO PREDITIVO

Um pequeno exemplo do comércio pode demonstrar o funcionamento da correlação de dados oferecida pela tecnologia. No sítio eletrônico da empresa *Amazon*, toda vez que uma pessoa acessa um item, ela vê uma seção de recomendação sobre o comportamento dos consumidores que o compraram. Ao correlacionar os dados históricos de bilhões de transações, aponta-se um entendimento sobre quais bens os consumidores geralmente compram juntos.

Esse tipo de cruzamento de informações com base em dados encontra na persecução penal um terreno fértil. Afinal, a atividade investigativa busca justamente informações relativas a interesses e inclinações individuais, além de conexões entre grupos e padrões de comportamentos. A polícia monitora, investiga, descobre e procura por padrões suspeitos. Considerando que as ferramentas *Big Data* constituem ferramentas de vigilância, a demonstração de interesse policial na tecnologia é facilmente assimilável.

Sistemas *Big Data* podem favorecer a priorização de certas informações, pessoas, lugares e horários. Listas podem ser geradas para intervenção, vigilância ou perseguição. Dossiês personalizados podem ser criados para monitorar as pessoas mais violentas e perigosas de uma cidade, de modo que, em qualquer jurisdição, a polícia possa desenvolver estratégias para intervir e pará-las. Esta é a grande promessa da polícia preditiva para reduzir a violência.

A informação sobre os interesses de pessoas e a correlação de dados históricos de transações e interações, quando transposta para análises de investigação, pode ser muito útil. Por exemplo, por meio de um policiamento *Big Data*, traficantes podem ser identificados com base em informações como compra de suprimentos, transações ou padrões em viagens. Não se trata de uma informação absoluta, porém ela indica correlações e caminhos de investigação: da mesma forma que a *Amazon* utiliza dados para verificar os compradores reincidentes, os dados trazem a promessa de prever o criminoso futuro (O'NEIL, 2016).

Essa promessa é recebida com entusiasmo por gestores e policiais. A utilização da inteligência artificial pode ser capaz de mudar drasticamente a forma de atuação das polícias. Em vez do patrulhamento ostensivo tradicional, a polícia atuaria de forma proativa para responder a situações pré-identificadas, com base em serviços de inteligência. Assim, o órgão centraria esforços no mapeamento de redes de indivíduos, identificando aqueles que podem gerar mais risco ou envolvimento em atos violentos, com vistas a adotar medidas concretas de dissuasão.

O auxílio prestado pela tecnologia *Big Data* emerge como uma ferramenta capaz de identificar com maior chance redes criminosas e relacionar comportamentos para investigações futuras. Ademais, a análise preditiva pode contribuir para identificar a má conduta de um policial que seja constantemente filmado ou identificar necessidades sociais e econômicas que levam à prática de um crime (FERGUSON, 2017, p. 5). Ou seja, a própria atuação das corporações poderia estar sujeita a um maior controle.

O problema, porém, reside no fato de que, por trás dos números da tecnologia, existem pessoas. Algumas se engajam nas práticas de crimes; muitas, não. A vigilância oferece os alicerces para um estado policial mais intrusivo, com violação permanente do direito à privacidade. Ao expandir o espectro de quem poderá ser vigiado, sob a promessa de uma aplicação inteligente da lei, a tecnologia gera o medo da vigilância totalizante.

Nos Estados Unidos, algumas experiências têm sido adotadas há algum tempo. As formas de policiamento preditivo podem se referir aos sujeitos (*person-based targeting*), aos locais (*place-based targeting*) e ao próprio tempo da prática de crimes (*time-based targeting*). Essas estratégias procuram identificar a *priori* pessoas que estariam mais propensas à prática de crimes ou concentrar os esforços nos lugares e horários em que os ilícitos são comumente mais perpetrados.

Na análise com base nas pessoas, os debates suscitam maior controvérsia. Neste caso, o policiamento preditivo tenta se antecipar e prever quem estaria mais propenso à prática criminosa. O *Big Data* promete visualizar como a violência se espalha pelas comunidades e prever o comportamento dos agentes e as vítimas mais prováveis de violência. Ao identificar esse cenário, a polícia pode agir antes de os fatos acontecerem, desestimulando a prática criminosa.

Uma das formas de prevenção consiste na *focused deterrence* (dissuasão focada), adotada em diversas cidades[5], por meio da qual o Estado apresenta uma mensagem explícita a uma fatia estreita da população de que a polícia, os promotores e a comunidade sabem quem está engajado em violência e que os assassinatos devem ter um fim (FERGUSON, 2017, p. 35). Um dos locais pioneiros foi Kansas City, onde a medida foi implementada a partir de 2012. No modelo da *focused deterrence*, não existe investigação sobre um caso específico, mas sim uma atuação policial com base nos dados sobre o comportamento de grupos locais que já atuaram em crimes anteriores e que não foram presos ou mesmo responsabilizados. A dissuasão focada compreende três passos: i)

[5] Estima-se que, em 2018, 84 cidades adotavam algum tipo de "focused deterrence" nos Estados Unidos. Como afirma Gary J. Pihlaja (2019), os modelos adotados podem ser agrupados em três categorias: i) programas que têm como alvo indivíduos; ii) programas que buscam atingir grupos de indivíduos; e iii) e programas que buscam atingir "hot spots" em relação a áreas de práticas criminosas, sobretudo com ênfase em mercados de drogas.

identificar atores responsáveis por crimes; ii) dar notícia a esses atores de que a polícia está ciente de suas atividades e oferecer serviços sociais; e iii) prender, processar e punir esses indivíduos que receberam o aviso, mas o ignoraram[6].

Outra estratégia corresponde à *Strategic Suspects List*, também chamada *heat list*, adotada pela polícia em Chicago desde 2013. Trata-se de um mecanismo de seleção por algoritmos de pessoas, as quais são identificadas como de alto risco com base na quantidade de vezes que foram presas com outras que posteriormente se tornaram vítimas de homicídio ou presas com outras que, por sua vez, foram presas com vítimas futuras de homicídio. O algoritmo estabelece uma classificação de todas as pessoas nessas condições, com uma pontuação que varia de 1 a 500[7]. As pessoas com uma pontuação mais alta representam um "maior risco" à sociedade. O algoritmo, que é secreto e não está sujeito a *accountability*, forja a estratégia policial, indica o uso da força e estabelece parâmetros para a atuação de segurança nas batidas policiais. Assim, quando uma pessoa é abordada pela polícia, o computador indica a sua pontuação, o que serve de informação sobre o risco que ela representa e as medidas que podem ser adotadas.

