O PARADIGMA DA IMPLANTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA BRASILEIRA: REGULAÇÃO VERSUS EFICIÊNCIA

Gleiner Pedroso Ferreira Ambrosio*
André Luis Jardini Barbosa**

RESUMO

A utilização da tecnologia da Inteligência Artificial (IA) tem se mostrado cada vez mais presente na sociedade em suas diversas áreas, sendo a esfera penal um dos mais notáveis exemplos de tal fenômeno. Isso porque os elevados índices de criminalidade violenta e patrimonial demandam estratégias frequentemente inexequíveis aos órgãos de segurança pública no Brasil, que enxergaram a adoção de algoritmos e sistemas de policiamento preditivo no campo internacional como uma oportunidade de auxílio no enfrentamento a esse cenário. Todavia, a despeito deste possível avanço, sua adoção tem demonstrado uma sujeição muito maior à discricionariedade das políticas públicas dos governos executivos do que à própria justiça enquanto fim, de forma que as legislações regulamentadoras de proteção de dados e IA pouco trataram da utilização dessa tecnologia no Direito Penal, sujeitando a coletividade não apenas aos perigos da criminalidade, mas também à insegurança da própria ferramenta de prevenção criminal, acometida de falhas metodológicas, vazamento de dados e até mesmo de um viés discriminatório. Assim, o presente artigo propõe traçar, metodologicamente, uma análise acerca da relação entre eficiência e a necessária regulação do uso de tal tecnologia na segurança pública, aplicar tal discussão a duas ferramentas atualmente utilizadas em diferentes estados do Brasil e trazer um contraponto ao seu estágio de discussão na esfera internacional, permitindo concluir o diagnóstico sobre a real falta de legitimidade de seu uso tecnológico no território nacional.

Palavras-chave: policiamento preditivo; algoritmo; inteligência artificial; atividade criminal.

Data de submissão: 31/03/2024
Data de aprovação: 18/08/2024

* Bacharel em Direito pela Universidade Presbiteriana Mackenzie. Pesquisador nas áreas de Direito Econômico-Concorrencial e Segurança Pública e Cidadania pela mesma instituição.

** Doutor em Direito pela FADISP, Mestre em Direito pela UNESP e especialista em Direito Processual Penal pela Escola Paulista da Magistratura. Delegado de polícia do Estado de São Paulo e professor universitário

THE PARADIGM FOR IMPLEMENTING ARTIFICIAL INTELLIGENCE IN BRAZILIAN PUBLIC SECURITY: REGULATION VERSUS EFFICIENCY

Gleiner Pedroso Ferreira Ambrosio
André Luis Jardini Barbosa

ABSTRACT

The use of Artificial Intelligence (AI) technology has become increasingly present in society in its various areas, with the criminal sphere being one of the most notable examples of this phenomenon. This is because the high rates of violent and property crime require strategies that are often unfeasible for public security agencies in Brazil, which have seen the adoption of algorithms and predictive policing systems in the international field as an opportunity to help tackle this scenario. However, despite this possible advance, its adoption has been much more subject to the discretionary public policies of executive governments than to justice itself as an end, so that the laws regulating data protection and AI have dealt little with the use of this technology in criminal law, subjecting the community not only to the dangers of crime, but also to the insecurity of the crime prevention tool itself, beset by methodological flaws, data leaks and even a discriminatory bias. Thus, this article proposes a methodological analysis of the relationship between efficiency and the necessary regulation of the use of such technology in public security, applying this discussion to two tools currently used in different states in Brazil and providing a counterpoint to their stage of discussion in the international sphere, allowing us to conclude the diagnosis on the real lack of legitimacy of their technological use in the national territory.

Keywords: predictive policing; algorithm; artificial intelligence; criminal activity.

Date of submission: 31/03/2024
Date of approval: 18/08/2024

INTRODUÇÃO

Ao longo das 4 (quatro) revoluções tecnológicas pelas quais a humanidade passou, sempre houve diferentes tempos de assimilação da sociedade para com as mudanças propostas por tais acontecimentos. De modo exemplificativo, é possível mencionar que a 1ª Revolução Industrial (séc. XVIII), que implicou em uma radical mudança nos meios de produção na sociedade inglesa, foi rapidamente inserida no convívio social ao alterar os meios de produção e as relações de trabalho então existentes, abarcando ramos como o da indústria têxtil, metalúrgica, entre outros. Por outro lado, a 3ª Revolução Industrial (séc. XX), responsável pelo desenvolvimento das áreas de telecomunicação, computação e sobretudo pelo advento da internet, teve uma maior dificuldade de implantação globalmente, fazendo com que países que apresentassem maior desenvolvimento econômico-social (como os EUA e outras potências europeias) conseguissem assimilar tais evoluções quase que de forma monopolista, pois quando países em desenvolvimento finalmente tinham acesso a essas novas tecnologias, quase sempre já se encontravam defasadas.

Ora, ao se adentrar na presente Revolução 4.0, não nos cabe, contemporaneamente, fazer uma comparação com as anteriores do ponto de vista da inovação, pois todas tiveram em seu bojo profundas modificações na ordem de funcionamento da sociedade. Porém, é inegável que a 4ª Revolução Tecnológica não só incide no maior número de áreas a serem transformadas como, também, mostra que tais transformações passam a ser cada vez mais indispensáveis à sociedade, pois se na 1ª Revolução Industrial, por exemplo, a manufatura ainda representava uma alternativa de produção, em pleno século XXI, é impossível se abster das transformações provenientes (e futuras) da 4ª Revolução Tecnológica, e uma destas reside justamente no emprego da Inteligência Artificial (IA).

A IA já é uma realidade global que afeta a realidade de milhões de pessoas. Por essa razão, a atração de órgãos públicos e privados pelo fenômeno tem se intensificado ano após ano, sendo aplicado no gerenciamento de dados populacionais, de dados de contratados de empresas, na organização de banco de dados, na captação e entrada de frequentadores de estádios de futebol, dentre tantos outros exemplos. Dentre eles, no entanto, aquele que mais tem tomado a atenção da sociedade nos últimos anos corresponde ao uso de algoritmos de IA na área de segurança pública, tendo o Brasil iniciado os primeiros passos em sua adoção recentemente.

