ReGeo ISSN: 2177-3246

EFEITOS DA BIOMETRIA NA SEGURANÇA PÚBLICA BRASILEIRA: UMA ANÁLISE SOBRE RECONHECIMENTO FACIAL E RACISMO ALGORITMO

EFFECTS OF BIOMETRICS ON BRAZILIAN PUBLIC SECURITY: AN ANALYSIS ON FACIAL RECOGNITION AND RACISM ALGORITHM

LOS EFECTOS DE LA BIOMETRÍA EN LA SEGURIDAD PÚBLICA BRASILEÑA: UN ANÁLISIS DE LOS ALGORITMOS DE RECONOCIMIENTO FACIAL Y RACISMO

10.56238/revgeov16n5-172

Pablo Ornelas Rosa[1]
Doutor em Ciências Sociais
Instituição: Pontifícia Universidade Católica de São Paulo (PUC/SP), Universidade Vila Velha (UVV), Centro Universitário Vale Cricaré (UNIVC)
E-mail: pablorosa13@gmail.com
Orcid: https://orcid.org/0000-0002-9075-3895
Lattes: http://lattes.cnpq.br/1908091180713668

Clécio José Morandi de Assis Lemos
Doutor em Direto
Instituição: Pontifícia Universidade Católica do Rio de Janeiro (PUC/RJ), Universidade Federal do Espírito Santo (UFES), Centro Universitário do Espírito Santo (UNESC)
E-mail: cleciojus@gmail.com
Lattes: http://lattes.cnpq.br/4912344889000121

Aknaton Toczek Souza
Doutor em Sociologia, Doutor em Direito
Instituição: Universidade Federal do Paraná (UFPR), Universidade Católica de Pelotas (UCPEL)
E-mail: aknatontoczek@gmail.com
Orcid: https://orcid.org/0000-0002-6946-6242
Lattes: http://lattes.cnpq.br/8961574472191125

Eudson Ferreira Bento
Mestre em Segurança Pública
Instituição: Universidade Vila Velha (UVV), Polícia Civil
E-mail: eudsonfbento@yahoo.com.br
Orcid: https://orcid.org/0009-0003-0875-8692
Lattes: http://lattes.cnpq.br/9956411821404367

RESUMO
O artigo apresenta uma revisão de literatura sobre a relação entre racismo e uso da tecnologia de reconhecimento facial pela Segurança Pública brasileira. O texto está organizado em quatro seções: na

[1] *Bolsista Capixaba de Produtividade da Fundação de Amparo à Pesquisa do Espírito Santo (FAPES)*

primeira, são apresentados fenômenos como plataformização, dataficação da vida, colonialismo de dados, capitalismo de plataforma e vigilância; na segunda, são expostas algumas características dessa tecnologia; na terceira, evidencia-se os estudos sobre discriminação racial através dos algoritmos; por fim, apresenta-se as principais consequências do racismo algorítmico na Segurança Pública. Conclui pela necessidade de um debate amplo acerca dessas práticas algorítmicas discriminatórias, visando evitar a violação de direitos e garantias fundamentais.

Palavras-chave: Racismo. Algoritmo. Segurança Pública. Direitos Fundamentais.

ABSTRACT

The article presents a literature review on the relationship between racism and the use of facial recognition technology by Brazilian Public Security, organized into four sections: in the first, phenomena such as platformization, datafication of life, data colonialism, platform capitalism are presented. and surveillance; in the second, some characteristics of this technology are exposed; in the third, studies on racial discrimination through algorithms are highlighted; in the fourth, the main consequences of algorithmic racism in Public Security are presented. It concludes that there is a need for a broad debate about these discriminatory algorithmic practices, aiming to avoid the violation of fundamental rights and guarantees.

Keywords: Racism. Algorithm. Public Security. Fundamental Rights.

RESUMEN

Este artículo presenta una revisión bibliográfica sobre la relación entre el racismo y el uso de la tecnología de reconocimiento facial por parte de la Seguridad Pública brasileña. El texto se organiza en cuatro secciones: la primera presenta fenómenos como la plataformización, la datificación de la vida, el colonialismo de datos, el capitalismo de plataformas y la vigilancia; la segunda expone algunas características de esta tecnología; la tercera destaca estudios sobre discriminación racial mediante algoritmos; finalmente, presenta las principales consecuencias del racismo algorítmico en la Seguridad Pública. Concluye con la necesidad de un amplio debate sobre estas prácticas algorítmicas discriminatorias, con el objetivo de prevenir la violación de los derechos y garantías fundamentales.

Palabras clave: Racismo. Algoritmo. Seguridad Pública. Derechos Fundamentales.

1 INTRODUÇÃO

Ferramentas como a inteligência artificial, certificação digital, internet das coisas, dentre muitas outras, são apenas alguns exemplos de como a tecnologia vem transformando o dia a dia de pessoas, empresas e do próprio Estado. Na medida em que vai se entranhando em nossos fazeres, gerando mudanças nos comportamentos, a tecnologia também apresenta impasses. Um desses questionamentos envolve a nova roupagem que o racismo assume, inclusive involuntariamente, nesse oceano de *bites*, contaminando-o com suas características estruturais, destacando-se operações de bloqueio algorítmico de pessoas negras e uso de robôs digitais (*bots*)[2] para discursos supremacistas, na maioria das vezes operando sem serem notadas (SILVA, 2020).

A sutileza desta nova modalidade de discriminação ocorre porque passamos a viver em uma sociedade caracterizada pelo uso intensivo de *softwares* que se tornam a forma prioritária das interações sociais, o que implica na ampla mobilização de algoritmos utilizados para finalidades preditivas (SILVEIRA, 2016; DA EMPOLI, 2019; ZUBOFF, 2020). O uso normalizado de aparelhos celulares, *tablets* e demais *gadgets* indica a crescente presença das tecnologias em nosso convívio, permeando intensamente nossas relações.

Contudo, nem os *softwares* e nem os algoritmos neles contidos operam de forma neutra. Ao contrário, eles geram efeitos porque foram criados e desenvolvidos por seres humanos visando determinadas finalidades. Assim, apesar de serem imateriais e aparentemente invisíveis, possuem um ponto de partida e um objetivo que pode expressar discriminação, ainda que de maneira não intencional.

Tais fatos ganham maior preocupação com a aplicação do reconhecimento facial pelos órgãos de Segurança Pública, o que torna imprescindível o estudo dos precedentes envolvendo a Inteligência Artificial e o racismo, compreendendo seus conceitos, história e estrutura. Sendo assim, o escrito apresentado, objetiva analisar essa nova faceta da discriminação racial, colaborando para o seu conhecimento e investigação, na medida em que busca compreender como ela ocorre hodiernamente. Já há algum tempo esse método de reconhecimento facial tem acompanhado polêmicas, notadamente quando estudos indicam que tal tecnologia é propensa ao cometimento de erros na análise de rostos de pessoas negras ou de outras minorias, merecendo nossa preocupação (*SILVA,* 2020; BEIGUELMAN, 2021; AMARAL, MARTINS, ELESBÃO, 2021; NOBLE, 2021).

