UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE CIÊNCIAS PENAIS

EDUARDO CANTON RODRIGUES

RECONHECIMENTO FACIAL NA VIGILÂNCIA PÚBLICA

Porto Alegre
2023

EDUARDO CANTON RODRIGUES

RECONHECIMENTO FACIAL NA VIGILÂNCIA PÚBLICA

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito, junto à Faculdade de Direito da Universidade Federal do Rio Grande do Sul.
Orientador: Marcus Vinícius Aguiar Macedo

Porto Alegre
2023

EDUARDO CANTON RODRIGUES

RECONHECIMENTO FACIAL NA VIGILÂNCIA PÚBLICA

BANCA EXAMINADORA

_____
Professor Doutor Marcus Vinícius Aguiar Macedo
Orientador

_____
Professor Doutor Odone Sanguiné
Avaliador

_____
Professor Doutor Pablo Rodrigo Alflen da Silva
Avaliador

Porto Alegre
2023

AGRADECIMENTOS

Primeiramente, agradeço ao Estado e ao povo brasileiro pela oportunidade de realizar meu curso de ensino superior em uma universidade pública e gratuita da maior qualidade. Igualmente agradeço à UFRGS e à Faculdade de Direito por me proporcionarem uma excelente formação.

Aos meus pais, tios e primos, pelo carinho e apoio essencial ao longo dos anos.

Aos meus amigos, aqueles que passaram pela minha vida e aos que continuam nessa caminhada comigo, em especial: Rafael, Bibiana, Anelise, Gabriela, Amanda e Paula, vocês me ensinaram muito e tornaram tudo melhor do que poderia ter sido.

“Whatever you plan on happening, never happens. Stuff you would never think of happens. So you just have to come on. Come on, come on, come on, come on…”

— C'mon C'mon (2021)

RESUMO

A introdução das tecnologias de reconhecimento facial para aprimorar a vigilância e segurança pública no Brasil tem gerado debates devido ao histórico de viés racial no sistema de justiça do país e à falta de transparência na gestão dessas ferramentas. Preocupações surgem devido à possibilidade de manipulação de dados, ameaçando as garantias individuais. A pesquisa, dividida em duas partes, tem como objetivo primevo aprofundar o uso do reconhecimento facial e, depois, examiná-la sob a perspectiva da questão processual penal. Na metodologia, será fundamentada em uma abordagem interdisciplinar, que combina elementos da pesquisa bibliográfica, análise de casos e avaliação crítica de políticas e regulamentações.

Palavras-chave: Reconhecimento Facial; Vigilância; Big Data; Sistema Penal.

ABSTRACT

The introduction of facial recognition technologies to enhance surveillance and public security in Brazil has sparked debates due to the country's history of racial bias in the justice system and the lack of transparency in the management of these tools. Concerns arise due to the potential for data manipulation, threatening individual rights. The research, divided into two parts, aims first to delve into the use of facial recognition and then to examine it from the perspective of the criminal procedural issue. In the methodology, it will be grounded in an interdisciplinary approach that combines elements of bibliographic research, case analysis, and critical evaluation of policies and regulations.

Keywords: Facial Recognition; Surveillance; Big Data; Penal System.

LISTA DE ABREVIATURAS OU SIGLAS

IA	Inteligência Artificial
COMPASS	Correctional Offender Management Profiling for Alternative Sanctions
LGPD	Lei Geral de Proteção de Dados
LAPIN	Laboratório de Políticas Públicas e Internet
IDEC	Instituto Brasileiro de Defesa do Consumidor
ANPD	Autoridade Nacional de Proteção de Dados
TRF	Tecnologia de Reconhecimento Facial
GDPR	Regulamento Geral de Proteção de Dados

SUMÁRIO

INTRODUÇÃO

O que antes era só era possível imaginar através da perspectiva cinematográfica futurista, estilo *Minority Report* agora pode caminhar para se tornar realidade. A prevenção de qualquer tipo de ato criminoso por uma sociedade sob vigilância total e permanente, apoiada em tecnologias avançadas de monitoramento.

No cenário contemporâneo, a interseção entre avanços tecnológicos e sua aplicação nas áreas de segurança pública tem gerado debates e reflexões acerca dos impactos socioculturais e éticos decorrentes dessas inovações. Uma das tecnologias que tem ganhado destaque é o reconhecimento facial, um campo da inteligência artificial que automatizará a identificação de indivíduos por meio de suas características faciais únicas. Essa tecnologia tem sido adotada por agências de segurança pública em diversos países, incluindo o Brasil, como uma ferramenta promissora para melhorar a vigilância, investigação e prevenção de crimes.

No entanto, à medida que essas tecnologias são implementadas e incorporadas às práticas policiais e de segurança, surgem preocupações significativas sobre suas implicações no tocante aos direitos civis, à privacidade e, especialmente, à perpetuação do viés racial. No contexto brasileiro, onde as desigualdades sociais e raciais historicamente persistem, o uso de tecnologias de reconhecimento facial na segurança pública apresenta um desafio complexo e multifacetado. A compreensão dos possíveis impactos dessas tecnologias no agravamento do racismo algorítmico torna-se essencial para uma análise crítica e informada.

A noção de “racismo algorítmico” destaca a preocupação de que sistemas de inteligência artificial e algoritmos possam inadvertidamente perpetuar discriminação racial devido a dados de treinamento enviesados ou características intrínsecas à sua concepção. Esse fenômeno pode se manifestar por meio de viés nos dados usados para treinamento, na própria estrutura do algoritmo, ou mesmo na retroalimentação contínua de preconceitos. Além disso, os impactos desproporcionais em grupos raciais e a falta de transparência e responsabilidade em relação às decisões algorítmicas são elementos fundamentais desse problema. Para enfrentar o racismo algorítmico, esforços estão sendo feitos para desenvolver algoritmos mais justos,

criar regulamentações e diretrizes que orientem o uso ético da IA em contextos sensíveis à raça e promover a transparência, garantindo que a IA seja uma ferramenta que promova a equidade em vez de reforçar preconceitos.

Este trabalho visa, portanto, investigar e analisar como o uso das tecnologias de reconhecimento facial na segurança pública contribui para o racismo algorítmico no contexto brasileiro, examinando como essas desigualdades históricas são refletidas e ampliadas nas aplicações práticas das tecnologias de reconhecimento facial.