A rigor, o Brasil ainda não tem um sistema de policiamento preditivo propriamente completo sendo aplicado, consistindo majoritariamente em bancos de dados com informações compartilhadas entre autoridades policiais. Porém, mesmo que tal configuração constitua um elemento fundamental por parte de qualquer sistema de policiamento preditivo consolidado, ainda há a carência um ponto central da tecnologia: a correlação dos dados captados por meio do algoritmo:

No Brasil ainda se caminha a passos curtos quando o assunto é política criminal. Não temos um projeto tecnológico consolidado sobre policiamento preditivo, senão alguns sistemas esparsos utilizados por forças policiais com processamento de dados e pesquisa criminal. O que temos são informações compartilhadas entre as entidades que trabalham na persecução penal com

informações policiais integradas, sem que exista um programa capaz de atender as demandas operacionais e realizar o policiamento preditivo (Moraes, 2022, p. 57)

Ainda assim, alguns poucos governos já começaram a aplicar tecnologias muito mais próximas daquelas utilizadas no campo internacional, como o Detecta (Governo de São Paulo), o Córtex (Governo Federal) e o Sistema de Atendimento e Despacho de Emergências (SADE) (PM do Paraná), de forma que, em maior ou menor grau, tais programas já se utilizam de tecnologias com algoritmos fazendo o cruzamento dos dados captados, e não apenas realizando o armazenamento. E como será visto mais adiante, não só casos como o do Detecta já conseguiram trazer resultados numerosos à polícia paulista como, também, são diversos os estados e municípios que passaram a utilizar câmeras de reconhecimento facial , drones com captação de imagens e afins, ferramentas estas já na esteira do maior escopo proporcionado por algoritmos de policiamento preditivo, reforçando uma tendência de incremento na adoção de tecnologias preditivas que, claro, também podem reforçar a expansão para o uso de algoritmos em escala nacional.

Mesmo assim, ainda que tal implementação aparente representar uma evolução tecnológica em prol da segurança pública brasileira, assim como foi dito nos primeiros parágrafos em relação à 3ª Revolução Tecnológica, transformações tão radicais como essa podem implicar em uma série de limitações (e perigos) em seu processo de implantação. E, sendo o Brasil um país em desenvolvimento e com uma infraestrutura de proteção de dados ainda incipiente, a gravidade pode ser ainda maior. A prova disso é que tal tecnologia vem sendo questionada e descontinuada em vários projetos ao redor do mundo, fenômeno este que já se manifestou negativamente desde os recentes princípios de sua inserção no Brasil.

Nesse sentido, o presente artigo buscará traçar um panorama de como o campo de proteção de dados se encontra amparado na realidade brasileira, como isso reflete no emprego de algoritmos de IA no campo da segurança pública brasileira, quais as possíveis intervenções a serem feitas na relação entre tal gestão de dados (tanto do ponto de vista legislativo quanto da prática policial) e como seria sua aplicação na segurança pública dos estados.

1 SEGURANÇA DE DADOS NO BRASIL

A proteção de dados pessoais, de uma forma geral, não constitui questão originária no ordenamento brasileiro, já que a própria Constituição Federal de 1988, em sua promulgação, apenas previa uma proteção à intimidade do indivíduo: "Art. 5°, X, CF: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Porém, antes mesmo nas décadas de 70 e 80, a legislação europeia já vinha buscando uma proteção direcionada à forma como os dados pessoais eram geridos por terceiros, ponto em que, a partir da 1978, países como França, Noruega, Suécia e Áustria já entraram com processo de instauração normativa de tal natureza (Brancher, 2022).

Seguindo esse *status* europeu, em outubro de 1995, o Parlamento Europeu e o Conselho da União Europeia lançaram a Diretiva 95/46/CE, responsável por efetivamente consolidar os meios de gestão, direcionamento e responsabilização

pelo uso de dados no contexto do continente, o que acabou por vincular ainda mais países-membros à elaboração de leis específicas em suas jurisdições.

Naturalmente, tal movimento haveria de reverberar no Brasil. No ano de 1991, para além do importante artigo 11º, capítulo 3, do Código de Defesa do Consumidor ("Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento"), a proteção de dados deixou de se limitar ao contexto consumerista e ganhar cada vez mais espaço em outras áreas.

O primeiro passo veio com a lei 9.296 de 1996, que acrescentou à redação constitucional a proteção ao sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas[1]. Porém, do ponto de vista técnico, ainda era algo bem limitado, demandando uma legislação específica para tanto.

Foi aí que, anos mais tarde, com o desencadeamento do Caso Snowden (2013), foi descoberto que até mesmo conversas pessoais da então presidente Dilma Rousseff estavam sendo monitoradas por terceiros, inclusive por parte de autoridades estrangeiras. Ora, se a própria Presidente, ostensivamente protegida por forças de segurança especiais, foi exposta a tal ataque, quanto pior poderia ser a toda a população. Assim, diante de tal preocupação, o então projeto de Marco Civil da Internet, que já vinha sendo discutido há anos, ganhou maior celeridade, entrando em vigor no ano de 2014.

Sua sanção, juntamente com a presente LGPD (2020), representa um importante passo no campo de proteção de dados no Brasil, dispondo de propósitos bem alinhados àqueles da Diretiva 95/46/CE. E, como substrato de tais documentos, devem ser destacadas três diretrizes centrais à aplicação dos algoritmos em suas mais diversas áreas de aplicação, de forma que não possam ser ignoradas pelos gestores dos dados, quais sejam:

i) Dever de informar quais os dados coletados;
ii) Dever de informar o tempo de armazenamento, devendo ser verificado se possuem natureza identificável e removível (art. 40, LGPD); e
iii) Justificar qual será a destinação dada aos dados *in casu* (art. 6º, II, LGPD).

De forma geral, tais princípios estendem uma proteção a várias áreas relevantes que empregam o uso da IA, mas outras, certamente, possuem demandas mais delicadas e urgentes, sendo uma delas a da segurança pública.

O grande problema do emprego da IA na segurança pública é que, se tal obediência já é acometida por uma série de controvérsias nos campos de prestação de serviços, relações de consumo, redes sociais e afins, quando tais dados são aplicados em algoritmos e sistemas de policiamento preditivo, sua gestão tende a ser mais problemática, pois com a atual legislação (MCI e LGPD) não delimitando especificamente a operabilidade dos algoritmos de policiamento preditivo, os estados e municípios vem adotando quase que uma "autorregulamentação" em sua

[1] CF, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

aplicação, fazendo com que erros parciais (discriminação algorítmica) e imparciais (falhas metodológicas), por exemplo, sejam de difícil fiscalização:

> Diante do aparente conflito entre avanços tecnológicos e restrições regulatórias, pode-se observar como os Estados vem consistentemente optando pela via da auto-regulamentação (mesmo que às vezes se esforcem na divulgação e publicação de documentos de soft law), talvez na esperança de que os marcos legais existentes sejam suficientes para contrabalançar as falhas dos algoritmos (Menezes; Sanllehí, 2021, p. 108).