O texto a seguir foi organizado da seguinte maneira: na primeira seção, foram expostos alguns dos pressupostos que versam sobre os fenômenos da plataformização e da dataficação da vida; na segunda, foram abordadas algumas das principais características que envolvem as tecnologias de reconhecimento facial; na terceira, foram evidenciados os elementos que as constituem; para, no fim,

[2] "Os bots são aplicações autônomas que rodam na Internet enquanto desempenham algum tipo de tarefa pré-determinada" (GARRET, 2022)

apresentar algumas das principais consequências dessa forma de controle social, enfatizando o campo da Segurança Pública.

2 CAPITALISMO DE PLATAFORMA E DE VIGILÂNCIA

No percurso para o XXI ocorreram transformações significativas referentes às maneiras pelas quais as pessoas passaram a se relacionar, assim como foram alteradas as formas como se constituem enquanto sujeitos, a partir da intensificação paulatina do uso das plataformas digitais em sua comunicação, alterando o acesso à informação antes marcado pelo domínio da interação face a face (ROSA; AMARAL; NEMER, 2021, p. 02).

Logo, importa descrever o processo de plataformização e de dataficação da vida, de cuja influência a Segurança Pública não se encontra imune. A respeito da plataformização, é necessário evidenciar as contribuições de Poell, Nieborg e Dijck (2020, p. 05) que a definem como uma forma de "penetração de infraestruturas, processos econômicos e estruturas governamentais de plataformas em diferentes setores econômicos e esferas da vida".

Seguindo os mesmos autores, é possível elucidar que as plataformas são modelos digitais programados que atuam sobre as interações entre pessoas e complementadores, fazendo isto por meio de uma coleta sistematizada de dados, uso de algoritmos e monetização.

Não obstante, também se faz necessário destacar outras significativas contribuições acerca desse fenômeno caracterizado pelo condicionamento das relações humanas nas redes sociais, descrito ora como "capitalismo de vigilância" (ZUBOFF, 2020) ora como "capitalismo de plataforma" (SRNICEK, 2018).

Ao compreender que ingressamos em uma era caraterizada pelo que chamou de capitalismo de plataforma, Nick Srnicek (2018, p. 44-45) elencou cinco tipos específicos de plataformas digitais que operam a partir de modelos distintos de negócios: a) as *plataformas publicitárias*, as quais extraem e utilizam, como produtos vendidos à publicidade, os dados de seus usuários, como fazem o *Google* e o *Facebook*; b) as *plataformas de nuvem*, proprietárias de *hardware* e de *software* de negócios, dependentes do digital, e que rendem lucros conforme as necessidades de suas empresas, a partir de uma enorme rede logística como *Amazon* e *Web Services*; c) as *plataformas industriais*, a exemplo a *General Eletric* e *Simens*, que produzem *hardware* e *software* necessários para a transformação da manufatura tradicional em processos conectados com a *internet*; d) as *plataformas de produtos*, como a *Rolls Royce* e a *Spotify*, em que transformam um bem tradicional em um serviço e cobram um aluguel ou uma taxa de inscrição; e) as *plataformas austeras*, como o *Uber* e o *Airbnb*, as quais atuam por meio de subcontratações, cobrando um alto custo pelo seu uso. O autor ainda esclarece que é possível a coexistência dessas divisões em uma mesma empresa.

De acordo com Zuboff (2020, p. 247), o impacto daquilo que chamou de capitalismo de vigilância, caracterizado pelo uso intensivo das plataformas digitais, é sentido nas infraestruturas dos mercados, da governança e, notadamente, dos dados.

Neste último caso, é possível constatar que ele gera a chamada dataficação da vida, entendida por André Lemos (2021, p. 02) como "formas de transformação de ações em dados quantificáveis, permitindo amplo rastreamento e análises preditivas", tendo potencial de se expandir para muitos outros campos, tais como a política, economia, cultura etc., atingindo o campo da Segurança Pública, por meio de seu consequente uso biométrico através das tecnologias de reconhecimento facial.

Ao aprofundarmos o entendimento acerca da dataficação da vida, é possível compreender que se trata de uma nova maneira de produzir o conhecimento, implicando em uma requisição ou mesmo tradução digital do mundo que possibilita certo domínio sobre objetos e/ou ações, com objetivo de simulá-los e testá-los em sistemas computacionais avançados operados a partir da inteligência artificial (IA). Sendo assim, temos uma nova forma hegemônica do conhecer e de gerir a vida no planeta (LEMOS, 2021, p. 197).

Nesse processo, a dataficação da vida tem influenciado vários saberes, inclusive o conhecimento científico, pois evidenciou-se que os dados não funcionam de forma neutra, na medida em que produzem enviesamentos, favorecendo um poder tecnocrático operado sob a tutela de especialistas em algoritmos e com interesses públicos.

Lemos (2021, p.198) ainda acrescenta que a dataficação do conhecimento poderia promover um poder conduzido por uma "epistocracia", operado através de uma "algocracia" calcada na neutralidade técnica da performatividade algorítmica, que decidiria sobre o fazer e o conhecer, na medida em que introduziria nas interações humanas uma espécie de lente que, assim como a matemática foi instrumentalizada por Newton no século XVII, poderia ser tratada como "o grande livro da natureza".

A compreensão desse fenômeno talvez fique mais evidente nas análises realizadas por Siva Vaidhyanathan (2011, p. 40), ao tratar da *Googlelização de tudo*. Segundo o autor, "o Google coleta os *gigabytes* das informações pessoais e o conteúdo criativo que milhões de usuários seus fornecem gratuitamente à rede todos os dias, e vende essas informações a anunciantes de milhões de produtos e serviços". Desse modo, ao verificar que o Google se impõe através do convencimento de que sabe exatamente o que fazer para melhorar as nossas vidas, Vaidhyanathan (2011, p. 29) constatou que essa empresa passou determinar o nosso comportamento, controlando a rede sem levantar nenhuma suspeita de exerce práticas autoritárias.