Para isso, será realizado um estudo das implicações éticas, legais e sociais dessa aplicação tecnológica, bem como a identificação de casos concretos onde o uso inadequado ou discriminatório dessas tecnologias tenha resultado em consequências prejudiciais, desproporcionais e injustas para grupos racialmente minorizados.

Ao longo dos próximos capítulos, serão explorados os aspectos fundamentais das tecnologias de reconhecimento facial, os mecanismos que contribuem para o racismo algorítmico, os desafios regulatórios e legais, bem como as reflexões sobre as possíveis soluções para mitigar os efeitos negativos dessa interseção entre tecnologia, segurança pública e questões raciais.

A adoção generalizada de tecnologias de reconhecimento facial também traz consigo riscos relacionados à erosão dos direitos civis e à invasão da privacidade dos cidadãos. A vigilância constante e indiscriminada pode impactar negativamente o exercício das liberdades individuais e coletivas, especialmente quando aplicada de forma discriminatória.

O entendimento aprofundado dos impactos do uso de tecnologias de reconhecimento facial na segurança pública pode fornecer percepções cruciais para a formulação de políticas públicas e regulamentações mais adequadas. Investigar as experiências passadas e atuais permitirá a identificação de boas práticas e a proposição de medidas que minimizem os riscos de discriminação racial e vieses algorítmicos.

Este estudo também visa a aumentar a conscientização pública sobre os riscos associados ao uso indiscriminado de tecnologias de reconhecimento facial. Ao fornecer informações substanciais sobre os possíveis impactos negativos, espera-se que os cidadãos estejam mais bem informados para participar de debates e

decisões que afetam suas liberdades individuais e coletivas.

Em vista dessas considerações, a relevância deste trabalho reside na sua capacidade de lançar luz sobre as interações complexas entre tecnologia, segurança pública e questões raciais no Brasil. Ao fornecer uma análise aprofundada e baseada em evidências, este estudo tem o potencial de informar tanto o público quanto os formuladores de políticas sobre os desafios e oportunidades inerentes ao uso de tecnologias de reconhecimento facial na busca por um sistema de segurança pública mais justo e igualitário.

A metodologia de pesquisa adotada neste trabalho será fundamentada em uma abordagem interdisciplinar, que combina elementos da pesquisa bibliográfica, análise de casos e avaliação crítica de políticas e regulamentações. Para alcançar os objetivos propostos e responder às questões de pesquisa, o seguinte roteiro metodológico será seguido: realização de uma pesquisa em fontes acadêmicas, literatura científica, relatórios governamentais, artigos de jornais e revistas especializadas, bem como documentos técnicos, que abordem os temas relacionados às tecnologias de reconhecimento facial, racismo algorítmico, segurança pública e questões raciais no contexto brasileiro. Seleção e análise de casos concretos onde o uso de tecnologias de reconhecimento facial na segurança pública tenha levado a situações de racismo algorítmico no Brasil. Serão investigados incidentes específicos de erro de identificação, discriminação e outros cenários relevantes, a fim de ilustrar os potenciais riscos e impactos dessas tecnologias.

A combinação dessas abordagens metodológicas permitirá uma análise abrangente e aprofundada do uso das tecnologias de reconhecimento facial na segurança pública e sua relação com o racismo algorítmico no contexto brasileiro. Além disso, contribuirá para uma compreensão mais holística das implicações éticas, sociais e regulatórias desse tema complexo e atual.

2. Tecnologias de reconhecimento facial

O funcionamento da tecnologia de reconhecimento facial se baseia no processamento de dados faciais. Inicialmente, ao capturar a imagem de um rosto, o sistema detecta características particulares da pessoa, como a distância entre os olhos, a largura do queixo e o comprimento da boca[1]. Utilizando esses dados, o software realiza cálculos para criar uma espécie de fórmula que corresponde à assinatura facial, tornando-se a chave para a identificação daquela pessoa.[2]

Essa assinatura é então contrastada com outras já armazenadas em um banco de dados contendo imagens de pessoas que se deseja localizar. Quando as assinaturas faciais correspondem, torna-se viável realizar uma identificação automatizada do indivíduo. Dado que os dados utilizados para construir essa assinatura facial estão diretamente ligados a características físicas exclusivas da pessoa, eles são categorizados como dados biométricos.[3]

Por digital *surveillance*, compreende-se o conjunto de ações direcionadas para a vigilância, segurança e manipulação de dados, as quais fazem parte das atividades destinadas a administrar comportamentos, informações e salvaguarda. Isso substituiu as abordagens disciplinares de confinamento durante períodos de crise institucional, caracterizados como a implantação gradual e dispersa de um novo regime de controle. Dessa forma, as práticas de administração de comportamentos, informações e segurança estabelecidas por meio das "novas tecnologias" constituem a vigilância digital.

Apesar disso, já estamos testemunhando situações reais em que indivíduos foram afetados pela tecnologia de reconhecimento facial, sendo erroneamente identificados como fugitivos da justiça. Isso evidência a necessidade de aprimorar

---

[1] A biométrica analisa características físicas do ser humano, características estas singulares, como as impressões digitais e padrões do rosto, possibilitando a identificação de um indivíduo, que, à partida, tem características físicas diferentes, cfr. RODRIGUES, Sara Raquel dos Santos, "Desenvolvimento de um Sistema de Reconhecimento Facial", ob. cit., p. 1; Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", junho, 01248/07/EN WP136, p.8, disponível em https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2007/wp136_en.pdf Acesso em: 5 ago. 2023.

[2] ELECTRONIC FRONTIER FOUNDATION (EFF). Face Recognition. 2017. Disponível em: https://www.eff.org/pages/face-recognition. Acesso em: 5 ago. 2023.

[3] THALES. Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) — 2020 review. 2020.

esse sistema, considerando seu impacto na vida de todos e a importância de evitar qualquer estigmatização com base na cor da pele de uma parcela da população. Uma condição essencial para o desenvolvimento do que é denominado pela autora como “internet das coisas” é que sua expansão não ocorra em detrimento da segurança e da privacidade dos seres humanos[4] .

É fato comprovado que, desde a implementação do monitoramento facial no Brasil, o número de detenções decorrentes do reconhecimento de imagens aumentou significativamente, especialmente em regiões como Bahia, Rio de Janeiro, Santa Catarina e Paraíba. Para muitos, isso pode parecer eficaz para a segurança pública. No entanto, isso resultou em um problema mais grave: constrangimento, prisões arbitrárias e violações dos direitos humanos[5].