Assim sendo, são levantados os seguintes questionamentos: diante dos avanços na aplicação de tais algoritmos, com qual realidade a legislação brasileira de proteção de dados e os órgãos fiscalizadores devem lidar perante a referida autorregulação de seu emprego pelos poderes executivos e suas respectivas forças policiais? Até que ponto uma maior regulação (seja legislativa, seja de órgãos superiores do judiciário) se faz necessária frente à eficiência proposta por tal tecnologia? Tais pontos serão desenvolvidos a seguir.

2 REFLEXOS E IMPACTOS ATUAIS NA SEGURANÇA PÚBLICA BRASILEIRA

Do ponto de vista constitucional, o legislador brasileiro expressou uma especial preocupação na manutenção e garantia da segurança pública a partir do art. 144, caput, da CF, com o duplo objetivo de "(i) preservação da ordem pública e (ii) da incolumidade das pessoas", tarefa essa correspondente às forças policiais descritas nos incisos do mesmo artigo, quais sejam: I- polícia federal; II- polícia rodoviária federal; III- polícia ferroviária federal; IV- polícias civis; V- polícias militares e corpos de bombeiros militares e VI- polícias penais federal, estaduais e distrital.

Com os órgãos policiais representando a *longa manus* do, ora, suas diferentes atuações refletem não apenas os parâmetros legais, constitucionais e infraconstitucionais, mas também o próprio planejamento da segurança pública dos municípios, dos entes federados e da própria federação brasileira. Por isso, estudar a aplicação de tecnologias pelas forças policiais no campo da segurança pública significa estudar os atos do poder público! A prova disso é que, dentre os casos concretos pelos quais os sistemas de policiamento preditivo tiveram alguma inserção no território brasileiro, quase sempre sua inserção partiu do posicionamento dos governos estaduais aos quais os agentes policiais eram subordinados, conforme será demonstrado nos casos a seguir.

2.1 GOVERNO DO ESTADO DO PARANÁ

A partir do ano de 2014, o Governo do Estado do Paraná celebrou um convênio com a Universidade de Chicago, tendo por objetivo a implantação de um sistema de análise preditiva voltado à prevenção e ao combate à criminalidade, fundamentado na análise desenvolvida pela conhecida empresa californiana *PredPol*, *The Predictive Policing Company* (Ensign; Friedler; Neville; Scheidegger; Venkatasubramanian, 2018, p. 3). Sua aplicação, baseada no uso de algoritmos

referentes a locais, datas e horários de incidência criminal anterior, permitiria aos órgãos policiais o preciso estabelecimento de parâmetros de definição de delitos futuros responsáveis por orientar e nortear a atuação policial a partir de seus dados gerados.

Tal convênio tinha como objetivo a transferência da tecnologia de um sistema que havia sido implementado na cidade de Chicago (EUA), baseando-se no cruzamento de "diversos padrões para tentar alcançar uma predição dos crimes, incluindo o grau de periculosidade de pessoas que possam ser abordadas e futuramente proporcionar que a Secretaria de Segurança Pública (SESP) desenvolva seus próprios métodos" (Oliveira Júnior; Santos, 2022, p. 50). O problema foi que, desde então, "não foram encontrados quaisquer registros de resultados práticos ou ações em andamento que sejam frutos dessa cooperação técnica" (Oliveira Júnior; Santos, 2022, p. 50).

Por isso, anos mais tarde, foi desenvolvida uma nova tecnologia menos ambiciosa, mas também com o objetivo de auxiliar na predição policial denominada Sistema de Atendimento e Despacho de Emergências (SADE), cujo foco do cruzamento de dados seria auxiliar no despacho de equipes policiais mais próximas ao local da ocorrência com base na geolocalização da viatura policial, com todo o processo sendo feito de forma automatizada (Oliveira Júnior; Santos, 2022). Todavia, no seu estágio experimental, foi possível constatar um novo benefício que o sistema permitiria em sua aplicação, descrito pelo SADE em seu informativo da seguinte forma: "Uso de Inteligência Artificial visando à aplicabilidade lógica do efetivo e meios disponíveis" (PMPR, 2022, on-line), demonstrando que o mero auxílio na predição dos locais mais propícios para o despacho policial evoluiu para uma maior autonomia do sistema na indicação da ocorrência de crimes – o que foi comprovado após sua fase experimental de aplicação, sendo utilizada até mesmo para programar o próprio sistema para a confecção dos relatórios de serviço (Santos, 2023), chegando a preparar relatórios diferenciados tanto para a própria polícia quanto relatórios externos para a imprensa, devido à necessária proteção de dados sigilosos.

Além da sua aplicação experimental como projeto-piloto na cidade de Apucarana, situada na região centro-norte do Paraná e pertencente à região do 2º Comando Regional de Polícia Militar (2º CRPM) e à área do 10º Batalhão de Polícia Militar (10º BPM), a tecnologia já tem proposta de extensão para os demais municípios do estado posteriormente.

Bem, feita essa exposição, em momento anterior do presente estudo, tivemos a oportunidade de afirmar que os métodos de policiamento preditivo e utilização de algoritmos em muito podem contribuir para o sistema até então vigente de atuação policial preventiva e para a investigação de crimes em termos numéricos. Mas antes de se compreender qual a racionalidade por trás da aplicação da tecnologia preditiva, o primeiro passo a ser dado é entender como o serviço de mapeamento da análise criminal em um determinado local ocorre em sua forma "manual", ou seja, antes do emprego da tecnologia. A esse respeito, mostra-se oportuna a apresentação metodológica da atuação tradicional da Polícia Militar do Estado do Paraná no tocante à atuação preventiva relativa aos crimes envolvendo drogas, que segue a seguinte dinâmica:

> a. Vítima/Alvo
>
> - Grande circulação de funcionários e usuários do comércio local e do transporte público.
>
> b. Criminoso/infrator
>
> - Massiva presença de moradores de rua e pessoas em situação de vulnerabilidade social em toda a Vila [...], estes mais propensos à prática de delitos como roubo e furto, devido à sua condição social;
>
> - Conivência dos moradores locais com algumas práticas delitivas ali presentes, principalmente em relação ao tráfico de entorpecentes, observada pela escassez de denúncias acerca de tal delito mesmo diante de sua grande incidência no local;
>
> - Divisão estratégica de funções e tarefas entre os infratores, a exemplo dos "olheiros" presentes nas esquinas das praças, estes atentos para avisar aos demais criminosos sobre a presença de policiamento nas proximidades;
>
> c. Lugar
>
> - Grande quantidade praças dentro da Vila [...], em sua maioria extensas e que possibilitam um bom campo de visão ao infrator, permitindo também a percepção antecipada da presença do policiamento local, facilitando a fuga da abordagem e a dispensa dissimulada de objetos do crime;
>
> - Considerável quantidade de casas abandonadas e terrenos baldios, próprios para o esconderijo dos infratores e depósito de objetos relacionados ao crime (drogas, armas, pertences de vítimas).
>
> - Iluminação deficiente em diversos locais da Vila [...] (Pereira, 2020, p. 3).