A dataficação da vida é entendida por André Lemos (2021, p. 199-200) como uma nova era da cultura digital, ancorada em algumas dimensões que podem ser sistematizadas em forma: a) de conhecimento, por se tratar de uma nova produção por meio da extração e gestão dos dados; b) de

sociabilidade, uma vez que torna rotineira a vigilância e a coleta de informações pessoais; e c) da natureza, na medida em que impacta negativamente o meio ambiente pela forma de consumo de bens naturais (minerais principalmente) e descarte do lixo eletrônico, além do alto consumo de energia dos *data centers*. Assim, embora esses impactos aparentem ser totalmente desconhecidos por parte do público, importa lembrar que:

> Dados não são encontrados na natureza, conforme alertou Couldry e Mejias (2019). Esse é um ponto crucial do fenômeno da dataficação. Eles são projetados e dependem de algoritmos de extração e armazenamento. Como bem apontou Tarleton Gillespie (2014), os dados são apresentados como objetivos e os algoritmos que os processam indicados como insuspeitos e incapazes de adotar posições ideológicas, sendo uma grande arma para superar controvérsias. [...]. Entretanto, avança os debates e as pesquisas que consideram não somente os vieses e preconceitos incorporados nas estruturas de dados como também nos códigos e algoritmos que portam a concepção dos seus desenvolvedores e financiadores (SILVEIRA, 2016, p.159-160).

Uma vez criados, os dados poderão ser extraídos dentro de um processo conhecido como colonialismo de dados, de maneira não muito transparente aos seus proprietários, de forma que os hábitos das pessoas se tornam um recurso comercializável, pois são essenciais na relação entre corporações e plataformas, podendo ser usados também para competição política (SILVEIRA, 2016), bem como no uso biométrico através das tecnologias de reconhecimento facial. Assim, nesta combinação de agentes estatais-corporativos, a colonialidade acaba reatualizada, com novos instrumentos, mas ainda perpetuando os mesmos desígnios destrutivos e desumanos próprios do capitalismo (GERVASONI; DIAS, 2023, p. 155)

Nesse sentido, é possível ponderar como o uso massivo de dados acabou proporcionando um governo de condutas, gerido de forma complexa e direcionada pelas plataformas e seus algoritmos, em um acúmulo progressivo de informações que serão úteis para garantir posições de vantagem estratégica.

Silveira (2016) constatou que as plataformas digitais passaram a criar cada vez mais projetos de dataficação que visam converter qualquer elemento digitalizável em um processo de reprodução do capital. Segundo o autor, isso acontece porque as relações entre produtores e consumidores de um certo produto, ou mesmo entre ofertantes e demandantes de determinados serviços, são instrumentalizados paulatinamente por plataformas gerenciadas por meio de algoritmos que permitem a consolidação dessas relações de forma cada vez mais rápida e em conformidade com os interesses publicitários: “Simultaneamente, esses gestores algorítmicos extraem dados dos mercados e os armazenam com finalidades de ampliar o conhecimento e o domínio de suas plataformas” (SILVEIRA, 2016, p.168).

Embora esteja comumente associado à Tecnologia da Informação e Comunicação, o conceito de algoritmo remonta aos primórdios da matemática, existindo de maneira independente da atual digitalização. Desde os tempos da civilização egípcia, os algoritmos eram utilizados para criar fórmulas que solucionavam desafios cotidianos, como a previsão das cheias do rio Nilo, representando

uma sequência específica de passos escritos para resolver um problema particular. Hoje, eles continuam sendo um elemento essencial em todo o processo de computação, visando intermediar atividades humanas e reduzir a quantidade de procedimentos repetitivos (ROCHA; PORTO; ABAURRE, 2020).

Os algoritmos desempenham um papel fundamental no funcionamento das inteligências artificiais, sendo essenciais para a execução de tarefas. Apesar de não haver um conceito universalmente aceito para tratar da Inteligência Artificial (IA), é comumente compreendida como a capacidade de máquinas reproduzirem comportamentos típicos de seres humanos, fundamentada na manipulação de algoritmos. Atualmente, a IA é aplicada em três principais áreas: aprendizado de máquina (*machine learning*), aprendizado profundo (*deep learning*) e processamento de linguagem natural (BON; SCHONS; LOPES-FLOIS, 2023, p. 227).

Segundo Costa (2021), o emprego de programas de aprendizado de máquina (*machine learning*) e sua vertente mais avançada, conhecida como aprendizado profundo (*deep learning*), conferiu às máquinas uma notável habilidade de evoluir por meio da experiência, bem como pela tomada de decisões de forma autônoma. Isso significa que, após o desenvolvimento do algoritmo, muitas etapas subsequentes podem ser realizadas sem a necessidade de intervenção humana.

No tocante ao reconhecimento facial, tido como a capacidade de identificar indivíduos através de características condicionadas por seus rostos, existem diversos autores que adotam uma abordagem otimista em relação ao seu uso para fins de controle social, argumentando que a identificação de pessoas a partir do emprego de técnicas pode se tornar uma alternativa segura e pouco invasiva, conforme reconhece Pablo Nunes *et al*. (2016).

Nesse caso, o argumento em defesa do uso desse tipo de estratégia no campo da Segurança Pública, de modo geral, pressupõe o desenvolvimento de tecnologias conduzidas pelo reconhecimento facial em associação aos sistemas de videomonitoramento já existentes, "que poderiam operar como ferramentas eficazes no combate à criminalidade, principalmente na localização e na identificação de foragidos, criminosos, desaparecidos etc." (Nunes *et al*., 2016, p. 114).

Todavia, ao prometer combater a criminalidade nacional com um recurso tecnológico pretensamente eficiente e objetivo, corre-se o sério risco de admiti-lo sem uma necessária análise crítica, desconsiderando aqueles riscos que afetam desproporcionalmente certos grupos sociais.

3 TECNOLOGIA DE RECONHECIMENTO FACIAL

O reconhecimento facial "é uma técnica de identificação biométrica, assim como a impressão digital, em que um *software* mapeia as linhas faciais e, por através de algoritmos, compara-os a uma imagem digital, reconhecendo (ou negando) sua identidade" (MAGNO; BEZERRA, 2020, p. 46). Seu conceito foi elaborado inicialmente na década de 1960, quando Woodrow Wilson Bledsoe, Helen Chan

Wolf e Charles Bisson desenvolveram o primeiro sistema semiautomático de reconhecimento (TRASLAVIÑA, 2015, p. 55).

No decorrer das décadas de 1970, 1980 e 1990, outras técnicas foram acrescentadas e aprimoradas. Entretanto, somente em 2001, durante um jogo do Super Bowl da Liga Nacional de Futebol Americano (NFL), foram capturadas, mediante a utilização de câmeras de vigilância, imagens dos rostos de torcedores para uma posterior confrontação em um banco de dados, demonstrando o potencial dessa tecnologia. (NUNES *et al*., 2016, p. 117).