As informações estatísticas indicam que as listas oferecem dados valiosos. Em um violento fim de semana do dia das mães em 2016, Ferguson relata que 70% das 51 pessoas que se envolveram em tiroteios nos dois dias haviam sido identificadas corretamente na *heat list* de Chicago. Em outro momento, em 2016, 78% de 64 pessoas nessas condições também estavam nela com alta pontuação. Sem embargo, existem questionamentos acerca da efetividade do programa, sobretudo quanto a medidas que efetivamente busquem remediar os riscos econômicos e sociais que foram identificados. Episódios violentos que ocorreram na região em 2016 mostraram certa ineficácia da política na atividade preventiva. Além disso, em estudo do mesmo ano, a *RAND Corporation* constatou que a lista se tornou uma mera lista de "mais procurados", tendo a polícia e outros órgãos deixado de acompanhar os casos ou notificações ou serviços sociais (SAUNDERS, HUNT e HOLLYWOOD, 2016).

Uma terceira estratégia consiste na *Math and Murder*, adotada em Nova Orleãs. Por meio de mapas, foram identificados os locais onde há mais crimes. Pelas redes sociais, uma análise permitiu apontar indivíduos específicos como vítimas prováveis de crimes violentos. Análises

[6]Veja-se, nesse sentido: Chicago Tribune. *Chicago police use 'heat list' as strategy to prevent violence*. Disponível em: <https://www.chicagotribune.com/news/ct-xpm-2013-08-21-ct-met-heat-list-20130821-story.html> Acesso em 3 jan. 2021.

[7]Veja-se nesse sentido: New York Times. *Inside the Algorithm That Tries to Predict Gun Violence in Chicago.* Disponível em: https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html

previram de 35% a 50% das vítimas prováveis de tiroteios de uma subpopulação de 3900 indivíduos de "alto risco". Foram identificadas vítimas prováveis de homicídio. Mas a estratégia foi além das pessoas: bombeiros passaram a ter maior presença em escolas particulares, e o departamento de serviços públicos passou a cuidar da iluminação pública. O departamento de saúde priorizou escolas de alto risco para a prevenção de violência, e a polícia mapeou territórios de grupos criminosos para identificar áreas de tensão.

A cidade, então, lançou uma estratégia holística para enfrentar a redução da violência, com ênfase em áreas de maior risco. Políticas de dissuasão focada foram implementadas por meio de anúncios e encontros (*Stop the shooting meetings*). Desde 2013, houve uma redução de violência e a aplicação de 29 programas diferentes que focaram na família, na escola, no trabalho, na comunidade e no desenvolvimento econômico. De 2011 a 2014, houve uma redução de 21,9% no número de homicídios. Além disso, houve a redução de 55% em assassinatos de integrantes de grupos criminosos.

As três estratégias citadas mostram que, ao mapear redes sociais de indivíduos, a polícia pode identificar aqueles que estejam em maior risco de envolvimento em episódios de violência. Dentro dessas redes, uma subpopulação pode ser identificada por algoritmos como se representassem risco ainda maior. Priorizando esses indivíduos, as atividades criminais podem ser reduzidas, pelo menos no curto prazo. No entanto, saber como usar os dados é uma questão fundamental[8].

Essa preocupação ganha relevo ao analisarmos o emprego da tecnologia de reconhecimento facial, cujo uso tem sido disseminado, inclusive no Brasil[9]. Em geral, a utilização do reconhecimento facial não se limita a questões de segurança pública. Ele pode ser utilizado em portões eletrônicos de um prédio particular, por exemplo. Ele pode, ainda, ser extremamente útil em situações como a busca de pessoas desaparecidas e a perseguição de terroristas, além de auxiliar no impedimento ao tráfico de pessoas.

[8]No caso da *heat list*, em Chicago, o uso foi limitado à lista de mais procurados e à sua persecução, sem pensar no passo seguinte. No caso de Nova Orleãs, por outro lado, aperfeiçoou-se a dissuasão focada e houve um esforço para além da identificação das pessoas de alto risco, com um aumento das lentes da tecnologia *Big Data* e o enfrentamento das causas da violência.

[9]No Brasil, há uma crescente realização de testes de reconhecimento facial, com o registro de experiências no Rio de Janeiro e na Bahia Sobre essas experiências, veja-se: NUNES, Pablo. O algoritmo e o racismo nosso de cada dia. Revista Piauí. Disponível em: <https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/> Acesso em 4 jan. 2021.Na próxima seção, abordaremos a lei aprovada no Distrito Federal para tratar do reconhecimento facial.

Em outras partes do mundo, após uma grande euforia inicial com a sua utilização, dadas as possibilidades de identificação em espaços públicos de pessoas que estejam foragidas ou sejam procuradas pela polícia, a possibilidade de enviesamento racial e de erros na identificação tem acarretado novas regulamentações ou mesmo o abandono desta tecnologia. Na União Europeia, a questão vem sendo avaliada pela Comissão Europeia[10], ao passo em que, nos Estados Unidos, Nova Jérsei[11] e Portland[12], por exemplo, vêm abandonando essa tecnologia.

O problema reside no armazenamento de dados. Qual base de dados será utilizada para comparação das imagens de vídeo? Por quanto tempo os vídeos serão armazenados? Além disso, a utilização dessa ferramenta em locais públicos pode gerar uma vigilância em massa, por meio da qual todas as pessoas em espaços públicos são capturadas em câmeras, oferecendo informações a um banco de dados. As imagens de comparação podem ficar armazenadas por tempo indeterminado, sem ser destruídas. Isso significa que todas as pessoas podem ser seguidas, e seus movimentos, seguidos.

Este não é um risco apenas do reconhecimento facial, mas de todas as tecnologias que fazem o chamado "tratamento de dados". Com vistas a conter e delimitar a utilização dessas informações, a União Europeia elaborou uma regulação mais abrangente sobre a proteção de dados pessoais. A Carta de Direitos Fundamentais da União Europeia já reconhece, em seu art. 8º, que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito (art. 8.1). Os dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei (art. 8.2). Além disso, todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação (art. 8.3), cabendo a uma autoridade independente realizar a fiscalização do cumprimento dessas regras.