Desses dados, depreende-se que a análise perpetrada pelo agente policial se baseia em um traçado triangular do crime – (I) vítima/alvo, (II) criminoso/infrator e (III) lugar, com estas três etapas apresentando uma clara relação de consequência entre si, de forma que, caso todas se alinhem quanto ao potencial da ocorrência de crimes, a atuação policial deverá incidir neste caso.

Porém, a despeito da relevância desse método de atuação policial aparentemente bem organizado, é inegável que sua aplicação se mostrou absolutamente limitada a fatores próprios como o subjetivismo do agente policial e até mesmo dos infratores, que ao perceberem a presença da polícia nos arredores de seu âmbito de ação, certamente procurarão por novos locais para o cometimento daqueles crimes, pois não faz sentido cometer delitos onde o destacamento policial está instaurado, mostrando não só um problema de eficiência como também de possíveis abusos que podem ocorrer em relação às vítimas.

Agora, a pergunta que precisa ser feita é: como a tecnologia de policiamento preditivo será usada de forma diferente do que é feito pelo agente policial se a programação do algoritmo de policiamento preditivo é feita com pressupostos igualmente subjetivos? Se a tecnologia é criada por homens com os mesmos pressupostos de atuação, ora, essa tecnologia nada mais fará do que reproduzir os

subjetivismos daquele que criou a tecnologia, mas agora de forma automatizada. E ainda que a ferramenta referida não disponha do algoritmo de policiamento preditivo, as tecnologias de armazenamento de dados e de vigilância, como drones, câmeras corporais e sistema integrado de dados, ainda assim serão empregadas de forma a auxiliar esse subjetivismo da atuação policial.

É claro que tudo isso traz preocupações à sociedade, mas a tecnologia aqui analisada ainda tem uma atuação muito localizada. Já o próximo caso, referente ao sistema "Detecta", possui um escopo maior de atuação e um maior espaço amostral dos resultados de sua aplicação, o que torna possível não apenas a manifestação de tais problemas em maior escala como, também, propicia o surgimento de novas e mais urgentes preocupações.

2.2 GOVERNO DO ESTADO DE SÃO PAULO

O sistema de vigilância que o Governo do Estado de SP vem implementando – com alterações cotidianas e de velocidade praticamente imediata – é denominado Detecta (sistema inteligente de monitoramento criminal). Partindo do modelo de vigilância eletrônica nascido na Polícia da cidade de Nova Iorque (NYPD), o Detecta tem na sua atuação o emprego de técnicas de monitoramento e vigilância de vias e espaços públicos em diversos municípios do estado.

Por meio das câmeras que o integram, são inseridos padrões de algoritmos de policiamento preditivo voltados à construção de padrões através de suas próprias bases programadas, onde é possível identificar novos padrões de crime e de criminosos, alimentando seu *Big Data* pelo *Machine Learning* conforme novos dados são coletados. Inclusive, em um cenário mais recente, o sistema evoluiu para a possibilidade de leitura de placas e seus fragmentos[2], armazenar a cor de veículos, acessar o banco nacional de mandados de prisão integrado, enfim, adições estas que contribuíram demais para a expansão de seu banco de dados, que se tornou o maior banco de dados da América Latina!

Apesar de ter sido implantado apenas no ano de 2014, sua maior difusão nos municípios de SP se deu a partir do ano seguinte, e até o ano de 2017, período em que foram apurados os seus últimos resultados, denotou-se um aumento expressivo no seu auxílio aos métodos tradicionais de atuação policial preventiva e investigação criminal.

De acordo com dados oficiais do Portal do Governo do Estado de São Paulo, por meio de balanço dos resultados feito no período de 2014 a 19 de abril de 2017, as imagens captadas em tal sistema contribuíram para a prisão de 4.731 (quatro mil setecentas e trinta e uma) pessoas em flagrante delito, interceptação de 3.320 (três mil trezentos e vinte) veículos, apreensão de 276 (duzentas e setenta e seis) armas de fogo e leitura de 20 (vinte) bilhões de placas de automóveis. E na capital, durante o mesmo período, 2.942 (duas mil novecentas e quarenta e duas) pessoas foram detidas, 2.172 (dois mil cento e setenta e dois) veículos foram interceptados e, por fim, foram apreendidas 162 (cento e sessenta e duas) armas

2 Não mais se limitando à leitura de caracteres, como ocorria nos estágios iniciais de implementação da tecnologia

de fogo. Denota-se, por assim dizer, um incremento considerável no resultado obtido a partir da sua implantação num curto espaço de tempo.

Não pode deixar de ser considerado, ainda, o fato de que o sistema "Detecta" se vale, ao menos quando analisada a sua atuação ainda restrita ao estado de São Paulo, de câmeras e sistemas de vigilâncias instaladas em vias públicas e de acesso ao público, o que significa dizer que essas câmeras não precisam necessariamente ser de propriedade do poder público. Ao contrário, grande parte desse sistema se encontra atualmente instalada em postos e praças de pedágio, consistindo em radares fixos e móveis instalados em estradas, rodovias, estações de ônibus e metrô, sendo a grande maioria desse sistema administrado por empresas ou consórcios de empresas privadas concessionárias de serviços públicos.

É preciso considerar, porém, que mesmo que em mãos de empresas particulares, a obtenção, o armazenamento e a administração das imagens captadas estarão a cargo dos órgãos incumbidos do exercício da segurança pública, pois gozam do dever legal para tanto.

Com a apresentação de tais informações, não há dúvidas a respeito da necessidade de adoção da tecnologia na atuação do estado, especialmente no que diz respeito à prevenção e repressão da criminalidade, que parece crescer em proporção geométrica. As ações criminais se alteram conforme é alterada a tecnologia, devendo a autoridade pública estar atenta a essa realidade e pronta a atuar, sobretudo porque, em um primeiro plano, os números são bastante expressivos e refletem a necessidade de adoção desses mecanismos de inteligência artificial. A questão que se coloca, porém, é: como se dá a política de alimentação dos dados por trás do sistema de predição criminal? Não estaria o sistema eletrônico retratando, também, a seletividade própria do sistema de segurança pública e de justiça criminal?