Não é por outro motivo que, no ano de 2019, em Hong Kong, território autônomo da China, participantes de protestos contra o governo daquele país destruíram câmeras de videomonitoramento em áreas públicas, não devendo essa atitude ser tratada como mero vandalismo, mas como forma de defesa contra futuras repressões individuais, ao evitar serem reconhecidos (ELESBÃO; SANTOS; MEDINA, 2020, p. 247).

No que tange ao seu funcionamento, a verificação das faces é feita basicamente em duas fases, no momento da detecção do rosto em si e na sua verificação, usando-se, simultânea ou separadamente, duas abordagens: a global, em que se reduz uma imagem de milhares de *pixels* para um conjunto de números, chamado de Métodos Holísticos; e a abordagem local, em que são extraídas as características "locais" da face, como olhos, boca e sobrancelhas, usando suas posições no rosto, chamado de Métodos Estruturais ou Locais (NUNES *et al*., 2016, p. 119-120).

Segundo pesquisa exposta no Projeto Aguará (Otegui *et al*., 2006, p. 80), o algoritmo deve levar em conta aspectos que dificultam o processo de reconhecimento, tais como: "estado de ânimo da pessoa em decorrência do reconhecimento de expressões (triste, alegre, enojado etc.); localização de características relevantes encontradas nos olhos, boca, sobrancelhas, queixo, orelhas etc.; tamanho do rosto; presença de lentes, barba, gorros etc.; expressão do rosto; problemas de iluminação; condições da imagem; quantidade desconhecida de rostos na imagem etc."

Dito isso, podemos afirmar que tal tecnologia tem se desenvolvido gradativamente nas últimas décadas, ascendendo a uma forma de funcionamento cada vez mais ampla e complexa, na medida que assimila novas variáveis. Isso porque a possibilidade de coletar mais dados, e processá-los com mais agilidade, tem permitido avanços significativos da acessibilidade a tais mecanismos, fazendo com que esse dispositivo se torne cada vez mais comum para finalidades de controle social, tanto na iniciativa privada quanto pública.

Segundo Nunes (2019), o Brasil adotou oficialmente o uso de tecnologias de reconhecimento facial na área da Segurança Pública somente em 2019, após um ano de experiências em alguns estados do país, agravando o encarceramento em massa principalmente em decorrência da detenção de jovens negros das periferias brasileiras. Naquele ano, o estado da Bahia figurou como o primeiro a adotar esse tipo de tecnologia durante o carnaval, resultando na prisão de 74 pessoas.

Embora as promessas associadas a essas tecnologias biométricas sejam tentadoras, vendo no uso do reconhecimento facial uma forma de aumentar a eficiência do trabalho policial, é preciso muita cautela em um país no qual a polícia é questionada por seu viés racista. Pois, há uma ameaça constante de se minimizar os riscos de preconceito racial nas tecnologias, na medida em que se pressupõe que o algoritmo seja "isento" em relação a tarefa de selecionar eventuais suspeitos (NUNES, 2019).

É preciso explicar que as partes do corpo mais utilizadas na biometria, seja a impressão digital ou o mesmo o rosto, nunca serão analisadas completamente, na medida em que são escolhidos alguns de seus pontos para calcular a probabilidade de serem traços da pessoa cadastrada no banco de dados. Caso se fixem níveis inferiores aos 90% de semelhança estabelecidos, poderá provocar grande número de identificações, gerando uma quantidade significativa de falsos positivos. Em sentido contrário, "se o nível de semelhança exigido do algoritmo for 99,9%, por exemplo, a chance de o sistema emitir alertas será muito baixa" (NUNES, 2019, p. 68). Não é difícil concluir que tais falsos positivos fatalmente representariam constrangimentos públicos, prisões arbitrárias e evidentes violações de direitos e garantias fundamentais.

A Rede de Observatórios da Segurança tem monitorado os casos de prisões e abordagens decorrentes do uso do reconhecimento facial, assim como projetos de implementação dessa modalidade de vigilância e controle no país. Segundo informa, foi constatado que, de março a outubro de 2019, foram monitorados casos de prisões decorrentes do uso de tecnologia de reconhecimento facial em quatros estados brasileiros: Paraíba, Bahia, Rio de Janeiro e Santa Catarina. "Dos casos monitorados pela Rede, a Bahia foi responsável por 51,7% das prisões, seguida do Rio de Janeiro, com 37,1%, Santa Catarina, com 7,3% e Paraíba, com 3,3%" (NUNES, 2019, p. 69).

Apesar de em alguns casos monitorados ter sido difícil encontrar informações precisas sobre o perfil das pessoas presas ou abordadas pelas polícias, em seu conjunto, ou seja, na totalidade dos 66 casos identificados, havia informações sobre sexo, idade, raça/cor e motivação. Dentre as pessoas investigadas, foi possível constatar que: 87,9% dos suspeitos eram homens e 12,1%, mulheres; a idade média do grupo averiguado era de 35 anos; e, que 90,5% das pessoas eram negras e 9,5% eram brancas. No que concerne à motivação, os maiores números ficaram com os crimes de trafico de drogas e roubo, 24,1% cada uma (NUNES, 2019, p. 69).

Nesse caso, parece necessário enfatizar que, ao mesmo tempo em que países como a Bélgica passaram a adotar a proibição de tecnologia reconhecimento facial, conforme destacou Nunes (2019), no Brasil essa abordagem parece caminhar em um sentido contrário, na medida em que cresce cada vez mais o número de entusiastas. Estados como Minas Gerais, Espírito Santo, Pará e o Distrito Federal já declararam estar em processo de contratação ou de implementação deste tipo de tecnologia no campo da Segurança Pública. O mesmo parece estar ocorrendo em todos os estados do Nordeste, motivados por projetos de empresas chinesas que estão sendo implementados nessa região.

O governo federal tem contribuído significativamente para a expansão desse tipo de tecnologia, conforme podemos identificar na portaria n° 793 de 24 de outubro de 2019, que regulamenta sobre o uso de dinheiro do Fundo Nacional de Segurança Pública para "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* – OCR, uso de inteligência artificial ou outros" (NUNES, 2019, p. 69).

Logo, torna-se preocupante pensar que, em um país em que historicamente são desrespeitados os preceitos básicos de transparência de dados nos campos da segurança pública, associados aos correntes projetos que desconsideram plenamente a Lei Geral de Proteção de Dados Pessoais (LGPD), parece não haver preocupação em desenvolver mecanismos de *accountability* destinados as tecnologias de reconhecimento facial, tampouco protocolos voltados para a garantia da segurança no uso dos dados coletados.