Para entender a razão por trás da tendência desse viés que tem afetado principalmente indivíduos negros, é necessário revisitarmos questões históricas e culturais. Essas questões mostram que o julgamento com base na cor da pele não é uma prática atual, algo que infelizmente continua presente nas relações sociais e, agora, se integra à tecnologia para determinar a liberdade das pessoas. No entanto, é importante lembrar que as máquinas seguem comandos humanos, e é através desses comandos que preconceitos racistas podem ser incorporados.

> Integrante do Grupo de Pesquisa em Políticas e Economia da Informação e Comunicação da UFRJ, Silvana Bahia ressalta que o racismo algorítmico reproduz e intensifica o racismo presente na sociedade. Nas palavras dela, “o racismo algorítmico ocorre quando sistemas matemáticos ou de inteligência artificial são pautados por informações enviesadas/tortas que alimentam e regem seu funcionamento. As consequências são muitas, mas talvez a maior delas seja o aumento de desigualdades, sobretudo em um momento onde estamos cada vez mais tendo muitos dos nossos gostos e políticas mediadas por máquinas, com o avanço da tecnologia”[6].

[4] MAGRANI. E. (2018). A internet das coisas. Rio de Janeiro: FGV Editora.
[5] NUNES, Pablo. O algoritmo e racismo nosso de cada dia: Reconhecimento facial aposta no encarceramento e pune preferencialmente população negra. Piauí, 2 jan. 2021. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-eracismo-nosso-de-cada-dia. Acesso em: 13 ago. 2023.
[6] HERCOG, A.; MELO, P. V. O racismo que estrutura as tecnologias digitais de informação e comunicação. Brasil de fato, 2019. Disponível em: https://www.brasildefato.com.br/2019/12/03/artigo-or-o-racismo-que-estrutura-astecnologias-digitais-de-informacao-e-comunicacao. Acesso em 13 ago. de 2023.

A vigilância digital não pode ser concebida como uma completa fragmentação destas inovações tecnológicas, e o desafio das câmeras com capacidade de reconhecimento facial também não pode ser simplificado restritamente. Isto se deve ao fato de que o reconhecimento facial não é alcançado exclusivamente por meio de câmeras. É fundamental o desenvolvimento de uma rede neural profunda (*software*), alimentada por um vasto conjunto de dados para viabilizar atividades de inteligência artificial limitada. A inteligência artificial deriva da tentativa de instruir uma máquina a emular a inteligência humana, representando assim uma das técnicas de aprendizado de máquina.

No panorama em constante evolução das inovações tecnológicas, poucos avanços capturaram a imaginação e a controvérsia do público, como as Tecnologias de Reconhecimento Facial. Essa vertente da inteligência artificial, que emulará a capacidade humana de identificar indivíduos através de suas características faciais distintas, testemunha um crescimento vertiginoso nas últimas décadas. Seja aplicada para fins de segurança, comodidade ou personalização, a capacidade das máquinas de decifrar a complexidade do rosto humano está remodelando a maneira como interagimos com o mundo ao nosso redor[7].

Ao conjunto vasto de informações disponíveis na internet damos o nome de *big data*, termo que descreve a prática de coletar e armazenar diversos tipos de dados. Isso está diretamente relacionado à mineração de dados, a qual envolve a extração de informações valiosas desse conjunto caótico. Esse processo é executado por algoritmos computacionais que correlacionam rapidamente dados e identificam padrões[8]. Uma das aplicações mais significativas dessa tecnologia está na criação de perfis individuais para cada usuário da internet, nos quais seu histórico, rede de contatos e preferências são discernidos, permitindo a previsão do comportamento dessa ampla comunidade de internautas.

A elaboração de perfis é amplamente empregada em plataformas online, como redes sociais e mecanismos de busca, com o propósito de personalizar a entrega de conteúdo e anúncios para cada usuário. Essa prática tem dois objetivos principais: o primeiro é garantir que o usuário receba informações pertinentes aos

[7] ZUBBOF, Shoshana. A Era do Capitalismo de Vigilância. 1 ed. Editora Intrínseca, 2021. p.18

[8] RODRIGUES, Anabela Miranda, "A Inteligência Artificial no Direito Penal", ob. cit., p. 23; FIDALGO, Sônia, "A utilização de inteligência artificial no âmbito da prova digital — direitos fundamentais (ainda mais) em perigo", ob. cit, p. 130

seus interesses, incentivando-o a permanecer mais tempo na plataforma; o segundo, consequentemente, é exibir anúncios publicitários mais propensos a serem eficazes para cada indivíduo, uma vez que essa é a principal fonte de receita das plataformas digitais na atualidade. Por essa razão, as entidades privadas online constituem a maior fonte de dados comportamentais na internet.

Quando o usuário dá permissão, mesmo sem pleno conhecimento, para o acesso aos seus dados, empresas de tecnologia, notáveis e únicas em sua abordagem, asseguram a utilização de seus sistemas e o acesso a suas ferramentas, sob a premissa de resolver problemas e atender necessidades, ocultando o viés subjacente de transformar toda a informação disponível em lucro [9]. Nesse contexto, em um arranjo de "troca" entre o usuário e a empresa, essas novas tendências de liderança garantem a obtenção de um vasto conjunto de dados, previamente considerados privados, porém com potencial para outras aplicações.

É relevante destacar que, no cenário do capitalismo do século XXI, o Estado não permanece indiferente a essas dinâmicas. Ele possui seus próprios sistemas de armazenamento, mecanismos de compartilhamento de dados públicos e práticas de colaboração com entidades privadas, inseridas no mercado de dados tecnológicos. No contexto onde as concepções de inteligência artificial são frequentemente moldadas pelo fascínio e lucratividade, especialmente diante da perspectiva de máquinas e sistemas superinteligentes, os inventores e financiadores dessas tecnologias podem desfrutar de vantagens significativas[10]. No entanto, é crucial não negligenciar a inteligência estreita, sendo amplamente empregada no cotidiano, como na visão computacional, reconhecimento facial, sugestões de conteúdo e assim por diante. Isso ocorre porque as interações complexas entre tecnologia, sociedade e políticas podem desencadear resultados prejudiciais[11] .

---

[9] MOROZOV, Evgeny. Bit tech: a ascensão dos dados e a morte da política. São Paulo: Ubu, 2018. p 28.

[10] ZUBBOF, Shoshana. Op. Cit., 2021. p.17.