Nesse sentido, deve-se ressaltar como o algoritmo enviesadamente aplicado no caso concreto é capaz de contaminar, por meio do *machine learning*, os resultados auferidos de forma idônea e imparcial, colocando em xeque a eficiência do algoritmo e colocando em risco o combate à criminalidade, de forma que sequer há um sistema de contraditório consolidado para o questionamento das supostas provas geradas pelo sistema aplicado:

> O uso de algoritmos enviesados no policiamento não apenas onera aqueles tidos como "falsos positivos", como, ainda, contamina os "verdadeiros positivos". Para criar uma ferramenta legal eficiente contra a ação policial discriminatória, deveria ser oferecida à defesa a possibilidade de contestar uma condenação decorrente de um policiamento tendencioso, com uma regra específica de não admissibilidade da prova (*exclusionary rule*), protegendo os "verdadeiros positivos" contra o uso de provas maculadas (Gless, 2020, p. 3).

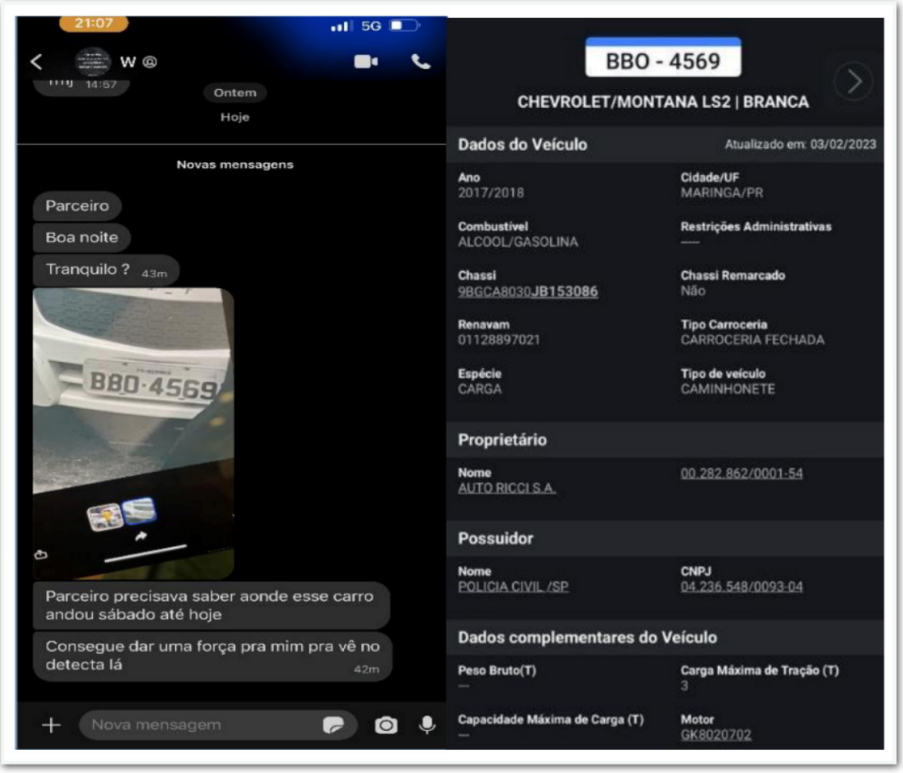
Por melhores que sejam os números apresentados em ambos os casos, a ausência de uma regulamentação mais detalhada para com o uso desses sistemas torna a legitimidade de sua aplicação questionável, sobretudo por diversos escândalos de discriminação e erros metodológicos perpetrados por outros

governos estrangeiros que adotaram determinado algoritmo, como no caso do mencionado *PredPol*, que inclusive teve sua aplicação pelo Governo do Estado da Califórnia em 2020 encerrada justamente por suas falhas metodológicas. E aqui, situações semelhantes também acompanharam a implementação da tecnologia.

No ano de 2023, por exemplo, em uma investigação conduzida pela Polícia Federal, foi descoberto que o PCC (Primeiro Comando da Capital), maior organização criminosa de São Paulo, tinha acesso às câmeras de vigilância integradas ao sistema "Detecta", descobertas após a retirada do sigilo de uma investigação sobre o plano de assassinato da organização em relação ao Senador Sérgio Moro (União Brasil) (Ribeiro, 2023).

Conforme é possível identificar na imagem abaixo, a partir do acesso às câmeras de vigilância, os criminosos conseguiram acessar informações identificadoras de uma viatura descaracterizada da Polícia Civil de SP, tais como: nome do modelo, chassi, proprietário e afins:

Figura 1 – Conversa entre criminosos do PCC com acesso às câmeras de vigilância do Detecta



Fonte: Ribeiro (2022)

Como se não bastasse tamanho absurdo, em 2016, o Tribunal de Contas do Estado já havia conduzido uma investigação acerca do funcionamento do Sistema Detecta por 15 meses, concluindo que o sistema simplesmente não funciona de forma eficiente por uma série de deficiências técnicas:

> Para os técnicos do TCE, que ficaram 15 meses investigando esse projeto - por meio da análise de documentos, entrevistas com policiais e vistorias in loco em centros de comando, delegacias e batalhões -, há conflitos entre sistemas operacionais, falta de infraestrutura e treinamento para que de fato se substituam agentes no monitoramento 24 horas de imagens de segurança (Agência Estado, 2016, *online*).

Apesar da informação conflitar com os dados apresentados pela Governo do Estado de SP, que prontamente refutou tal investigação, a ausência de uma regulação adequada de tais tecnologias certamente dificulta a aferição e o controle real do uso desse tipo de tecnologia.

E mesmo com escândalos de vazamento do acesso do sistema aos criminosos, frente à exposição de dados sensíveis de pessoas e de informações absolutamente protegidas pelo estado e o questionamento do funcionamento da tecnologia, alguns locais estão expandindo ainda mais o raio de atuação do sistema, sem que haja o devido controle de segurança necessário. Como exemplo, é possível citar o caso da prefeitura de Diadema que, conforme dados apresentados em seu site no ano de 2023, simplesmente dobrou o número de barreiras do sistema "Detecta", com metas de ainda maiores de aumento. Como isso é possível?

Ora, a matéria de segurança pública diz respeito a uma política de governo, de forma que alcançar resultados aparentemente positivos ou fazer investimentos no simples aumento da disponibilidade de tecnologia de combate à criminalidade traz benefícios políticos ao governo que adotou o sistema de policiamento preditivo. Como saber se seu uso está ou não sendo enveredado para favorecimentos numéricos no efetivo de prisões, por exemplo, se não existe uma regulamentação adequada sobre a aplicação destes algoritmos e sequer a possibilidade de acesso a esses dados pelo cidadão comum? Nem a própria Lei de Acesso à Informação parece ser aplicável, pois como saber se o sistema captou e armazenou meus dados se não tenho acesso *per se* a ele?