A Diretiva 2016/680, do Parlamento Europeu, dispõe de forma detalhada sobre o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detenção ou repressão infrações penais. Essa regulamentação inspirou o anteprojeto brasileiro sobre uma lei de proteção de dados no âmbito penal, como se verá na próxima seção. O item 26 do *considerandos*

[10]"European Commission hasn't completely ruled out biometric facial recognition ban in public spaces". Disponível em: <https://www.biometricupdate.com/202009/european-commission-hasnt-completely-ruled-out-biometric-facial-recognition-ban-in-public-spaces> Acesso em 4 jan. 2021.
[11]"Facial recognition can ID you in a crowd. But NJ wonders who's using it, how to regulate it" Disponível em: <https://www.northjersey.com/story/news/2020/02/06/facial-recognition-clearview-police-new-jersey-attorney-general/4666380002/ > Acesso em 4 jan. 2021.
[12]"Portland passes broadest facial recognition ban in the US". Disponível em: <https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html> Acesso em 4 jan. 2021.

da diretiva contém uma orientação clara, baseada no princípio da "lealdade de tratamento" dos dados, que ressalta a necessidade de previsão legal para o tratamento de dados e observância do princípio da proporcionalidade. Nesse ponto, impõe-se a necessidade de fixação de prazos para a utilização dos dados:

> (26) (...) A lealdade de tratamento, que constitui um dos princípios da proteção de dados, é uma noção distinta do direito a um tribunal imparcial, tal como definido no artigo 47.o da Carta e no artigo 6.o da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH). (…) **É especialmente necessário garantir que os dados pessoais recolhidos não sejam excessivos nem conservados durante mais tempo do que o necessário para os efeitos para os quais são tratados. Os dados pessoais só deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios.** A fim de assegurar que os dados são conservados apenas durante o período considerado necessário, **o responsável pelo tratamento deverá fixar prazos para o seu apagamento ou revisão periódica**. Os Estados-Membros deverão prever garantias adequadas aplicáveis aos dados pessoais conservados durante períodos mais longos a fim de fazerem parte de arquivos de interesse público ou de serem utilizados para fins científicos, estatísticos ou históricos. (grifamos)

Deve-se ressaltar, ainda, a importância do tratamento de dados sensíveis, como aqueles que revelam a origem racial ou étnica:

> (37) Os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, merecem uma proteção especial, dado que o contexto do tratamento desses dados pode implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» na presente diretiva que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. **Tais dados pessoais não deverão ser objeto de tratamento, a menos que este esteja sujeito a garantias adequadas dos direitos e liberdades do titular dos dados e seja permitido em casos autorizados por lei ou, se ainda não tiver sido autorizado por lei, se for necessário para a proteção dos interesses vitais do titular dos dados ou de um terceiro, ou ainda se estiver relacionado com dados que tenham sido manifestamente tornados públicos pelo titular dos dados**. As garantias adequadas dos direitos e liberdades do titular dos dados podem, por exemplo, incluir a possibilidade de recolher esses dados apenas em ligação com outros dados sobre a pessoa singular em causa, a fim de garantir devidamente a segurança dos dados recolhidos, o estabelecimento de regras mais rigorosas sobre o acesso do pessoal da autoridade competente aos dados ou a proibição da transmissão desses dados. (…) (grifamos)

De qualquer modo, em qualquer tecnologia a ser utilizada, é fundamental que as correlações de *Big Data* reconheçam um problema anterior, relacionado à premissa de alimentação dos dados. A decisão que estabelece as diretrizes de funcionamento de sistemas parte de algumas

pressuposições que podem embutir uma carga discriminatória ou atingir de forma desproporcional certos grupos sociais, como a população negra (*black data*).

O fator raça pode não entrar no algoritmo, porém as decisões políticas, as prisões e a determinação de vínculo a grupos criminosos correlacionam-se diretamente com leis e práticas racialmente discriminatórias. Como afirma Angela Davis, o aumento da punição desses grupos não é um fator natural, pois decorre do aumento da vigilância sobre eles (2019, p. 38-39). Se os dados são racializados (*black data*), isso significa que os sistemas de policiamento preditivo (que usam aqueles dados) podem gerar resultados enviesados. Assim, a afirmação de que "pessoas jovens negras no sul de Chicago são mais propensas a praticar crimes" pode parecer neutra, porém é bastante opaca. Quem enuncia a frase dirá que a afirmação não é racista, pois a decisão se fundamenta no algoritmo, mas é necessário entender que este devolve dados com base naquilo que lhe foi colocado. Se os dados começam e se baseiam em julgamento humano, então os resultados que o algoritmo oferecerá vão refletir o viés.

Nos Estados Unidos e no Brasil, por exemplo, o sistema de justiça criminal prende, processa e encarcera mais as pessoas negras. Se condenações anteriores influenciam como fatores objetivos para periculosidade, então essas estatísticas devem importar não apenas para crimes passados, mas também para situações futuras. Ou seja, o fator raça distorce o julgamento. O mesmo tipo de problema vale para a identificação de grupos criminosos, outro *input* crítico para a priorização algorítimica. Ir à escola com o membro de um grupo criminoso ou ser primo dele não poderia gerar etiquetamento (*labeling approach*). O fato de estar próximo a pessoas que praticam crimes e ter certos hábitos não necessariamente faz da pessoa um criminoso. Quanto enviesamento o *Big Data* pode evitar? Confiar em variáveis socioeconômicas em uma jurisdição onde condições socioeconômicas correlacionam-se com raça fatalmente levará ao resultado racial discriminatório, mesmo sem qualquer intenção expressa. Andrew Ferguson (2017) suscita cinco questões essenciais para guiar o debate acerca do tema, as quais nos parecem fundamentais.

A primeira delas diz respeito à identificação dos riscos que a tecnologia está tentando enfrentar. É necessário reconhecer, neste caso, que a decisão sobre o melhor sistema e os riscos que serão analisados é, antes de tudo, política. A ilusão de uma tecnologia neutra ou da construção objetiva de informações deve ceder ao reconhecimento de que a definição de questões extremamente relevantes se situa em uma esfera que não é marcada unicamente pela técnica. Por conseguinte, deve haver a transparência necessária para o exercício do controle da decisão da Administração Pública, com forte controle social. Assim, presunções tecnológicas erradas podem

levar à perda da vida de um agente público, ao passo que uma determinada comunidade pode entender mais adequada a preservação de sua privacidade. É por isso que se fala em *community input* acerca das decisões.