[11] SILVA, Tarcizio. Dos autômatos e robôs às redes difusas de agência no racismo algorítmico. In: TAVARES, A. R. Vestígios do Futuro: 100 Anos de Isaac Asimov. Rio de Janeiro: Editora Etheria, 2020. Acesso em: https://tarciziosilva.com.br/blog/dos-automatos-e-robos-as-redes-difusas-de-agencia-no-racismo-algoritmico/

2.1 HISTÓRIA

O reconhecimento facial tem suas raízes na década de 1960, quando os primeiros passos foram dados para explorar a identificação facial através da correspondência de características geométricas em fotografias. Entretanto, os métodos eram rudimentares na época e limitados pela tecnologia disponível.
O marco inicial para as Tecnologias de Reconhecimento Facial modernas pode ser traçado até a década de 1960, quando os primeiros estudos científicos começaram a explorar a viabilidade de automatizar esse processo.

Nas décadas de 1960[12] e 1970, os pesquisadores pioneiros começaram a desenvolver algoritmos e técnicas rudimentares para analisar as características faciais e compará-las com dados armazenados. Entretanto, a tecnologia da época limitava significativamente a precisão desses sistemas. Foi somente nas décadas seguintes, com o aumento do poder de processamento dos computadores e avanços na visão computacional, que os primeiros sistemas de reconhecimento facial mais robustos começaram a surgir.

A década de 1980 viu um crescente interesse em reconhecimento facial, mas os avanços eram limitados devido à falta de poder computacional e dados disponíveis.

Nos anos 1990, ocorreu um avanço com o desenvolvimento de algoritmos mais sofisticados de correspondência de características e técnicas de detecção de rosto, bem como a exploração de sistemas baseados em redes neurais artificiais.

A virada do século XXI testemunhou um crescimento exponencial no desenvolvimento de Tecnologias de Reconhecimento Facial, trouxe avanços significativos, com algoritmos baseados em Eigenfaces[13], redes neurais convolucionais e técnicas de aprendizado de máquina, tornando o reconhecimento facial mais preciso e robusto.

Na década de 2010, o reconhecimento facial se tornou mais visível com a inclusão dessa tecnologia em smartphones e câmeras digitais para desbloqueio de

[12] Em 1960, o professor Paul Ekman, da Universidade da Califórnia, realizou uma série de estudos sobre microexpressões faciais humanas. Seus estudos no campo da Psicologia até hoje influenciam na construção de Tecnologias de Reconhecimento Facial. Dr. Ekman's Work: A timeline of achievements. Disponível em: https://www.paulekman.com/about/paul-ekman. Acesso em: 08 jun. 2021.
[13] Conjunto de autovetores de uma matriz de covariância formada por imagens de faces (rostos)

dispositivos e classificação de fotos. Empresas como *Apple* e *Google* lançaram seus próprios sistemas de reconhecimento facial.

Empresas e instituições governamentais começaram a explorar ativamente seu potencial em diversas áreas, desde segurança e aplicação da lei até o comércio e a interação com dispositivos eletrônicos. A proliferação de câmeras digitais e smartphones possibilitou a coleta de uma quantidade imensa de dados faciais, alimentando algoritmo de aprendizado de máquina que aprimoraram a precisão desses sistemas.

2.2 Reconhecimento facial na segurança pública

No contexto da segurança pública, a tecnologia de reconhecimento facial desempenha um papel significativo na identificação e localização de indivíduos suspeitos ou procurados pelas autoridades. Esse sistema é construído com base na captura e análise de imagens faciais, comparadas com registros presentes em bancos de dados que contêm informações sobre criminosos, suspeitos e pessoas sob investigação.

Os bancos de dados utilizados para comparação contêm imagens faciais de pessoas procuradas pela polícia, criminosos condenados e outros indivíduos de interesse para as autoridades. Essas informações são alimentadas no sistema, que realiza uma correspondência entre as imagens capturadas pelas câmeras e os registros no banco de dados. O grau de similaridade entre as características faciais determina a probabilidade de identificação correta[14].

Quando uma pessoa capturada pela câmera é identificada como tendo uma semelhança significativa com alguém nos registros, o sistema emite um alerta para as autoridades responsáveis. A partir daí, os policiais ou agentes de segurança podem tomar medidas apropriadas, como investigar mais a fundo, abordar o indivíduo suspeito ou efetuar uma verificação mais detalhada de identidade.

As tecnologias de reconhecimento facial são promovidas como eficazes ferramentas de supervisão e vigilância no âmbito da segurança pública, sendo

[14] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital — direitos fundamentais (ainda mais) em perigo", ob. cit., p. 142.

consideradas recursos essenciais para o desenvolvimento das Cidades Inteligentes. Contudo, na prática, essas tecnologias têm um alto custo e demonstram uma falta de efetividade para atingir seus objetivos.

> Diga-se ainda que, do mesmo modo que o plano insiste em estabelecer novos valores como fundamento de sua ordem urbana, seu intuito é também o de eliminar da sociedade brasiliense os valores injustos que os arquitetos associam à estratificação social-espacial capitalista. Neste plano para o desenvolvimento da sociedade, a criação de uma nova cidade e de uma nova sociedade acarreta a destruição da ordem urbana e social anterior. Esta dupla intenção é perceptível nos termos de uma analogia médica com frequência utilizada pelos modernistas europeus, sobretudo Le Corbusier, para justificar seus projetos. Assim como se pode tratar de uma doença suprimindo seus sintomas, também pela negação arquitetônica dos efeitos e dos símbolos da estratificação social o plano procura eliminar, ou pelo menos tornar sem efeito (isto é, "neutralizar" os princípios dessa estratificação, na medida em que possam acabar influenciando as determinações governamentais quanto às benfeitorias públicas c o uso que delas venha a fazer a população. Na utopia do plano piloto, a distribuição desigual de vantagens originadas por diferenças de classes, raça, emprego, riqueza e família teria pequeno papel e pouca eficácia na organização da vida urbana. E como o Estado iria controlar, por meio do plano, a construção de toda a cidade como uma benfeitoria pública, as propostas do plano aparecem como a inversão inescapável de uma evolução social, na qual os arquitetos projetam os traços fundamentais da sociedade.[15]

A falta de transparência inerente a esses modelos matemáticos se torna um ponto central na discussão sobre como equilibrar segurança e privacidade. Isso se torna evidente quando questionamos as decisões automatizadas resultantes das tecnologias de vigilância, já que esbarramos na ausência de clareza em relação às estruturas subjacentes, os parâmetros internos envolvidos e os critérios que orientam as tomadas de decisão. É importante notar, porém, que essas tecnologias são desenvolvidas usando linguagens extremamente complexas e que estão ao alcance de um grupo bastante restrito de programadores.