Esse é, sem dúvida, o grande questionamento posto em discussão, a respeito do qual não existe, ainda, uma resposta precisa, já que sua aplicação não apresentou a transparência necessária à sociedade civil brasileira até o momento. E o pior: este vácuo legislativo – consistente na primeira linha de pressuposto regulatório *in casu* – é ainda mais injustificado quando analisada a discussão pela óptica internacional, muito mais avançada e pormenorizada em comparação à nacional, pois mesmo que longe do ideal, ainda representa um espelho basilar para a perspectiva regulatória brasileira.

3 FALTA DE ADEQUAÇÃO LEGISLATIVA E TÉCNICA NACIONAL PERANTE DOCUMENTOS INTERNACIONAIS

O Brasil, como ressaltado anteriormente, tem como conquista mais recente a sanção da LGPD em 2020, que traçou uma série de proteções mais específicas e consistentes em relação ao uso e proteção de dados, abrangendo até mesmo dispositivos que direcionam obrigações de reparação quando do descumprimento de suas diretrizes, tal como em seu art. 42:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Aqui, partindo de uma análise mais teórica (e, portanto, sem vincular uma interpretação ao uso dos algoritmos de policiamento preditivo), há duas partes passiveis que possuem alguma responsabilização em relação ao tratamento de dados: o operador e o controlador. Em suma, o operador corresponde à "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VII, LGPD), sendo a parte diretamente encarregada de gerir e operar os dados pelos quais a empresa ou o órgão armazena. Por outro lado, o controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", não consistindo na parte que diretamente trata de tais dados, mas sim da parte que os regula, que determina a forma de gestão dos dados em seu domínio, o que consequentemente demonstra uma relação de subordinação do operador em relação ao controlador.

Diante dessas definições, vale mencionar e exemplificar a relação entre uma empresa de *e-commerce* e empresas de logística quanto ao uso das plataformas de entrega: enquanto as empresas de logística ficam responsáveis por operar o sistema da empresa e lidar com os dados dos cadastros dos funcionários e dos compradores (assumindo o papel de 'operadoras'), a própria empresa de *e-commerce* fica responsável por ditar as regras sobre como tais dados serão operados, se encaixando no papel de "controladora".

Deslocando tal lógica para o uso de algoritmos de policiamento preditivo, assim como exposto no item anterior, os governos estaduais ficam responsáveis por adquirir a tecnologia e delegar sua utilização a um terceiro (geralmente sob coordenação da secretaria de segurança pública do estado em cada caso). Frente a isso, enquanto esses terceiros representam os operadores dos sistemas de vigilância, o governo estadual fica responsável por estabelecer quais os propósitos de aplicação dos algoritmos (delimitar as regiões estratégicas, o raio de atuação etc.).

No entanto, sob quais premissas o governo estadual lastreia aquilo que pode ou não pode na vigilância? Para além das legislações criminais, não há sequer

um controle ou fiscalização em relação a tal uso, o que pode ensejar não só um futuro vazamento de dados sensíveis – que já ocorreu no caso do Detecta – como, também, ser gerada uma incerteza a respeito desses dados, que podem não estar sendo usados de forma isonômica e própria como determinada a lei[3]. Apesar da falta de delimitação normativa para a utilização da tecnologia, não há sequer como mensurar se há respeito à política de proteção de dados da LGPD, pois os próprios estados se autorregulam. E a pergunta que deve ser feita é: tal autorregulação ocorre em todos os sistemas de policiamento preditivo no mundo?

A resposta é não: apesar de o uso dos algoritmos de policiamento preditivo ser bastante controverso nos locais aplicados mundialmente, há exemplos onde sua aplicação goza de muito maior comprometimento do que se projeta nacionalmente. Como exemplo, foram elaborados diversos documentos bem recentes que orientam sobre o uso regrado de algoritmos de inteligência artificial, sendo alguns dos mais importantes a Declaração de Toronto (2018) e a Declaração sobre Ética e Proteção de Dados em IA (2018). Para além destes, várias organizações e eventos ao redor do mundo começaram a pautar uma atuação em prol de uma governança ética para com o emprego de algoritmos, como a Conferência Internacional dos Delegados para a Proteção de Dados e Privacidade (ICDPPC) e o próprio governo britânico (Lemes, 2009). Para estes, destacam-se as inúmeras bases para o uso racional, humano e regrado da IA, o que consequentemente atesta a existência de uma base principiológica muito carente na legislação brasileira para a temática:

> Assim, em face dos trabalhos estudados, identificou-se que os princípios recomendados se encaixavam sob as seguintes categorias principais: transparência, *accountability*, responsabilidade, inteligibilidade, explicabilidade, precisão, auditabilidade, respeito aos direitos humanos, engajamento público, justiça e imparcialidade (Lemes, 2009, p. 22).

Mas, de toda a legislação pertinente sobre o tema elaborada até o momento, aquela que mais trouxe completude em sua perspectiva regulatória diz respeito ao *AI Act* (2023), que é a legislação do Parlamento Europeu dedicada à regulação do uso da inteligência artificial em seu território. Nela, logo de cara já é possível identificar que a comissão responsável pela elaboração teve uma preocupação universal quanto à aplicação da IA, inclusive quanto ao seu uso na área da segurança pública, ressaltando justamente o ponto mais sensível da problemática aqui no Brasil: a falta de equilíbrio de poder entre o agente operador da tecnologia (estado ou município responsável pela implantação da tecnologia, viabilizada por meio do órgão policial competente) e o indivíduo sujeito à captação de dados e a sujeição deste às discricionaridades da política de governo na aplicação do sistema:

> As ações das autoridades policiais que implicam certas utilizações dos sistemas de IA são caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem

3 Em especial pelos diversos casos de discriminação algorítmica nos países que implementaram algoritmos em locais públicos.

> como ter outros impactos adversos nos direitos fundamentais garantidos pela Carta. Em particular, se não for treinado com dados de alta qualidade, não cumprir os requisitos adequados em termos de exatidão ou solidez ou não tiver sido devidamente concebido e testado antes de ser colocado no mercado ou em serviço, o sistema de IA pode destacar pessoas de uma forma discriminatória ou incorreta e injusta. Além disso, o exercício de importantes direitos fundamentais processuais, como o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa, pode ser prejudicado, em particular, se esses sistemas de IA não forem suficientemente transparentes, explicáveis e documentados (European Comission, 2021, p. 30).