A preocupação se agrava quando verificamos que os projetos que envolvem o uso do reconhecimento facial por parte das forças policiais de alguns estados brasileiros operam em consonância com a criação do Banco Nacional Multibiométrico e de Impressões Digitais proposto pelo então Ministro da Justiça, Sérgio Moro. Este banco foi apresentado como uma importante e necessária forma de modernização da prática policial, porém, segundo os especialistas, ele tem sido tratado como um retrocesso em relação à eficiência, transparência e proteção de dados pessoais da população (NUNES, 2019).

4 DISCRIMINAÇÃO RACIAL ALGORÍTMICA

Silva afirma que os algoritmos e a inteligência artificial, cada vez mais presentes em nosso dia a dia, com a utilização de biometria para desbloqueio de smartphones e o reconhecimento facial para acesso a determinados espaços, podem suscitar diversas preocupações relacionadas a preconceitos associados a raça, gênero, classe social, localização e neurodivergência. Segundo o autor, tais tecnologias não operam de maneira isenta, uma vez que implicam em um processo de racialização e opressão algorítmica que resultam em experiências discriminatórias. Assim, a programação pode ser responsável pela perpetuação de diversos preconceitos e equívocos (*SILVA*, 2020).

Apesar de terem sido concebidos com o objetivo de imparcialidade, visando superar as limitações de racionalidade dos seres humanos, os algoritmos absorvem escolhas, inclinações e preconceitos de seus programadores, mesmo que de forma não intencional, justificando aqui a preocupação com a discriminação algorítmica racial (FRAZÃO, 2021).

Ao analisar a crescente discriminação racial na rede mundial de computadores, Cardozo (2022) constatou que as mulheres negras são comumente vítimas de discursos de ódio nas mídias sociais. Segundo o autor, a discriminação algorítmica racial emerge contemporaneamente como o principal desafio para o enfrentamento da questão, que se consolida na infraestrutura e interface das tecnologias

digitais, nos recursos para processamento de imagens, na recomendação de conteúdos, dentre outras questões que evidenciam a necessidade de se discutir a "brancura" externada na internet.

Estudiosos evidenciam um exemplo significativo de discriminação algorítmica a partir do funcionamento do COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions* - Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativas), um sistema de inteligência artificial empregado pelos tribunais estadunidenses para estimar a probabilidade de reincidência de um réu. Os critérios avaliados, como local de residência, histórico de envolvimento com drogas, antecedentes familiares e desempenho escolar, resultaram em uma classificação de "alto risco" de reincidência para pessoas negras de maneira significativamente mais frequente e em maior número do que para indivíduos brancos. Este cenário expõe os preconceitos embutidos nos algoritmos a partir dos parâmetros definidos pelos programadores (SOARES et al., 2022).

De acordo com Taute (2020), o algoritmo é como uma receita, uma instrução que a máquina segue e, para executá-la, é necessário realizar consulta em um banco de dados. Se esse banco de dados contém preconceitos de raça, muitas pessoas são incluídas e excluídas do processo, acentuando disparidades. Sobre isso, vale lembrar a pesquisa desenvolvida por Joy Buolamwini, uma mulher negra de 30 anos, pesquisadora do Media Lab, do Instituto de Tecnologia de Massachusetts (MIT).

Ao desenvolver um protótipo de espelho inteligente, capaz de reconhecer a face da pessoa a sua frente, projetando feições de figuras inspiradoras como Serena Williams, Joy Buolamwini acoplou uma câmera para captar a imagem do seu rosto e transmiti-la ao seu computador que, por meio de um algoritmo de reconhecimento facial, iria identificar a pessoa e vincular às informações personalizadas. Porém, quando iniciou o experimento, o protótipo não detectou o seu rosto, só vindo a ter sucesso após utilizar uma máscara branca, demonstrando que a cor de sua pele inviabilizava o resultado (NUNES, 2021).

Um outro exemplo que deve ser mencionado trata da escolha de quem seria o sucessor do ator Daniel Craig na figuração do personagem James Bond. Inicialmente, havia sido divulgado que a indicação para esse papel se daria por meio do uso da Inteligência Artificial e direcionada a uma mulher negra. Porém, a seleção contrariou o que havia sido noticiado em 2019, resultando na contratação do ator Henry Cavill para o papel, outro homem branco. Ocorre que a IA foi alimentada com dados da indústria cinematográfica produzida no Norte global, possuindo uma ínfima participação de pessoas negras entre seus protagonistas (BEIGUELMAN, 2021).

Um estudo realizado por Tarcízio Silva et al. (2020, p. 30) sobre as falhas da rotulação pelo *Google Cloud Vision*, com foco nas imagens de mulheres negras, "mostrou que as fotos apresentavam recorrentemente o rótulo 'peruca', sempre que seus cabelos estavam em evidência", demonstrando a ausência em seus bancos de dados da indicação para fios cacheados ou não lisos, limitação essa de caráter cultural dos responsáveis pelos algoritmos. Logo, segundo os autores, "[...] esse universo de

relações sociais que está na base das IAs esclarece que a suposta misoginia e o racismo dos algoritmos têm dimensões humanas e políticas incontestes" (*SILVA et al.,* 2020, p. 33).

Conforme aponta a *National Institute of Standards and Technology* (NIST) do governo dos Estados Unidos da América, os algoritmos normalmente usados são muito menos precisos na identificação facial de indivíduos afro-americanos e asiáticos do que na indicação dos caucasianos. Nesse contexto analisado, as mulheres negras tinham maiores probabilidades de serem identificadas de forma errônea, perpetuando-se práticas racistas sob um viés tecnológico (NUNES, 2019).

O trabalho de Christina Baker (2005) também se destaca por reconhecer que os estereótipos midiáticos atribuídos às mulheres brancas e negras diferem substancialmente, na medida em que as imagens mais comuns associadas às mulheres negras não acompanham a mesma afabilidade e submissão que as mulheres brancas, que não são tratadas recorrentemente de um ponto de vista imagético como sexualmente agressivas e animalescas, ameaçando os homens em sua masculinidade.

Amaral, Martins e Elesbão (2021) mencionam pesquisas realizadas sobre o conteúdo presente nos bancos de imagens, envolvendo os padrões raciais de famílias nas plataformas digitais, que mantem majoritariamente o perfil de pessoas brancas.

> No banco de imagens Getty Images, das 300 imagens resultantes para a expressão family, 107 eram de famílias totalmente brancas, 24 eram de famílias totalmente negras, e 22 de famílias inter-raciais e de outras raças/etnias. Já no banco de imagens Shutterstock, das 319 imagens resultantes, 214 eram de famílias totalmente brancas, 20 eram de famílias totalmente negras, e 20 de famílias inter-raciais e de outras raças/etnias. Por fim, no banco Stock Photos de imagens, das 301 imagens resultantes para a expressão family, 213 eram de famílias totalmente brancas, 14 eram de famílias totalmente negras, e 15 de famílias inter-raciais e de outras raças/etnias. (AMARAL; MARTINS; ELESBÃO, 2021, p. 07).