Nesse contexto, a experiência do uso do reconhecimento facial no Brasil atrai

[15] HOLSTON, James. A Cidade Modernista: uma crítica de Brasília e sua utopia/ James Holston; Tradução Marcelo Coelho.- São Paulo: Companhia das Letras, 1993, p 23.

especial atenção. Isso é especialmente notável quando se discute vigilância pública e, por consequência, as políticas criminais implementadas pelo Estado para alcançar uma maior eficácia. Torna-se impossível abordar esse tema sem explorar as questões de racismo e a seletividade do sistema penal no país. O sistema penal brasileiro, que em grande medida reflete traços arraigados do período de escravidão e carrega um significativo viés racial, concentra sua abordagem na busca por um determinado perfil de criminoso, impactando de maneira desproporcional indivíduos negros em comparação aos brancos.

Diante disso, a adoção de qualquer forma de instrumento ou tecnologia com potencial de contribuir para esse sistema pode resultar, direta ou indiretamente, na perpetuação e amplificação dessas formas de discriminação. Ainda que as novas tecnologias se concentrem nas plataformas digitais e em todo o conjunto tecnológico que sustenta essas inovações, é crucial não perder de vista que aqueles que gerenciam, participam ou se beneficiam dessas ferramentas são seres humanos, inseridos em um contexto histórico e influenciados por suas próprias crenças e preconceitos, tal qual ocorre no mundo real.

No Brasil, a adoção da tecnologia na segurança pública tem se espalhado rapidamente devido a doações e acordos de cooperação técnica estabelecidos com empresas fabricantes. Essas parcerias de fornecimento gratuito evoluem para contratos e processos de licitação que envolvem montantes na casa dos milhões[16]. Como exemplo, no ano de 2021, o estado da Bahia investiu R$ 665 milhões em sistemas de reconhecimento facial. Entretanto, em 2019, apenas 3,6% dos 903 alertas de identificação de suspeitos na Bahia resultaram em mandados de prisão, representando menos de 34 pessoas[17]. Similarmente, no Rio de Janeiro, durante uma operação policial realizada no Estádio do Maracanã em 2019, dos 11 indivíduos detidos com base no uso da tecnologia, 7 foram identificados erroneamente pela máquina, totalizando 63% dos casos[18].

Ao não apresentar dados que confirme se o número de indivíduos procurados

[16] Relatório Vigilância Automatizada: uso de reconhecimento facial pela Administração Pública. Laboratório de Políticas Públicas e Internet: 2021.

[17] Rui costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial — The Intercept Brasil

[18] Nunes, Pablo. Um Rio de olhos seletivos [livro eletrônico]: uso de reconhecimento facial pela polícia fluminense / Pablo Nunes, Mariah Rafaela Silva, Samuel R. de Oliveira. – Rio de Janeiro : CESeC, 2022

e identificados pelo sistema justifica a grande coleta de dados pessoais de multidões que transitam pelas áreas públicas equipadas com câmeras, a ausência de evidências concretas gera dúvidas quanto à relação entre o custo e o benefício de se utilizar esses sistemas.

Entretanto, a implementação de sistemas de reconhecimento facial pode desencadear consequências prejudiciais à privacidade e ao exercício de direitos em ambientes sociais compartilhados. Por exemplo, a presença de câmeras equipadas com essa tecnologia em toda a cidade torna viável rastrear a trajetória de uma pessoa, possibilitando a identificação de detalhes íntimos de sua vida com base na análise dos locais que frequentou durante um período específico. Em razão disso, o indivíduo pode optar por evitar atividades que normalmente realizaria caso não estivesse sob vigilância constante e identificação, mesmo que essas atividades não tenham nenhuma natureza ilegal. A participação em grupos políticos, religiosos ou relacionados à identidade sexual, ou de gênero poderia ser influenciada pelo receio de discriminação, caso essa informação caia nas mãos equivocadas.

Portanto, visto que essa atividade interfere profundamente e de maneira direta no exercício de diversos direitos fundamentais, o uso da tecnologia de reconhecimento facial deve ser precedido por uma autorização legislativa específica. Isso se deve ao fato de que as Secretarias de Segurança Pública dos Estados estão atualmente apoiados na permissão genérica do art. 144 da Constituição Federal[19] para empregar qualquer método viável visando melhorar a segurança pública. Contudo, reconheceu-se a necessidade de uma lei particular que aborde essas peculiaridades, considerando os riscos e impactos negativos associados à tecnologia, incluindo a coleta em grande escala de dados pessoais.

2.3 Capitalismo de datificação

Para discernir padrões, as novas tecnologias, quando aplicadas ao cenário social, quantificam a sociedade, permitindo que algoritmos leiam e interpretem desejos, amizades e expressões pessoais. Nesse contexto de datificação da

[19] CF, Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos.

sociedade, as plataformas de mídia social transformam dados pessoais em uma espécie de nova mercadoria, transformando as conexões estabelecidas no mundo virtual em moedas de troca. Consequentemente, os usuários são responsáveis por fornecer seus dados ao adentrar o ambiente virtual.

> Para um segmento dos analistas do capital é preciso reconhecer que o mercado de dados pessoais será um dos principais ou o principal mercado da economia informacional. Seguindo a lógica neoliberal, não há como enfrentar o mercado sem prejudicar toda a sociedade. Portanto, deveríamos olhar os dados não do ponto de vista do direito, mas sob a ótica do bem ou da mercadoria. As pessoas devem buscar ganhar dinheiro com seus dados pessoais. Impedir e restringir a coleta massiva de dados não será possível diante da força da livre iniciativa agora com um apetite voraz pelas informações sobre tudo que possa gerar lucro. Como utilizaremos cada vez mais dispositivos cibernéticos, mais dados serão gerados sobre quem os utiliza.[20]

Partindo dessa premissa, é possível afirmar que tanto o avanço tecnológico quanto a aplicação de algoritmos no contexto econômico e social possibilitam que ferramentas digitais exerçam influência sobre o indivíduo. No entanto, devido à falta de estabilidade nas correlações resultantes de padrões identificados a partir de conjuntos de dados, surge a preocupação com os riscos à democracia, particularmente no âmbito da justiça criminal, quando o indivíduo se torna parte desse contexto. Um exemplo disso é a discriminação, a vigilância em massa, o auxílio à disseminação de desinformação, o aumento da segregação e a influência sobre o indivíduo. É crucial, portanto, avaliar os perigos contínuos no contexto da justiça na era da datificação da sociedade, mediante a utilização das tecnologias emergentes.