Tal preocupação não é desmedia, pois dentre todos os prejuízos que um sistema algorítmico pode causar na esfera da segurança pública, aquele que demonstra maior sensibilidade e impacto na discussão pública é justamente o potencial discriminatório que tais algoritmos podem causar, pois ao mesmo tempo que a ferramenta busca facilitar o combate e a prevenção ao crime, seu uso frequentemente acaba por abrir espaço para a discriminação racial e de gênero, o que não apenas é vedado pela Constituição Federal como, também, é tipificado na legislação penal brasileira. E pior: este é um problema que acomete tal tecnologia há vários anos na experiência internacional, apesar de seu estágio mais avançado em relação ao Brasil.

Em uma análise desenvolvida pela corporação jornalística *ProPublica* a respeito do *Correctional ofender Management Profiling for Alternative Sanctions* (COMPAS), software americano com a finalidade de aferir a probabilidade de cometimento de novos crimes por parte de réus condenados no sistema jurídico americano, foi constatado que tal tecnologia possui um evidente viés racial em sua aplicação, com 57,6% dos infratores afro-americanos recebendo uma classificação de risco alta enquanto apenas 33,1% dos caucasianos recebem tal classificação (Brackey, 2019). E para piorar, a mesma pesquisa apontou que o software analisado possui uma taxa de eficiência próxima aos 66% (Brackey, 2019), ou seja, não só há um evidente viés discriminatório no bojo do software como, também, há um problema de precisão da tecnologia em si por meio de valores inaceitáveis (Zhang; Han, 2021). Ora, como uma tecnologia aplicada no bojo do Direito Penal enquanto *ultima ratio* continua sendo aplicada a despeito de sua baixa precisão e, pior, diante de seu sabido viés discriminatório? Com base na função ressocializante da pena, como o apenado conseguirá ser reinserido na sociedade se a tecnologia responsável por o reavaliar é incapaz de fazer uma análise neutra e justa dos fatos?

As revoluções tecnológicas representam um caminho sem volta que permeará os confins da sociedade cada vez mais, logo, negar seu desenvolvimento, tal como feito nos históricos movimentos ludistas na Revolução Industrial, é negar a realidade. No entanto, séculos depois, a sociedade foi capaz de garantir conquistas sociais e liberais cuja natureza é inegociável, não havendo tecnologia com o mínimo de legitimidade para suplantá-las, mas sim para obedecê-las e respeitá-las. E nesse sentido, Ferrajoli (2022) observa que tais garantias representam uma evolução moral no seio coletivo responsável por atribuir legitimidade ao Direito Positivado, de maneira que elementos supervenientes a sua consagração representam um

retrocesso a este status, sendo a discriminação um claro exemplo de prejuízo a essas conquistas:

> Muitos dos princípios morais que servem de base para negar a justificação de certas proibições ou para justificar certos delitos estão incorporados ao direito positivo como outros tantos limites ou condições ou princípios jurídicos de deslegitimação de uns e de legitimação de outros. E o caso do princípio constitucional de igualdade, que permite considerar como não válidos, antes mesmo de qualquer juízo de justiça, os atos de discriminação entre os destinatários dos preceitos penais em razão de raça, sexo ou outras condições de status', ou daquelas normas penais sobre "eximentes", "causas de exculpação" ou "causas de justificação", que permitem em todos os ordenamentos evoluídos justificar, não só moralmente, senão também juridicamente, os delitos praticados em determinadas circunstâncias, como o estado de necessidade, a legítima defesa, o exercício regular de um direito etc. Mas, sobretudo, podemos encontrar os princípios inerentes às garantias penais e processuais, formalizados no nosso sistema SG, como outras tantas prescrições sobre as condições da pena. E, ao contrário, a incorporação limitadora de todos estes princípios ou valores sob a forma de garantias o que distingue, conforme vimos, o moderno Estado de direito em matéria penal; e somente por meio do número, qualidade e nível de efetividade dos princípios assim incorporados pode-se valorar sua justiça e medir seu grau de garantismo. (Ferrajoli, 2002, p. 369)

Diante disso, vários algoritmos aplicados ao redor do mundo, quando não descontinuados, estão passando por uma restrita revisão de seus elementos constitutivos a fim de que suas falhas metodológicas sejam superadas, perpassando pela necessidade do sistema de IA ser treinado com dados de alta qualidade (I), pelo cumprimento de requisitos adequados em termos de precisão ou robustez (II) e pela concepção e testagem da tecnologia antes de ser colocada no mercado ou de entrar em serviço (III), deixando claro que grande parte dos pontos deficientes apontados ao longo do texto na legislação nacional (ou sua falta) constituem questões basilares na operabilidade tecnológica internacional, principalmente em um contexto europeu, que vem buscando tais mudanças por meio de alterações legislativas e regulatórias significativas. Obviamente, nem todos os documentos possuem caráter vinculante, mas, ao menos no que diz respeito ao caráter instrutório, certamente é nítido o contraste.

Por isso, com o Brasil adquirindo tais tecnologias de fornecedores estrangeiros, a expectativa é que os erros aqui apontados sejam devidamente observados pelo poder público nacional de forma preventiva, que deverá se manifestar por meio de um arcabouço legislativo-regulatório capaz de proteger as garantias fundamentais aqui contempladas e protegidas, além de auxiliar as forças policiais nos diversos problemas crônicos da segurança pública brasileira.

CONCLUSÃO

Diante de todo o exposto, fica claro que a proposta apresentada pelos estados na implantação dos algoritmos de policiamento preditivo goza de legitimidade constitucional no sentido de se aderir conquistas tecnológicas aos mecanismos de prevenção de crimes já existentes nas circunscrições policiais. Todavia, a falta de uma legislação própria e de entendimentos jurisprudenciais dos órgãos superiores em relação ao tema constitui um conjunto de empecilhos à implementação de tais tecnologias por parte do poder público, pois a autorregulamentação por seus governantes e secretarias de segurança pública, como exposto, não foi capaz de demonstrar a devida transparência no funcionamento dos algoritmos utilizados, principalmente em como operam em relação ao Big data cada vez mais alimentado com dados sensíveis. Quando comparado aos nortes de documentos internacionais de governança ética no uso da inteligência artificial, tal disparidade é ainda mais evidente.

A eficiência de tais sistemas no Brasil não está ligada à obtenção de dados favoráveis a curto prazo, mas sim ligada a uma gestão de dados coerente, ética e voltada a tão somente suprimir problemas sensíveis à coletividade, e não os substituir – os problemas metodológicos, discriminatórios e de vazamento de dados expostos apenas comprovam essa urgência! Por isso, acredita-se que o mais correto seria que o legislativo tomasse como referência medidas e tratados internacionais consolidados sobre o tema para que houvesse o mínimo de regulamentação específica em sua implementação, sobretudo pelo fato de a LGPD ter sido aprovada há pouco tempo, o que ensejaria uma série de discussões muito ricas para tanto.