Nesse contexto, o Poder Judiciário pode ter um papel relevante, de modo a viabilizar um diálogo institucional com os órgãos de execução quanto ao grau de deferência democrática das diretrizes estabelecidas. Em outras palavras, na esteira do que propõe Barry Friedman (2017, p. 110-111), as Cortes devem enxergar a si próprias não como a palavra final em polícia, mas como parceiros dos elaboradores de normas – legisladores, corpos administrativos, polícia – em garantir que a polícia não é apenas constitucional, mas também democrática. As cortes devem dar atenção ao processo democrático para alcançar regras que governem a polícia[13].

A segunda questão corresponde à possibilidade de defesa dos *inputs* do sistema. É possível defender a precisão dos dados e da metodologia? Garantir o mecanismo adequado é um passo fundamental para assegurar legitimidade e efetividade do sistema *Big Data*. Da mesma forma, o local onde se colocará uma câmera, a informação que será destacada e a forma de geração de alertas automáticos influenciam em todos esses processos. Para confiar nos dados, é necessário saber de onde eles provêm, quem os coleta, quem faz o *double checking* e quem os corrige. Além disso, é necessário que o estabelecimento de relações causais esteja baseado também em outras informações e análises, devidamente fundamentadas, sob pena de ser transferido à tecnologia um ônus que é do administrador. Deve-se atentar ainda às generalizações baseadas em informações bem específicas, o que é incorreto, e na precisão temporal, uma vez que os dados podem variar ao longo do tempo. Como afirma Cathy O'Neil (2016, p. 204), o Big Data codifica o passado; ele não inventa o futuro. Assim, é necessário internalizar valores melhores nos algoritmos e criar modelos de Big Data atentos a diretrizes éticas.

A terceira questão abrange os *outputs* do sistema. A tecnologia pode atender à meta de redução de taxas de crimes, mas há fatores cujo sucesso é de difícil mensuração, como o respeito da comunidade pelos órgãos policiais. Tratar o cidadão como objeto de vigilância pode ter consequências no convívio do Estado com os cidadãos, além de colocar certos grupos em permanente condição de suspeitos.

A quarta questão diz respeito às medidas de *accountability* que a Administração pode adotar. Cabe ressaltar que a governança da segurança pública não se confunde com detalhes

[13]Ao utilizar a deferência democrática como ferramenta, as cortes podem indicar os horizontes e os quadrantes nos quais a polícia deve se basear antes de atuar. Exigir a atuação democrática antes do estabelecimento de regras pode ser um antídoto à falta de regras transparentes e um estímulo à participação social.

operacionais e sigilosos da atividade investigativa. É natural que o segredo seja mantido em relação a certos aspectos da segurança pública, mas ele não pode ser utilizado como salvo-conduto para a falta de transparência da própria política.

Por fim, a quinta questão: haverá respeito à autonomia das pessoas impactadas pela tecnologia? O deslocamento da investigação direcionada a uma pessoa individualmente considerada para a suspeição de grupo ou lugar encoraja a estigmatização e culpa por associação. Em sociedades fortemente marcadas por históricos de discriminação sistemática, o sistema Big Data tende a aprofundar distorções.

3. CAMINHOS PARA O POLICIAMENTO PREDITIVO DENTRO DO MARCO CONSTITUCIONAL BRASILEIRO

O debate sobre o policiamento preditivo já chegou ao Brasil, e diversas iniciativas começam a ser gestadas. Mapeamento de lugares afetados pela prática de crimes, monitoramento de veículos e propostas de reconhecimento facial já vêm sendo discutidas com bastante interesse e perspectiva sobre a melhora nos índices de segurança pública. Convênios vêm sendo firmados para o uso de tecnologia não apenas em espaços estratégicos – como aeroportos -, mas no cotidiano das grandes cidades[14].

Sem embargo, as negociações e discussões carecem de um maior envolvimento social. Embora a Lei nº 13.675/2018, que instituiu o Sistema Único de Segurança Pública, tenha enfatizado a importância das tecnologias na modernização da política de segurança pública, ela também destacou a necessidade de participação social em todas as esferas, de modo a permitir um melhor planejamento da política, o que não vem sendo devidamente observado.

Cabe destacar que a Constituição de 1988 contém, de forma inédita em relação aos textos constitucionais anteriores, um capítulo específico sobre o tema "segurança pública", bem como a distinção entre esta e a segurança nacional, mas as inovações param aí. Como observa Luiz Eduardo

[14]Veja-se: CASTRO, Renato de. **Como a inteligência artificial já está turbinando a segurança no Brasil.** Tilt, o canal sobre tecnologia do UOL. 15/07/2019. Disponível em: https://cidadesmaisinteligentes.blogosfera.uol.com.br/2019/07/15/como-a-inteligencia-artificial-pode-transformar-a-seguranca-publica/ Acesso em: 01/11/2020.; Redação. **Roubos de veículos caem mais de 65% em Niterói este ano (Dados são do Observatório de Segurança da Prefeitura).** O São Gonçalo. 03/11/2020. Disponível em: https://www.osaogoncalo.com.br/seguranca-publica/89751/roubos-de-veiculos-caem-mais-de-65-em-niteroi-este-ano. Acesso: 04/11/2020; SSPDS. **Combate à criminalidade com uso de inteligência artificial no Ceará é destaque em evento internacional em Brasília.** Secretaria da Segurança Pública e Defesa Social. 25/07/19. Disponível em: https://www.sspds.ce.gov.br/2019/07/25/combate-a-criminalidade-com-uso-de-inteligencia-artificial-no-ceara-e-destaque-em-evento-internacional-em-brasilia/. Acesso: 04/11/2020.

Soares (2019, p. 47), a arquitetura das instituições de segurança pública, sobretudo o modelo policial, preservou o formato organizacional que já possuíam no período autoritário e não houve um olhar mais acurado acerca do horror das práticas e dos crimes da ditadura, fazendo perpetuar uma organização muito fechada e pouco transparente ao povo, inviabilizando o seu controle.

Como se viu, a preocupação com a governança democrática dos órgãos de segurança não é uma preocupação apenas do Brasil. Deve-se admitir, não obstante, que o caso brasileiro é diferenciado não só em razão dos índices crescentes e do impacto desproporcional[15] que as políticas de segurança acarretam sobre grupos minoritários, mas também em razão de práticas aberta e formalmente afrontosas aos direitos humanos, colocando estes como os adversários à sua concretização.