Logo, a discussão dessa temática se faz urgente, já que potencialmente as desigualdades raciais se refletem por meio dos algoritmos, como uma extensão de opiniões, valores e padrões sociais do programador, a exemplo da forma como as imagens são disponibilizadas aos usuários na *internet* (AMARAL; MARTINS; ELESBÃO , 2021, p. 05).

5 RECONHECIMENTO FACIAL E RACISMO NA SEGURANÇA PÚBLICA

No que concerne à aplicação do reconhecimento facial na área de Segurança Pública, sua história remete ao evento terrorista ocorrido nos Estados Unidos no dia 11 de setembro de 2001. Foi a partir desse acontecimento que se impulsionou a utilização dessa tecnologia com fins de prevenção de crimes para diversos países, sendo um verdadeiro marco (NUNES *et al.*, 2016, p. 123-124).

Desde então, o reconhecimento facial tem sido cada vez mais tratado como uma tecnologia promissora na área da Segurança Pública. Através de algoritmos avançados, promete-se identificar indivíduos com base em características únicas de seus rostos, comparando-os com bancos de dados de imagens previamente cadastradas. Assim, segundo seus entusiastas, isso possibilitaria a identificação

rápida de suspeitos, pessoas procuradas pela justiça e indivíduos envolvidos em atividades criminosas (MELO; SERRA, 2022).

Segundo Rola (2022), a tecnologia biométrica mais impactante nos dias de hoje é o reconhecimento facial. Ao contrário de outras formas biométricas, como impressões digitais, leitura de íris ou da retina e voz, o reconhecimento facial é rápido e discreto em termos de coleta de dados, já que geralmente não exige a cooperação da pessoa a ser identificada. Diferentemente de outras modalidades biométricas, que requerem consentimento do indivíduo, a facial desponta como instrumento investigativo.

No entanto, conforme já apontado, o reconhecimento facial pode ser influenciado por fatores ambientais, como iluminação, ângulo de captura, expressão facial, pose, maquiagem e acessórios como óculos e chapéus. Desta feita, os eventuais equívocos no reconhecimento facial destacam uma fragilidade muito perigosa na seara da segurança. Em outras palavras, esses erros ressaltam a importância de aprimorar os algoritmos de reconhecimento facial, caso sejam de fato implementados, por meio de avanços na inteligência artificial, a fim de torná-los mais robustos e precisos, atendendo às demandas policiais sem significar uma criminalização imprudente.

Assim, investimentos contínuos em pesquisa e desenvolvimento podem contribuir para reduzir as taxas de erro e aumentar a confiabilidade do reconhecimento facial como ferramenta de segurança. Além disso, é fundamental garantir que a ética e a proteção de dados sejam consideradas na implementação dessas tecnologias, buscando um equilíbrio entre segurança e privacidade dos indivíduos (ROLA, 2022).

Segundo Francisco, Hurel e Rielli (2020, p.17), em face das falhas de procedimento citadas anteriormente, muitos são contra a utilização da tecnologia do reconhecimento facial pelos órgãos de Segurança Pública, em razão das pesquisas científicas demonstrarem grandes margens de falha ao analisarem rostos de mulheres e de pessoas negras. Não obstante o controle regulatório se desenvolver lentamente, nota-se um crescimento de sua incidência no Brasil, já que a aplicação de reconhecimento facial por polícias, guardas civis e outros órgãos de Segurança Pública tem ocorrido em ao menos 30 cidades, distribuídas por 16 estados do país, até o ano de 2022.

Um monitoramento feito pelo Intervozes revelou que, dentre os 26 prefeitos de capitais empossados em janeiro de 2021, 17 deles apresentaram propostas que versam sobre o uso de Tecnologias da Informação e Comunicação no campo Segurança Pública, abarcando também a implementação da tecnologia de reconhecimento facial (GOMES, MOURA, 2022).

Por sua vez, já foram noticiados diversos problemas relevantes em seu uso, tais como o ocorrido durante um período de testes da tecnologia de reconhecimento facial na praia de Copacabana. No segundo dia do experimento, uma mulher foi reconhecida como sendo Maria Lêda Félix da Silva, condenada por homicídio e procurada pela polícia, motivo pelo qual foi presa e conduzida à delegacia.

Depois de todo o constrangimento inerente a este tipo de procedimento, a mulher foi libertada quando seus familiares levarem seus documentos comprovando não ser a pessoa apontada pelo algoritmo.

O caso evidencia mais um exemplo, de uma série de erros que essas tecnologias promovem, porém com um agravante: Maria Lêda, a "mulher procurada", já estava cumprindo pena em um presídio havia quatro anos. Nesse caso, não só os algoritmos erraram, mas também a polícia que utilizou um banco de dados desatualizado (NUNES, 2021).

A questão ganha contornos relevantes quando há uma visão geral de que a tecnologia, juntamente com a ciência, é tida como objetiva, dificultando seu entendimento. Essa objetividade é contestável, já que seus fomentadores responsáveis tem um papel importante no resultado. Trata-se de uma área em acelerado crescimento, sem uma devida discussão política e ética geral, produzindo, assim, o que podemos denominar de racismo algorítmico, entendido como "o modo pelo qual a atual disposição de tecnologias e imaginários sociotécnicos em um mundo moldado pela supremacia branca fortalece a ordenação racializada de conhecimentos, recursos, espaço e violência em detrimento de grupos não-brancos" (*SILVA,2020*; SILVEIRA, 2022).

Portanto, importa lembrar o caso da cidade de Oakland, no estado americano da Califórnia, cujo Conselho Municipal proibiu em 2019 a utilização do reconhecimento facial por órgãos públicos, incluindo a própria polícia, em função do risco que ela traz aos moradores da cidade, com possibilidade de identificação equivocada de indivíduos, com posterior mal uso da força, prisões errôneas e perseguição de minorias (MAGNO; BEZERRA, 2020 p. 51).

Ao compreender que os riscos e malefícios referentes ao uso da tecnologia de reconhecimento facial são maiores que seus eventuais benefícios, a prefeitura de São Francisco foi a primeira estadunidense a banir o seu uso por parte dos agentes de Segurança Pública, em maio de 2019. Segundo o argumento apresentado pelos legisladores, o reconhecimento facial permite a exacerbação da injustiça social, ameaçando potencializar riscos já existentes.