REFERÊNCIAS

AGÊNCIA ESTADO. Sistema Detecta da polícia não identifica crimes, diz TCE. *Estado de Minas,* 2016. Disponível em: https://www.em.com.br/app/noticia/nacional/2016/08/13/interna_nacional,793718/sistema-detecta-da-policia-nao-identifica-crimes-diz-tce.shtml. Acesso em: 17 mar. 2023.

AGRELA, L. Inteligência artificial começa a chegar à segurança pública. Revista *Exame,* jul. 2021. Disponível em: https://exame.com/tecnologia/inteligencia-artificial-comeca-a-chegar-a-seguranca-publica/. Último acesso em: 29 jul. 2021.

BRACKEY, A. *Analysis of Racial Bias in Northpointe's COMPAS Algorithm.* Tulane University School of Science and Engineering, 2019. Disponível em: https://www.proquest.com/openview/492b784291d8ff8e65dfdc3b7fe92206/1?pq-origsite=gscholar&cbl=18750&diss=y. Acesso em: 16 jun. 2024.

BRANCHER, P. M. R. Proteção internacional de dados pessoais. Enciclopédia jurídica da PUC-SP. *In:* Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). *Tomo:* Direito Internacional. Cláudio Finkelstein, Clarisse Laupman Ferraz Lima (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em: 27 fev. 2024.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*, de 5 de outubro de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 ago. 2021.

BRASIL. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 19 ago. 2021;

ENSIGN, D.; FRIEDLER, S. A.; NEVILLE, S.; SCHEIDEGGER, C.; VENKATASUBRAMANIAN, S. Runaway Feedback Loops in Predictive Policing. *Procedings of Machine Learning Research*. [S. l.] Vol. 81, pag. 1-12, 2018. Disponível em: https://proceedings.mlr.press/v81/ensign18a.html. Acesso em: 21 ago. 2021.

EUROPEAN COMISSION. *Regulamento do parlamento europeu e do conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da União.* Bruxelas, EU: European Comission, 2021. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. Acesso em: 20 mar. 2024.

FERRAJOLI, L. *Direito e Razão:* Teoria do Garantismo Penal. São Paulo: Editora Revista dos Tribunais, 2002.

GLESS, S. Policiamento preditivo: em defesa dos "verdadeiros positivos". *Revista Direito GV*, vol. 16, n. 1, São Paulo: 2020. Disponível em: https://periodicos.fgv.br/revdireitogv/article/view/81697. Acesso em: 19 mar. 2024.

GOMES, L. S.; ANDRADE, W. L. S. Novas tecnologias de vigilância e o policiamento brasileiro. *In*: *Fórum Brasileiro de Segurança Pública*. Ed. 51, 2020. Disponível em: https://fontesegura.forumseguranca.org.br/novas-tecnologias-de-vigilancia-e-o-policiamento-brasileiro/. Acesso em: 21 mar. 2024.

GOVERNO DO ESTADO DE SP. Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo. *Portal do Governo de São Paulo*. São Paulo, SP: 2017. Disponível em: https://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-o-estado-de-sao-paulo-com-3-mil-cameras-de-video/. Acesso em: 07 ago. 2021.

LEMES, M. M. *Inteligência artificial, algoritmos e policiamento preditivo no poder público federal brasileiro*. Tese (graduação em Direito) – Universidade de Brasília, Brasília, 2009. Disponível em: https://bdm.unb.br/handle/10483/24565. Acesso em: 27 ago. 21.

MENEZES, C. S.; SANLLEHÍ, J. R. A. Big data, inteligência artificial e policiamento preditivo: bases para uma adequada regulação legal que respeite os direitos fundamentais. *Revista Novos Estudos Jurídicos - Eletrônica*, Vol. 26, n. 1, 2021. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/17553. Acesso em: 19 ago. 2021.

MORAES, F. O. *Policiamento preditivo e aspectos constitucionais.* 2022. Dissertação (Mestrado em Direito) - Direito da Pontifícia Universidade Católica do Rio de Janeiro (PUC-RIO), Rio de Janeiro, 2022. Disponível em: https://www.maxwell.vrac.puc-rio.br/colecao.php?strSecao=resultado&nrSeq=59303@1. Acesso em: 20 mar. 2024.

OLIVEIRA JUNIOR, I.; SANTOS, F. C. C. Inteligência artificial e policiamento preditivo: possibilidades de inovação tecnológica para a Polícia Militar do Paraná no enfrentamento aos crimes violentos contra o patrimônio com emprego de explosivos. *Brazilian Journal of Technology,* Curitiba, v.5, n.1, p. 30-62, 2022.

PEREIRA, V. A. *et al*. *Análise criminal.* Relatório de análise situacional (Curso Superior de Polícia). 25 f. Academia Policial Militar do Guatupê, São José dos Pinhais, 2020.

POLÍCIA MILITAR DO PARANÁ (PMPR). *Sistema de Atendimento e Despacho de Emergências* (SADE), ed. 1, Curitiba: PMPR, 2022.

PREFEITURA DE DIADEMA. Diadema dobra número de barreiras eletrônicas do Sistema Detecta. *Site da Prefeitura de Diadema*, 2023. Disponível em: https://portal.diadema.sp.gov.br/diadema-dobra-numero-de-barreiras-eletronicas-do-sistema-detecta/. Acesso em: 05 mar. 2024.

RIBEIRO, B. PCC tinha acesso a sistema de câmeras do governo de SP, diz PF. *Metrópoles*, 2023. Disponível em: https://www.metropoles.com/sao-paulo/policia-sp/pcc-tinha-acesso-a-sistema-de-cameras-do-governo-de-sp-diz-pf#:~:text=S%C3%A3o%20Paulo%20%E2%80%93%20A%20c%C3%A9lula%20do,segundo%20relat%C3%B3rio%20produzido%20pela%20Pol%C3%ADcia. Acesso em: 13 mar. 2024.

SANTOS, T. F. M. A implantação do sistema de atendimento e despacho de emergências via mobile no 10º batalhão da Polícia Militar do Paraná. *Brazilian Journal of Development*, Curitiba, v.9, n.3, p. 11214-11241, 2023. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/58189/42417. Acesso em: 21 mar. 2024.

ZHANG, J.; HAN, Y. Algorithms Have Built Racial Bias in Legal System-Accept or Not? Advances in Social Science, Education and Humanities Research, *Atlantis Press,* vol. 631, p. 1217-1221, 2021.