Ao longo do tempo, permitimos que as *Big Techs*, na maioria influenciadas pela mentalidade do Vale do Silício, assumam um papel poderoso em nossas vidas cotidianas. Isso resultou em uma adaptação das pessoas aos formatos que essas empresas impõem. No entanto, um problema surge quando tentamos forçar a conformidade dessas plataformas à cultura e ao contexto específico de cada país

[20] SILVEIRA, Sergio Amadeu da. Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais. São Paulo: Edições Sesc São Paulo, 2017 — p. 38.

em que operam. Para alcançar esse objetivo, não é viável nivelar redes sociais com formatos originalmente não digitais, como o jornalismo.

Essa equiparação entre duas perspectivas distintas diminui a responsabilidade das *Big Techs* no que diz respeito à moderação e responsabilização legal pelos crimes ocorrendo em suas plataformas. Esse argumento é apresentado no artigo “Elites tecnológicas”, de Safyia Noble[21]. A visão predominante no Vale do Silício é a de atribuir causas fundamentais para movimentos sociais a ações individuais, o que acaba por deslocar também a responsabilidade para o âmbito individual. Esse cenário dificulta o uso de ferramentas jurídicas para lidar com tais situações. No contexto brasileiro, por exemplo, a consideração do racismo como crime é uma conquista importante para o movimento negro.

Não é sensato buscar soluções que equiparem práticas e contextos diferentes sob a mesma problemática. Devemos lembrar que essas redes sociais não foram concebidas no Brasil, e apenas algumas delas se preocupam em adaptar suas ferramentas para atender a esse contexto específico. Da mesma forma que critico esse aspecto no Projeto de Lei das *Fake News*, acredito que também seja benéfico promover uma mudança cultural em relação a auditorias e ferramentas proprietárias. Abrir os processos dessas redes permitiria investigar e encontrar os melhores caminhos para ferramentas abertas e mais adequadas à realidade brasileira.

Recentemente, o *Twitter* enfrentou diversos problemas, incluindo relatos de contas recebendo mensagens sobre denúncias efetuadas contra perfis, mesmo quando os usuários não haviam realizado tais denúncias. Teríamos muito a questionar e muitas mudanças a promover se tivéssemos conhecimento sobre como essa “funcionalidade” é concebida e implementada pelas equipes responsáveis.

No âmbito geral, a falta de transparência e os vieses são especialmente evidentes nas discussões mais sociais. Isso nos faz perceber que as limitações humanas também podem ser reproduzidas no ambiente tecnológico. Como seres humanos, possuímos ferramentas mentais e emocionais que nos capacitam a reconhecer as limitações tecnológicas. Devemos basear nosso debate na realidade concreta, ao invés de nos apegarmos a utopias. Certamente, não estamos vivendo

[21] NOBLE, S. ROBERTS, S. T. Elites tecnológicas, meritocracia e mitos pós raciais no Vale do Silício.6 Vol. 22 Nº 1 - janeiro/abril 2020. Revista Fronteiras - estudos midiáticos.

no universo fictício dos Jetsons.

A discriminação se intensifica quando o usuário é categorizado em um grupo específico e julgado com base em características genéricas, resultando na exclusão de algumas nuances individuais do contexto social. O viés algorítmico espelha a inclinação existente na rede social, e o racismo é uma faceta intrínseca à sociedade, não sendo meramente um “defeito” a ser corrigido nas máquinas algorítmicas. O poder de análise crítica do ser humano é reduzido quando ele se submete aos dados, mantendo-se preso a ideais discriminatórios, enquanto se encontra enclausurado em sua própria bolha.

A presença crucial da Inteligência Artificial na vida das pessoas é inegável, uma vez que ela se estabeleceu como uma verdadeira aliada na resolução de casos. Isso se deve à sua capacidade ágil de identificar suspeitos e indivíduos foragidos, bem como de fornecer um enfoque analítico aos dados que nutrem a IA com informações, incluindo imagens e descrições de criminosos, abrangendo até detalhes como a cor da pele. Nesse contexto, é essencial avaliar se a tecnologia de reconhecimento facial é de fato eficaz ou se está sujeita a erros no que diz respeito à precisão na identificação da tonalidade da pele.

> A IA permite, a partir da tecnologia, em considerável medida, alterar a relação entre pessoas, potencializando suas capacidades criativas e habilidades. Tem, assim, uma função disruptiva e está diretamente associada à produtividade de ações e conhecimentos. A IA associa-se à engenhosidade humana, contribuindo com velocidade e precisão, especialmente em tarefas que demandariam muito tempo, repetição de esforços e fidelidade de parâmetros[22].

No decorrer do processo de aprendizado, os algoritmos de *machine learning* buscam identificar elementos que possam estabelecer uma relação entre comportamento preditivo e objetivos nos diversos modelos possíveis.

São esses algoritmos incorporados nas máquinas que desempenham a tarefa de rastreamento até localizar indivíduos envolvidos em atividades criminosas, apresentando-nos, assim, uma identificação por meio do reconhecimento facial. Isso

[22] HARTMANN PEIXOTO, Fabiano; MARTINS DA SILVA, Roberta Zumblick. Inteligência artificial e Direito. v. 1. Curitiba: Alteridade Editora, 2019 - p. 21.

traz à tona considerações cruciais, como a segurança e a preservação da privacidade de informações pessoais. No contexto brasileiro, essa abordagem é uma forma de perícia policial que visa contribuir com investigações e oferecer suporte aos profissionais que atuam na esfera forense.

Uma considerável parcela desses sistemas encontra-se sob o controle de grandes corporações, governos e outras entidades, sem passar por auditorias nos algoritmos e no ciclo de criação, além de carecer de transparência quanto às reais finalidades dessas inovações. Um exemplo recorrente — que suscitou inúmeras interrogações em 2021, no Brasil — é a implementação da TRF na área da segurança pública. Esse episódio revisitou o uso preconceituoso do fenótipo como critério de tomada de decisão em prisões e resultou em numerosas detenções injustas no Brasil, sobretudo de indivíduos negros. Outros empregos do reconhecimento facial também foram objeto de questionamento, mas pouco se conhece sobre o processo de desenvolvimento, coleta e processamento adotado pelas empresas responsáveis por essas tecnologias.