Diante disso, os defensores da proibição do uso desse tipo de tecnologia pelas forças de Segurança Pública apontam que os modelos algorítmicos usados para treinar a tecnologia de reconhecimento facial são feitos, em sua maioria, por homens brancos, o que aumenta consideravelmente a probabilidade de identificação incorreta de pessoas negras. Além disso, para treinar esse tipo de tecnologia é necessário que o sistema faça uma varredura daqueles rostos que circulam por vias públicas, ainda que essas pessoas não saibam, ampliando o estado de constante vigilância (GOMES, MOURA, 2022).

Assim, embora lide com preocupações bem complexas, que tem causado discussões éticas e políticas, ainda se trata de uma área em desenvolvimento sem a abordagem crítica necessária. Os riscos de afetação a direitos fundamentais garantidos pela Constituição da República brasileira são grandes, sobretudo considerando que os efeitos de injustiças no campo da segurança pública remetem

diretamente a uma exposição pública vexatória da imagem, a restrições de liberdade e eventualmente até à morte.

6 CONSIDERAÇÕES FINAIS

O artigo apresentou uma revisão bibliográfica sobre a utilização da tecnologia de reconhecimento facial na área de Segurança Pública, associando-a a perpetuação de práticas discriminatórias por meio do chamado racismo algorítmico. Nessa intenção, buscou-se fornecer noções básicas de plataformização, dataficação da vida, colonialismo de dados, capitalismo de vigilância e de plataforma, discriminação racial algorítmica etc., bem como questionamentos sobre a sua utilização pelos órgãos de Segurança Pública brasileiros.

Nesse sentido, foi possível constatar que os algoritmos não são imparciais por natureza e podem, de fato, incorporar os preconceitos dos seus criadores ou dos conjuntos de dados utilizados durante o seu treinamento. Durante essa etapa, é possível que o desempenho do algoritmo apresente um viés tendencioso, uma vez que os preconceitos presentes nos dados de treinamento serão refletidos em suas decisões e ações.

Essa questão é particularmente importante quando se trata de aplicações que impactam diretamente a vida das pessoas, principalmente a partir da utilização de sistemas de tomada de decisões decorrentes do uso desse tipo de tecnologia biométrica. Se os dados utilizados para treinar esses algoritmos contêm preconceitos, seja de gênero, raça, classe social ou outros quaisquer, é provável que o sistema reproduza e até amplifique esses comportamentos em suas decisões.

Dessa forma, o poder é exercido com sutileza, em que a capacidade de matar ou de deixar viver é feita sem ser notada, com uma tecnologia que não opera pela utilização neutra de seus dados. Logo, necessário se faz compreender e limitar sua aplicação sob pena de submeter uma parcela da sociedade a uma nova ferramenta de discriminação racial, com uma maior propagação de práticas opressoras.

Compreender o sopesamento entre o direito à Segurança Pública e o direito ao devido processo legal é absolutamente necessário, ante o imperativo de garantir o direito constitucional do não tratamento desigual injustificado. Em um contexto de prestação do serviço público de proteção à coletividade, é preciso toda cautela considerando a história de inúmeras violências e discriminações raciais num país com herança escravagista.

REFERÊNCIAS

AMARAL, Augusto Jobim do; MARTINS, Fernanda; ELESBÃO, Ana Clara. Racismo algorítmico: uma análise da branquitude nos bancos de imagens digitais. Revista Pensar, Fortaleza, v. 26, n. 4, p. 1-9, out./dez. 2021. Disponível em: https://ojs.unifor.br/rpen/article/view/11806 Acesso em: 23 jul. 2024.

BAKER, Christina N. Images of women's sexuality in advertisements: a content analysis of black and white oriented women's and men's magazines. Sex Roles. v. 52. n. 1/2. p. 13-27, jan. 2005. Disponível em: https://link.springer.com/article/10.1007/s11199-005-1190-y Acesso em: 24 jul. 2024.

BARROS, Isabel Maria Pereira Paes de; SILVA, Isabel Inês Bernardino de Souza. Utilização do reconhecimento facial eletrônico por empresas para identificação de suspeitos: segurança ou violação do estado democrático de direito? Revista Transgressões: Ciências Criminais em debate. Vol. 8, n. 1, jul. 2020. Disponível em: https://periodicos.ufrn.br/transgressoes/article/view/19909 Acesso em: 23 jul. 2024.

BEIGUELMAN, Giselle. Políticas da imagem: vigilância e resistência na dadosfera. São Paulo: Ubu Editora, 2021.

CARDOZO, Glenda Dantas. A atuação estratégica de mulheres negras no combate às brechas digitais de gênero e raça. Internet & Sociedade, v. 3, n. 2, p. 5-19, dez. 2022.

COSTA, Diego Carneiro. A discriminação algorítmica e as novas perspectivas sobre o tratamento de dados pessoais sensíveis. In: REQUIÃO, Maurício (Org.). Proteção de dados pessoais: novas perspectivas. Salvador: Editora da Universidade Federal da Bahia, 2021.

DA EMPOLI, Giuliano. Os engenheiros do caos. Rio de Janeiro: Vestígio, 2019.

ELESBÃO, Ana Clara Santos; SANTOS, Jádia Larissa Timm dos; MEDINA, Roberta da Silva. Quando as máscaras (do reconhecimento facial) caírem, será um grande carnaval. In: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldissera Carvalho (Orgs.). Algoritarismo. 1. ed. São Paulo. Editora Tirant lo Blanch., 2020. p. 247-259.

FOUCAULT, Michel. Em defesa da sociedade. São Paulo: Martins Fontes, 1999.

FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; RIELLI, Mariana Marques. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituto Igarapé + Data Privacy Brasil Research, jun. 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf Acesso em: 13 out. 2023.

FRAZÃO, Ana. Discriminação algorítmica: por que os algoritmos preocupam quando acertam e quando erram? Jota, ago. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-por-que-algoritmos-preocupam-quando-acertam-e-erram-04082021 Acesso em: 07 set. 2023.

GARRET, Filipi. ROBOS (BOTS). Disponível em: https://www.techtudo.com.br/noticias/2018/07/o-que-e-bot-conheca-os-robos-que-estao-dominando-a-internet.ghtml. Acesso em: 21 jan. 2024.

GERVASONI, Tássia A.; DIAS, Felipe V. Violações de Direitos Humanos pelas Big Techs: contribuições do pensamento decolonial e de uma leitura criminológica do dano social. Revista de Garantias e Direitos Fundamentais, Vitória, v. 24, n. 03, p. 137-173, set-dez, 2023.

GOMES, Sheley; MOURA, Iara. De Oakland ao Jacarezinho: os sistemas de reconhecimento facial precisam ser banidos. Revista Capital, 2022. Disponível em: https://www.cartacapital.com.br/blogs/de-oakland-ao-jacarezinho-os-sistemas-de-reconhecimento-facial-precisam-ser-banidos Acesso em: 21 jan. 2024.