Quando se analisam os dados da violência no Brasil, essa percepção torna-se mais evidente. Segundo o Atlas da Violência de 2018, publicação do Instituto de Pesquisas Econômicas Aplicadas (IPEA) em parceria com o Fórum Brasileiro de Segurança Pública (FBSP), o Brasil alcançou a marca de 62.517 homicídios naquele ano. Nos últimos dez anos, a taxa de homicídios de indivíduos não negros diminuiu 6,8%, ao passo que a taxa de vitimização da população negra aumentou 23,1%[16]. Em 2016, a taxa de homicídio para a população negra era de 40,2 por 100 mil habitantes; para o resto da população, 16 por 100 mil habitantes. Em outras palavras, 71,5% das pessoas que são assassinadas a cada ano no país são pretas ou pardas.

Além disso, o documento aponta que a maioria das pessoas assassinadas é jovem. Das 62 mil vítimas de homicídio, 33,6 mil tinham entre 15 e 29 anos, sendo a maioria de homens. Enquanto a taxa de homicídio geral é de 30,3 por 100 mil, a de jovens corresponde a 65,5 por 100 mil, mais

[15]O chamado "impacto desproporcional" abrange justamente essas práticas neutras que, sem intencionalidade ou necessidade de demonstração de motivação discriminatória, atingem de forma diferenciada certos indivíduos e grupos. A teoria do "impacto desproporcional" (*disparate impact*) surge nos Estados Unidos em debates trabalhistas (caso *Griggs v. Duke Power, Co*), mas a sua ampla aplicação é reconhecida na doutrina e jurisprudência. O Supremo Tribunal Federal já reconheceu a discriminação indireta em leis ou emendas constitucionais aparentemente neutras. O caso mais emblemático corresponde à ADI nº 1946/DF, na qual se tratou a constitucionalidade da limitação de valores de benefícios ao teto e o impacto sobre mulheres beneficiárias do salário-maternidade, cuja renda mensal corresponde exatamente à remuneração auferida pela segurada. O STF entendeu que, se fosse admitida a limitação do benefício em questão ao teto, haveria uma discriminação indireta em relação às mulheres trabalhadoras, em afronta ao princípio da igualdade (STF, ADI nº 1946/DF, Pleno, Rel. Min. Sydney Sanches, julgado em 03 de abril de 2003). Mais recentemente, cabe fazer menção ao voto vencedor do Ministro Roberto Barroso na ADPF 291, que tratou da previsão do Código Penal Militar que, ao criminalizar atos libidinosos em ambientes sujeitos à administração militar, faz referência expressa a termos como "pederastia ou outro" e "homossexual ou não". (STF, ADPF nº 291, Pleno, Rel. Min. Roberto Barroso, julgado em 28 de outubro de 2015, p. 31).

[16]Dados disponíveis em: <http://www.ipea.gov.br/portal/images/stories/PDFs/relatorio_institucional/180604_atlas_da_violencia_2018.pdf>. Acesso em 11 mar. 2019.

do que o dobro da média da população. Em síntese: a maior parte das vítimas são jovens, homens e negras. Por outro lado, a letalidade policial é um ponto de constante preocupação: em 2019, das 47.773 mortes violentas que ocorreram em 2019, 6.357 foram causadas por policiais[17].

Considerando esse cenário de desigualdade e de violência praticada pelos próprios agentes de segurança, a crença na aplicação neutra de tecnologias, que não saiba diferenciar correlações e causalidades, pode aprofundar discriminações e gerar uma aplicação de políticas de segurança de forma altamente enviesada. É por essa razão que as preocupações apontadas na seção anterior devem ter a mesma intensidade no Brasil.

Agrava o problema o fato de a lógica da atividade policial no Brasil ser baseada no policiamento ostensivo, que se baseia fundamentalmente em abordagens e apreensões. Com isso, a lógica policial é a da seleção de suspeitos, de forma aparentemente aleatória, porém muito marcada pela filtragem racial, penalizando pessoas negras e – em certas localidades - indígenas, por exemplo. A seleção de suspeitos não se apresenta como um desvio, mas, na prática, como técnica.

Com as tecnologias, não há qualquer mudança estrutural no modelo. O método para a produção dos dados segue artesanal, de modo que a tecnologia apenas mecaniza e digitaliza aquilo que já está carregado de estigmatização acerca dos suspeitos a serem selecionados. Diante disso, discutir o uso de tecnologias deve pressupor a discussão da a própria formulação da política de segurança pública. A necessidade de transparência e de observância de regras e diretrizes previamente definidas, baseadas em crivos constitucionais e democráticos, deveria ser um processo natural, porém a estrutura hermética dos órgãos de segurança a torna um desafio.

O Judiciário e o Legislativo têm indicado uma preocupação crescente com a utilização de dados pessoais para a atuação estatal, o que indica um caminho no tratamento da matéria. O Supremo Tribunal Federal, ao julgar a ADI nº 6387, que analisou a constitucionalidade da Medida Provisória 954[18], reconheceu o direito fundamental à proteção de dados pessoais. Já o Congresso se prepara para, após ter aprovado em 2018 a lei geral de proteção de dados (Lei nº 13.709/2018), analisar um projeto de lei que trata especificamente da proteção de dados no âmbito penal e na

[17]Veja-se: A alta da letalidade policial em 2019. E a sequência em 2020 | Nexo Jornal Acesso em 4 jan. 2021.
[18]A medida provisória trata do compartilhamento de dados pelas empresas de telecomunicação, prestadoras de Serviço Telefônico Fixo Comutado (STFC) e de Serviço Móvel Pessoal (SMP), com o Instituto Brasileiro de Geografia e Estatística (IBGE) para dar suporte à produção estatística durante a pandemia do novo coronavirus. Entre outros argumentos, o STF entendeu que "não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia.

segurança pública, formulado com base na diretiva da União Europeia[19].

O julgamento da medida cautelar na ADI nº 6387[20] indica premissas importantes para guiar o presente debate. Em primeiro lugar, os votos dos ministros do STF apontam o caráter constitucional da proteção de dados pessoais. A ministra Rosa Weber, relatora do caso, ressaltou que a proteção dos dados pessoais se insere nas cláusulas constitucionais da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Por essa razão, a sua manipulação e tratamento deve respeitar os limites delineados pela proteção constitucional.