2.4 Como os algoritmos podem perpetuar viés racial

Quando um pesquisador condensa dados para futura apresentação, pode inadvertidamente revelar suas próprias inclinações morais. Informações não sujeitas a um processo de curadoria exigem esse filtro subjetivo para serem usadas, e isso é efetuado com intenções específicas pré-existentes. Optando pela transparência, a manifestação dessa subjetividade nos resultados deve ser examinada e justificada. Assim que o modelo final é concebido, torna-se possível exercer algum grau de controle sobre suas implicações intrínsecas.

> O *deep machine learning*, que usa algoritmos matemáticos para replicar o pensamento humano, se baseia em valores específicos de tipos específicos de pessoas - nomeadamente, as instituições mais poderosas da sociedade e as pessoas que as controlam.[23]

[23] NOBLE, Safiya Umoja. Algorithms of oppression: how search engines reinforce racism. NYU Press, 2018 p. 29.

A aplicação de sistemas de inteligência artificial como apoio à tomada de decisão e para a chamada “análise preditiva” suscita preocupações substanciais relacionadas à falta de responsabilidade, participação da comunidade e auditoria no processo. As técnicas de aprendizado de máquina em redes neurais (simuladas) extrai padrões de conjuntos de dados específicos, seja com ou sem soluções “corretas” previamente fornecidas. Isso ocorre por meio de abordagens supervisionadas, semi-supervisionadas ou não supervisionadas. Através dessas técnicas de “aprendizado”, o sistema identifica padrões nos dados.[24]

Esses padrões são rotulados para parecerem relevantes para as decisões do sistema, embora o programador muitas vezes desconheça quais padrões específicos nos dados foram realmente utilizados. Na realidade, os programas estão em constante evolução. Portanto, quando novos dados são incorporados ou novos feedbacks são fornecidos (“isso estava correto”, “isso estava incorreto”), os padrões empregados pelo sistema de aprendizado se alteram. Quando o resultado não é transparente nem para o usuário, nem para os programadores, ele se torna opaco, conforme observado por Cathy O’Neil[25], se o processo já é opaco para aqueles envolvidos no desenvolvimento, imagine a opacidade para aqueles que não participam do processo de criação.

A mesma autora alega que a tecnologia não pode ser tida como neutra, e que os modelos computacionais (entre eles, os algoritmos de realização de perfis) carregam vieses e opiniões de quem os programou.

Segundo Almeida[26], o racismo possui natureza política, visto que viabiliza a influência e configuração da estrutura social pela discriminação sistêmica, a qual requer influência política para se concretizar. Caso contrário, a discriminação sistemática de comunidades inteiras seria improvável de ocorrer. A esfera política é predominantemente representada por indivíduos do gênero masculino e de etnia branca em diversas instâncias. Essa característica sistêmica assegura que tais indivíduos determinem a hierarquia da sociedade e sua organização. Emerge, portanto, uma estrutura hierárquica em forma de pirâmide, na qual homens brancos

[24] BEUTIN, Lyndsey. Racialization as a Way of Seeing: The Limits of Counter-Surveillance and Police Reform. 2017. Surveillance & Society 15(1): 5-20.
[25] Cathy O'Nei autora do livro: Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça à democracia. 1ª edição. Tradução: Rafael Abraham, Santo André, SP: Ed. Rua do Sabão, 2020.
[26] ALMEIDA, Silvio. Racismo estrutural: Feminismos plurais. São Paulo: Jandaíra, 2019.

ocupam o ápice, seguidos por mulheres brancas, homens negros e mulheres negras na base. Essa disposição reflete um distanciamento considerável em relação aos processos políticos e ao próprio poder. A sub-representação desses indivíduos negros nesses contextos reforça a propagação do racismo estrutural em esferas como a econômica, social e institucional, alimentando um ciclo contínuo do fenômeno.

> No livro The racial contract[27], o pensador afro-americano Charles W. Mills sugere que consideremos a inquestionável supremacia branca ocidental no mundo como um sistema político não identificado, uma vez que ela estrutura uma sociedade organizada racialmente, um Estado racial e um sistema jurídico racial, onde a classificação de brancos e não-brancos é claramente definido pela lei e pelo costume[28]. (CARNEIRO, 2011, p. 86)

Para Davis[29], é essencial considerar a criminalização e a estereotipamento como conceitos cruciais ao aprofundarmos nossa compreensão do racismo na sociedade. De fato, por meio dessa abordagem, torna-se possível examinar como os sistemas de poder tendem a favorecer indivíduos de origem branca em detrimento dos de origem negra em diversos contextos. A posição desses indivíduos dentro desse sistema permanece fixa, limitando-lhes o acesso aos direitos fundamentais para viver com dignidade na sociedade.

> O racismo, do modo como se desenvolveu ao longo da história dos EUA, sempre implicou certo grau de criminalização, de maneira que não é difícil entender como as suposições estereotipadas de que pessoas negras são criminosas persistem até os dias atuais (DAVIS, 2018, p. 45).

Treinada principalmente com base em imagens de indivíduos brancos, a ferramenta de reconhecimento facial internaliza a ideia de que os modelos matemáticos que definem um rosto como humano aderem a limites étnicos baseados em certas características[30]. O viés algorítmico decorre da falta de

---

[27] MILLS, Charles. The Racial Contract. Nova York: Cornell University, 1997.
[28] Carneiro, Sueli. Racismo, sexismo e desigualdade no Brasil / Sueli Carneiro. São Paulo: Selo Negro, 2011 p. 86
[29] DAVIS, Angela. A liberdade é uma constante. Trad. Heci Regina Candiani. 1ª ed. São Paulo: Boitempo, 2018
[30] "[...] boa parte dos bancos de imagens utilizados para treinar esses algoritmos são compostos por

representação de outras etnias em seu ambiente de programação predominantemente branco e masculino. Assim como os humanos são influenciados pelo meio em que vivem, esses computadores refletem o mundo ao qual foram expostos, ignorando imagens que desafiam suas noções preconcebidas.