LEMOS. André. Dataficação da vida. Revista Civitas, maio-ago. 2021. Disponível em: http://dx.doi.org/10.15448/1984-7289.2021.2.39638 Acesso em: 09 jan. 2024.

MAGNO, Madja Elayne da Silva Penha; BEZERRA, Josenildo Soares. Vigilância negra: o dispositivo de reconhecimento facial e disciplinaridade dos corpos. Revista Novos Olhares, vol. 09, nº 2, ago./dez. 2020. Disponível em: https://www.revistas.usp.br/novosolhares/article/view/165698 . Acesso em: 30 jan. 2024.

MELO, Paulo Victor; SERRA, Paulo. Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. Comunicação e Sociedade, v. 42, p. 205-220, 2022. Disponível em: https://journals.openedition.org/cs/8111 Acesso em: 23 jul. 2024.

NUNES, Fernanda Todesco et al. Um estudo sobre técnicas de biometria baseadas em padrões faciais e sua utilização na Segurança Pública. In: SPANHOL, Fernando J.; LUNARDI, Giovani M.; SOUZA, Márcio Vieira de (org.) Tecnologias da Informação e Comunicação na Segurança Pública e Direitos Humanos. Coleção Mídia, Educação, Inovação e Conhecimento, vol. 2., Editora Edgard Blücher Ltda., p. 113-132, 2016.

NOBLE, Safiya. Algoritmos da opressão. Santo André: Rua do Sabão, 2021.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. In: REDE de Observatório de Segurança. Retratos da violência: cinco meses de monitoramento, análise e descobertas. Centro de Estudos em Segurança e Cidadania, 2019.

NUNES, Pablo. O algoritmo e racismo nosso de cada dia. Revista Piauí. 02 jan. 2021, Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/ Acesso em: 23 jul. 2024.

OTEGUI, C. A. et al. Proyecto Aguará – Reconocimiento de Caras. Montevideo: Facultad de Ingeniería Universidad de la República, 2006.

_____. O algoritmo e racismo nosso de cada dia. Folha de São Paulo [on line], São Paulo, 02 jan. 2021. Questões de vida digital. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia Acesso em: 07 jan. 2024.

POELL, Thomas; NIEBORG, David; DIJCK, José van.
Plataformização. Revista Fronteiras - estudos midiáticos. Vol. 22, nº 1 – jan. abr. 2020. Disponível em: https://revistas.unisinos.br/index.php/fronteiras/article/view/fem.2020.221.01 Acesso em: 23 jul. 2024.

ROCHA, Jannotti da; PORTO, Lorena Vasconcelos; ABAURRE, Helena Emerick. Discriminação algorítmica no trabalho digital. Revista de Direitos Humanos e Desenvolvimento Social, v. 1, e 205201, 2020. Disponível em: https://seer.sis.puc-campinas.edu.br/direitoshumanos/article/view/5201/3164. Acesso em: 07 dez. 2023.

ROLA, Eulálio do Carmo da Silva. Os principais contributos da inteligência artificial para o processamento de imagens digitais a utilizar na Segurança Pública. 2022, 146 f. Dissertação (Mestrado em Segurança e Justiça) – Universidade Lusíada, Lisboa, 2022.

ROSA, Pablo Ornelas; AMARAL, Augusto Jobim do; NEMER, David Baião. Datapolítica, governamentalidade algorítmica e a virada digital: uma genealogia da modulação comportamental através das plataformas digitais. Revista Eletrônica do Curso de Direito da UFSM. v. 18, n. 03, 2023. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/85510 Acesso em: 23 jul. 2024.

ROUVROY, Antoinette; BERNS, Thomas. Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? Revista Eco Pós. Rio de Janeiro, v. 18, n. 2, p. 36-56, 2015. Disponível em: https://doi.org/10.29146/eco-pos.v18i2.2662 Acesso em: 18 nov. 2023.

SILVA, Tarcízio. Visão computacional e racismo algorítmico: branquitude e opacidade no aprendizado de máquina. Revista ABPN, v. 12, p. 428-448, dez. 2019/fev. 2020. DOI: 10.31418/2177-2770.2020. Disponível em: https://abpnrevista.org.br/site/article/view/744/774 Acesso em: 07 set. 2023

SILVEIRA, Sérgio Amadeu. Governo dos algoritmos. Revista de Políticas Públicas, v. 02, nº 01, p. 267-281, 2016. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4452794/mod_resource/content/1/S%C3%A9rgio%20Amadeu%20SILVEIRA%20%20Governo%20dos%20Algoritmos.pdf Acesso em: 26 jan. 2024.

_____. Sistemas algorítmicos, subordinação e colonialismo de de dados. In: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldissera Carvalho (organizadores). Algoritarismo. 1. ed. São Paulo: Editora Tirant lo Blanch, 2020. p. 158-1709.

SOARES, Marcelo Negri et al. Inteligência artificial e discriminação: um panorama sobre a antagonização entre exclusão e o Estado Democrático de Direito Brasileiro à luz dos direitos da personalidade. Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE), v. 10, n. 2, p. 567-597, 2022. Disponível em: https://portal.unifafibe.com.br/revista/index.php/direitos-sociais-politicas-pub/article/view/1311 Acesso em: 07 jan. 2024.

SRNICEK, Nick. Capitalismo de plataforma. Buenos Aires: Ed. Caja Negra, 2018.

SILVA, Tarcízio et al. “Apis de visão computacional: Investigando mediações algorítmicas a partir de estudo de bancos de imagens”. Logos, n. 1, v. 27, 5 jun. 2020, pp. 25-54. Disponível em: https://www.e-publicacoes.uerj.br/logos/article/view/51523/33928 Acesso em: 26 jul. 2024.

TAUTE, Fabian. Reconhecimento Facial e suas controvérsias: O reconhecimento facial não só traz a possibilidade de instaurar uma vigilância em massa, mas também contém uma tendência preconceituosa contra certos grupos de nossas sociedades – com as mulheres negras sendo as mais afetadas. Heinrich Böll Stiftung, Rio de Janeiro, 7 fev. 2020. Disponível em: https://br.boell.org/pt-br/2020/02/05/reconhecimento-facial-e-suas-controversias Acesso em: 07 set. 2023.

TRASLAVIÑA, C. M. G. Introducción a la biometría. 2007. Disponível em: https://www.academia.edu/9374109/Introducci%C3%B3n_a_la_biometr%C3%ADa Acesso em: 17 nov. 2023.

VAIDHYANATHAN, Siva. A Googlelização de tudo. São Paulo: Cultrix, 2011.

ZUBOFF, Shoshana. A era do capitalismo de vigilância: Luta por futuro humano na nova fronteira de poder. Rio de Janeiro: Ed. Intrínseca, 2020.