Necessário destacar a observação do Ministro Luiz Fux, que, ao citar Daniel J. Solove (2011, p. 61), sublinhou a importância do respeito do direito à privacidade em tempos de crise. Segundo o autor estadunidense, haveria um "argumento de pêndulo": em tempos de crise, este permite o sacrifício de direitos em favor da segurança, enquanto que, em tempos de paz, ele voltaria à valorização da liberdade e da proteção dos direitos.[21] Já o Ministro Gilmar Mendes destacou que o direito fundamental à proteção de dados pessoais decorre de uma compreensão integrada do direito constitucional, que está fundamentada:

> (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa[22].

Citando Laura Schertel Mendes (2014, p. 140 e 176-177), o ministro asseverou que o direito fundamental à proteção de dados abarcaria, assim, uma dimensão subjetiva e uma dimensão objetiva. A primeira diz respeito à proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e, em uma perspectiva objetiva, a atribuição ao indivíduo da garantia de controlar o fluxo de seus dados.

No caso da dimensão subjetiva, o legislador tem o ônus de justificar, de forma constitucionalmente adequada, qualquer intervenção que afete a autodeterminação informacional. É necessário, assim, indicar a finalidade e os limites conferidos ao tratamento de dados em padrão específico, preciso e claro para cada área. Quanto à dimensão objetiva, existe um dever de proteção

[19]Trata-se do anteprojeto elaborado por uma comissão de juristas designada pelo Presidente da Câmara de Deputados, sob a presidência do Ministro do Superior Tribunal de Justiça Nefi Cordeiro. Disponível em: <https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf> Acesso em 30 dez. 2020.
[20]Brasil. Supremo Tribunal Federal. ADI 6387, Rel. Min. Rosa Weber, julgado em 7 de maio de 2020.
[21]SOLOVE, 2011, p. 61;
[22]Brasil. Supremo Tribunal Federal. ADI 6387, Rel. Min. Rosa Weber, julgado em 7 de maio de 2020, p. 20.

estatal do direito à autodeterminação informacional, a ser efetivado por meio de normas de organização e procedimento (*Recht auf Organisation und Verfahren*) e normas de proteção (*Recht auf Schutz*). Assim, não basta assegurar o respeito e a governança, é necessário dotar as instituições dos mecanismos necessários para fazer valer esse direito fundamental, o que se dá por meio de uma autoridade independente de proteção de dados, na esteira do art. 8º da Carta de Direitos Fundamentais da União Europeia.

O julgamento proferido pelo STF confere balizas para a análise do anteprojeto a ser discutido no Congresso, além de indicar parâmetros constitucionais e democráticos que servem ao desenvolvimento do policiamento preditivo no país. Há necessidade de que legislação seja elaborada com alto grau de deferência democrática, associada à estrita observância do princípio da proporcionalidade na utilização de dados pessoais e no controle do enviesamento das tecnologias são aspectos fundamentais.

No campo do reconhecimento facial, por exemplo, o Distrito Federal aprovou a Lei nº 6.172, de 10 de novembro de 2020, que dispõe especificamente sobre o uso dessa tecnologia. Em 10 artigos, a lei proíbe a vigilância contínua de indivíduos ou grupos de indivíduos por reconhecimento facial (art. 3º), e estabelece que o seu uso na segurança pública está restrito a equipamentos públicos em espaços públicos, devendo haver publicidade quanto à sua aplicação (art. 4º). A lei classifica os dados como sensíveis e proíbe o tratamento por pessoas de direito privado. Não há, contudo, clareza quanto à forma de organização e sistematização de dados, tampouco o período de armazenamento ou a possibilidade de destruição. É necessário definir o objetivo do sistema, examinar a forma de uso e ter conhecimento acerca do banco de dados de referência. Mostra-se imprescindível, ainda, observar a proporcionalidade da utilização dessa tecnologia, o que demonstra a necessidade de regulação exaustiva sobre o tema.

De forma incipiente, a Lei Geral de Proteção de Dados (Lei federal nº 13.709/2018) trouxe uma extensa regulação do tratamento de dados no Brasil inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e diversos princípios relevantes a se irradiarem por todas as atividades que demandem tratamento de dados, tais como a necessidade de respeito à privacidade, autodeterminação informativa, inviolabilidade da intimidade, honra e da imagem e o consentimento prévio como regra.

Apesar disso, a LGPD não se aplica ao tratamento de dados realizados para fins exclusivos de segurança pública, seguindo o modelo europeu[23] que reserva ato normativo próprio ao tratamento

[23] Na Europa, o tratamento de dados em segurança pública é regulado pela Diretiva 2016/680;

de dados no âmbito da segurança pública.

Desse modo, atualmente, não há qualquer óbice legal ou condicionantes à realização de tratamento de dados na segurança pública. Vale ressaltar que, no Brasil, há diversos exemplos de utilização de algoritmos preditivos na segurança pública e, inclusive, de erros crassos decorrentes de seu manuseio (NUNES, 2021). Nesse sentir, ante a lacuna de regulação legislativa sobre o tema e a definição, pelo Supremo Tribunal Federal, da proteção de dados pessoais como um direito fundamental, as experiências de uso de tecnologia na segurança pública devem receber um olhar ainda mais crítico, quanto à constitucionalidade e transparência, pelo Poder Judiciário, ainda mais diante da baixa publicidade e de clareza informacional sobre os dados que estão sendo coletados.

A fim de suprimir a ausência de amparo legal à proteção de dados na segurança pública, uma comissão de juristas elaborou um anteprojeto de lei que está sendo avaliado pela Presidência da Câmara dos Deputados. Em seus 68 artigos, o anteprojeto estipula salvaguardas e prevê a elaboração de "relatório de impacto" para tratamento de dados sensíveis, sigilosos ou que representem risco para direitos fundamentais do titular ou que possam acarretar medidas coercitivas ou restritivas de direito, que possam gerar decisões automatizadas e, ainda, a utilização de tecnologias de monitoramento.

Conforme o anteprojeto, o relatório de impacto seria uma "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco". Em específico, previu-se que o referido relatório deverá "conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" (art. 29, §3º).

A mera previsão de elaboração e publicação de relatório de impacto é medida que, em tese, trará maior *accountability* aos processos de tratamento de dados, permitindo aos cidadãos afetados a possibilidade de questiona-los quando representarem riscos incompatíveis com a ordem constitucional.

Outra importante salvaguarda no anteprojeto é a *deferência democrática* ao se exigir comando legal específico para o tratamento de dados sensíveis[24], sigilosos, na utilização de tecnologia de monitoramento e no tratamento de dados de elevado risco, nas quais a potencialidade

[24] "Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou dado biométrico".

de dano a direitos, garantias e liberdades de titulares é alta. Nesses casos, há necessidade, ainda, de elaboração de análise de impacto regulatório para instruir o processo legislativo. Nesse sentido, o objetivo do anteprojeto é agir como uma *metanorma* ao delinear aspectos do processo legislativo que potencialmente acarretará na legislação sobre tratamento de dados na segurança pública. Um aspecto relevante consiste na necessidade de que a análise de impacto regulatório seja submetida à "consulta pública com ampla participação social", o que reforça a *deferência democrática* da previsão de lei específica.

Ademais, o anteprojeto também trouxe previsões específicas quando o tratamento de dados gerar decisões automatizadas, como a supramencionada utilização de mecanismos de policiamento preditivo por meio do manuseio de big data, como *focused deterrence*, *heat list* e *math and murder*.

Inicialmente, toda decisão tomada com base no tratamento automatizado de dados pessoais deve ser precedida, além da publicação do relatório de impacto, de autorização do CNJ (órgão supervisor). Quando essas decisões ensejarem um elevado risco para os direitos fundamentais do titular ou que possam acarretar medidas coercitivas ou restritivas de direitos, estas deverão ser precedidas de autorização do CNJ e autorizadas por Lei a ser instruída com análise de impacto regulatório.

Além disso, a fim de superar a problemática acerca da falta de opacidade e caráter racializante de alguns algoritmos, o anteprojeto prevê que os sistemas deverão ser auditáveis, não discriminatórios e passíveis de comprovação de sua precisão e grau de acurácia. Prevê-se especificamente a possibilidade de o CNJ realizar auditoria com o fim de analisar a existência de vieses e aspectos discriminatórios no tratamento automatizado de dados pessoais, entre outros pontos.

Em específico quanto à garantia de não-discriminação e transparência, o anteprojeto prevê especificamente que se deve analisar o "peso de dados pessoais, incluindo aqueles referentes à situação socioeconômica e os dados demográficos relacionados à residência ou os demais, sejam potencialmente capazes de revelar informações sensíveis" e que a auditoria destes aspectos deverão avaliar a "precisão, incluindo a taxa de falsos positivos ou falsos negativos", e a "reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento".

Foi prevista a possibilidade de revisão da decisão automatizada por uma pessoa natural e veda a adoção de medida coercitiva ou restritiva de direitos exclusivamente com base em decisão automatizada. O anteprojeto, ainda, estipula a impossibilidade de restrição de auditoria dos sistemas responsáveis por decisões automatizadas em razão de segredo industrial e comercial, em relevante

avanço em relação à utilização destes sistemas em outros países onde ainda se defende a necessidade de preservação destes em detrimento da transparência dos algoritmos.

O anteprojeto trata, também, de tecnologias de monitoramento, consistentes em "equipamento, programa de computador ou sistema informático que possa ser usado ou implementado para tratamento de dados pessoais captados ou analisados em vídeo, imagem, texto ou áudio" (art. 5º, inc. XXIII). Estas devem ser precedidas de previsão legal específica, análise de impacto regulatório e relatório de impacto à proteção de dados. Na era do "capitalismo de vigilância", a definição de balizas para a realização de monitoramento de cidadãos é medida de maior relevância para a proteção de direitos fundamentais.

Quanto à avaliação de riscos, o anteprojeto impõe a consideração, ao menos, de pontos como a natureza dos dados pessoais envolvidos, as finalidades específicas do tratamento, a quantidade de agentes de tratamento de dados envolvidos, a quantidade de titulares de dados potencialmente atingidos, existência de nova tecnologia, a possibilidade de tratamento discriminatório e as expectativas legítimas do titular de dados.

Ademais, o anteprojeto também traz requisitos específicos a serem observados na análise de impacto regulatório[25] e o estabelecimento de uma política de uso e garantias dos direitos dos titulares[26]. Ao final, o anteprojeto veda a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.

---

[25] § 2º O processo legislativo será instruído de análise de impacto regulatório que contenha: I - uma descrição do escopo do tratamento e das capacidades da tecnologia de vigilância; II - quaisquer testes ou relatórios relativos aos efeitos do tratamento e da tecnologia de vigilância na saúde e na segurança de pessoas; III - quaisquer impactos potencialmente díspares do tratamento de dados e da tecnologia de vigilância ou de sua política de uso em quaisquer populações específicas; IV - as medidas previstas para fazer frente aos riscos mencionados nos incisos anteriores; V - as garantias, as medidas de segurança e os mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade do tratamento com a presente lei; e VI - a política de uso e as garantias dos direitos dos titulares, conforme o disposto no § 3º deste artigo.

[26] § 3º A lei deve estabelecer política de uso que garanta os direitos dos titulares de dados e contenha: I - regras, processos e diretrizes emitidas pela autoridade competente que regulem o tratamento de dados, incluindo o acesso e o uso interno de tal tecnologia de vigilância; II - salvaguardas ou medidas de segurança destinadas a proteger as informações coletadas por tal tecnologia de vigilância contra o acesso não autorizado, incluindo, mas não se limitando à existência de criptografia e mecanismos de controle de acesso; III - políticas e práticas relacionadas à retenção, acesso e uso dos dados tratados; IV - políticas e procedimentos relativos ao acesso ou uso dos dados tratados por meio de tal tecnologia de vigilância por membros do público; V - as hipóteses de uso compartilhado, se admitido; VI - se algum treinamento é exigido pela autoridade competente para um indivíduo realizar o tratamento, usar tal tecnologia de vigilância ou acessar informações tratadas; VII - uma descrição da auditoria interna e mecanismos de supervisão dentro da autoridade competente para garantir a conformidade com a política de uso que rege o uso de tal tecnologia de vigilância. VIII - diretrizes sobre realização, atualização e revisão do relatório de impacto de proteção de dados pessoais.

Como se observa, as medidas previstas no anteprojeto demonstram uma preocupação legislativa em evitar violações a direitos fundamentais através da adoção de mecanismos que reforçam a *accountability* e *deferência democrática* do acréscimo destes instrumentos tecnológicos no policiamento. Tanto o anteprojeto de Lei quanto o julgamento da ADI pelo Supremo Tribunal Federal demonstram avanços no panorama brasileiro de tratamento de dados pessoais no âmbito da segurança pública. Ambos demonstram a relevância da fixação de parâmetros objetivos para resguardar os direitos fundamentais dos cidadãos sem prejudicar a consecução de atividades de policiamento e segurança pública no país dentro de um marco constitucional democrático e que confira *accountability,* deferência democrática e respeito à autonomia dos indivíduos.

CONSIDERAÇÕES FINAIS

O Brasil observou ao longo das últimas décadas um exponencial aumento de violência em todas as suas regiões. Paralelamente, as políticas de segurança pública até então implementadas se demonstraram insuficientes para lidar com a crescente criminalidade. Dessa forma, a adoção de inovações tecnológicas aptas a auxiliar na repressão de práticas criminosas e prevenção de ilícitos surge como uma janela de oportunidades para equipar o aparato de segurança estatal de meios adequados para a execução de sua missão constitucional.

No caso do policiamento preditivo, um possível resultado é a maior efetividade na atuação policial pela utilização mais eficientes dos dados disponíveis por meio de algoritmos para prevenir e impedir ilícitos. Por outro lado, esses algoritmos também trazem alguns riscos, tais como a inclusão de viés racializante nos programas utilizados e violações de direitos fundamentais das pessoas cujos dados sofreriam tratamento.

Com vistas a equilibrar os interesses envolvidos, é necessário construir um modelo constitucional e democrático para a regulação dos algoritmos a serem utilizados no policiamento preditivo. Como indicativo de características a serem buscadas na regulação, destacam-se a deferência democrática, compatibilidade dos *inputs* e *outputs* do sistema com a ordem constitucional e busca pela eficiência, *accountability* dos responsáveis por estes e respeito à autonomia das pessoas afetadas pela tecnologia.

Atualmente, esses algoritmos e mecanismos de policiamento preditivo estão em plena utilização no Brasil, sem que exista qualquer regulação para seu manuseio. Há, portanto, um estado de coisas propício ao cometimento de erros, violações de direitos fundamentais e dificuldade na

responsabilização. As indicações da ADI 6387 e a aprovação de legislação sobre o tema poderão pavimentar o caminho para uma solução ponderada ao tema. Além disso, é fundamental que as premissas constitucionais e democráticas sejam internalizadas pelos órgãos de segurança pública, sob pena de a tecnologia apenas reproduzir, de forma acrítica e aparentemente neutra, um modelo enviesado de atuação das polícias.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAUJO, Valter Shuenquener de. Efeitos da inovação no direito administrativo brasileiro: queremos saber o que vão fazer com as novas invenções. *Quaestio Iuris,* vol. 11, no. 03, Rio de Janeiro, 2018. pp. 1687-1703

BALKIN, Jack M. Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *University of California, Davis.* Vol. 51:1149, 2018.

BAPTISTA, Patrícia e KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, Vol. 273, 2016, p. 127

BINENBOJM, Gustavo. *Uma Teoria do Direito Administrativo*: direito fundamentais, democracia e constitucionalização. 3ª Ed. Rio de Janeiro: Ed Renovar, 2014

CHRISTENSEN, Clayton M; BOWER, Joseph L. Disruptive techonologies: catching the wave. *Harvard Business Review,* Jan-Fev 1995

DAVIS, Angela. *A democracia da abolição*: para além do império, das prisões e da tortura. Tradução de Artur Neves Teixeira. 2ª ed. Rio de Janeiro: Difel, 2019.

FERGUSON, Andrew Guthrie. *The rise of Big Data policing*: surveillance, race, and the future of law enforcement. New York: New York University Press, 2017.

FRIEDMAN, Barry. *Unwarranted*: policing without permission. New York: Farrar, Straus and Giroux, 2017.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014

O'NEIL, Cathy. *Weapons of math destruction*: How Big Data increases inequality and threatens democracy. New York: Broadway Books, 2016.

SAUNDERS, Jennifer; HUNT, Priscila; HOLLYWOOD, John S. Predictions Put into Practice: a quasi-exxperimental evaluation of Chicago's Predictive Policing Pilot. 12 J. *EXPERIMENTAL CRIMINOL*. 347, 355-65 (2016).

SOARES, Luiz Eduardo. *Desmilitarizar*: segurança pública e direitos humanos. São Paulo: Boitempo, 2019.

SOLOVE, Daniel J. *Nothing to hide*: The false tradeoff between privacy and security. Yale University Press, 2011.

SOUZA NETO, Cláudio Pereira de. A segurança pública na Constituição Federal de 1988: conceituação constitucionalmente adequada, competências federativas e órgãos de execução das políticas. *Atualidades jurídicas*, Brasília, n. 1, mar./abr. 2008.

TRUBNIKOV, Dmitrii. Analysing the Impact of Regulation on Disruptive Innovations: The Case of Wireless Technology. *J Ind Compet Trade (2017)* 17:399–420. DOI 10.1007/s10842-016-0243-y

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. New York: Public Affairs, 2019

Sobre os autores:

Valter Shuenquener de Araujo
Professor Associado da Faculdade de Direito da UERJ, Departamento de Direito do Estado, Mestre e Doutor em Direito Público pela UERJ e KZS pela Ruprecht-Karls Universität de Heidelberg
Universidade do Estado do Rio de Janeiro - UERJ, Rio de Janeiro, RJ, Brasil
Lattes: http://lattes.cnpq.br/8284713431239760 ORCID: https://orcid.org/0000-0003-1584-5340
E-mail: saraujo19@gmail.com

Júlio José Araujo Junior
Mestre em Direito Público pela Universidade do Estado do Rio de Janeiro (UERJ). Doutorando em Direito Público pela UERJ. É especialista em Política e Sociedade pelo Instituto de Estudos Sociais e Politicos (IESP-UERJ). Procurador da República.
Universidade do Estado do Rio de Janeiro - UERJ, Rio de Janeiro, RJ, Brasil
Lattes: http://lattes.cnpq.br/2244172481620032
E-mail: juliojaraujo@gmail.com

Lucca Fernandes de Albuquerque
Mestrando em Direito na UERJ na linha de pesquisa em Direito Público. Possui especialização em Direito Público pela Universidade do Estado do Amazonas (2018).
Universidade do Estado do Rio de Janeiro - UERJ, Rio de Janeiro, RJ, Brasil
E-mail: lucca.albuquerque93@gmail.com

Os autores contribuíram igualmente para a redação do artigo.