Por exemplo, conforme indicado pela Rede de Observatórios da Segurança, até novembro de 2019, aproximadamente 90,5% dos indivíduos detidos eram de ascendência negra. Nesse contexto, o Estado da Bahia estava à frente em termos de abordagens e prisões. Isso evidencia o potencial discriminatório no uso desses sistemas, que pode contribuir para a perpetuação de detenções arbitrárias, constrangimentos e violações dos direitos [31] . Essa situação ressalta o aumento da adoção de câmeras de vigilância, sistemas de inteligência artificial e softwares de reconhecimento facial no Brasil, supostamente para auxiliar os Centros de Operações de Inteligência e a Segurança Pública. No entanto, pouco se sabe sobre os resultados dessas implementações.

Um exemplo claro desse cenário foi o substancial investimento feito pelos governos estaduais, como visto no Estado da Bahia, onde cerca de 665 milhões de reais foram alocados. Contudo, apesar das justificativas que se baseiam nas promessas de redução da violência, não foram registrados avanços positivos significativos. Em 2019, apenas 3,6% dos 903 alertas emitidos resultaram em mandados de prisão efetivos[32]. Além dos resultados pouco expressivos, a situação em Salvador, na Bahia, levanta questões fundamentais, como a possibilidade de ampliação do viés seletivo do sistema penal através do uso da tecnologia e a ocorrência de numerosos casos de identificações errôneas nas iniciativas brasileiras. Esses casos reforçam as constatações e denúncias de pesquisadores internacionais sobre questões de racismo, discriminação de gênero e outras problemáticas

---

pessoas brancas". Ver mais em: NUNES, Pablo. O algoritmo e racismo nosso de cada dia: Reconhecimento facial aposta no encarceramento e pune preferencialmente população negra. Piauí, 2 jan. 2021. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-eracismo-nosso-de-cada-dia. Acesso em: 13 ago. 2023.

[31] NUNES, Pablo. EXCLUSIVO: LEVANTAMENTO REVELA QUE 90,5% DOS PRESOS POR MONITORAMENTO FACIAL NO BRASIL SÃO NEGROS. Intercept_Brasil, novembro de 2021. Disponível em: https://www.intercept.com.br/2019/11/21/presos-monitoramento-facial-brasil-negros/. Acesso em: 13 ago. 2023.

[32] FALCÃO, Cíntia. LENTES RACISTAS Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial. Intercecpt_Brasil, 2019 Disponível em: https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/>. Acesso em: 13 ago. 2023.

associadas aos mecanismos preditivos do sistema penal, como o reconhecimento facial.

Dessa forma, embora a correlação efetuada por uma máquina possa aparentar imparcialidade, sugerindo que está apenas revelando informações verídicas e precisas com base em pistas deixadas na internet, esse procedimento é direcionado pelos interesses da empresa detentora do algoritmo. Sob a justificativa de proteção de propriedade intelectual e segredos comerciais, a empresa não oferece transparência em relação ao seu código nem fornece explicações sobre seu funcionamento. Isso resulta na ausência de informações para as pessoas afetadas pelo processamento dos dados, deixando-as sem compreender por que determinado resultado foi alcançado.

2.5 O QUE A LEI BRASILEIRA DIZ SOBRE O USO DE RECONHECIMENTO FACIAL

É importante ter em mente que, na legislação brasileira da Lei Geral de Proteção de Dados Pessoais, o consentimento é apenas uma das bases legais disponíveis para o processamento de dados pessoais sensíveis, incluindo a biometria facial. Em outras palavras, o consentimento é apenas uma das condições que autoriza o tratamento desse tipo de dado pessoal. Em certas circunstâncias, como para o cumprimento de obrigações legais, prevenção de fraudes e garantia da segurança do titular dos dados, o tratamento é dispensado. No entanto, mesmo nessas situações (onde o consentimento não é necessário), é importante observar os princípios delineados no art. 6 da LGPD. Entre eles, destaca-se o princípio da necessidade, que estabelece a restrição do processamento dos dados ao mínimo essencial para alcançar seus objetivos. Isso significa que, nos casos em que for viável atingir a finalidade desejada ou necessária sem processar um dado tão sensível quanto a biometria facial, a opção deve ser não coletar esse tipo de dado. Assim, é necessário avaliar em cada situação a justificativa apresentada pelo responsável pelo processamento desses dados, a fim de determinar se a medida é verdadeiramente necessária e se pode ser implementada junto aos clientes.

Outro aspecto relevante a ser ponderado é que, dado tratar-se de uma informação pessoal sensível, a obtenção do consentimento para a coleta,

armazenamento e utilização da biometria facial deve ocorrer de maneira precisa e destacada, e restrita a finalidades específicas. Isso quer dizer que os utilizadores ou clientes de um determinado serviço ou produto devem ser clara e transparentemente informados sobre as finalidades do uso da tecnologia de reconhecimento facial, e devem dar o seu consentimento de forma específica para o processamento proposto pelo fornecedor do serviço ou produto naquela situação específica.

A LGPD é uma legislação que aborda o processamento de informações pessoais, tanto em formatos físicos como digitais. Conforme o artigo 5º da Lei, os dados biométricos (como a biometria facial) são categorizados como um tipo especial de informação pessoal, chamado de 'informação pessoal sensível'. Portanto, é possível afirmar que, em geral, a LGPD é aplicável quando há utilização de tecnologias de reconhecimento facial.

Contudo, existem situações específicas na qual a LGPD não se aplica. Tais circunstâncias estão definidas no artigo 4º, inciso III, da LGPD, que estabelece que a Lei não abrange o processamento de dados realizados exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e combate a crimes. Por exemplo, o uso de tecnologias de reconhecimento facial por parte das forças policiais não seria regido pela LGPD — embora os princípios gerais de proteção e os direitos dos titulares de dados devam ser sempre respeitados.

Sob a ótica do gerenciamento de informações, a LGPD definiu princípios, proteções, obrigações e prerrogativas dos indivíduos, dos provedores de serviços e do próprio setor público. É notável que a legislação colocou este último sob suas orientações de forma explícita, como evidenciado na cláusula inicial do artigo 23 da lei:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n.º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

De acordo com a explicitação das entidades de direito público mencionadas no parágrafo único do artigo 1º da Lei n.º 12.527/2011 (Lei de Acesso à Informação),

é relevante reproduzir a identificação destas entidades:

> Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Vale a pena mencionar que existe um Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigação Criminal, também conhecido como "LGPD Penal", em tramitação na Câmara dos Deputados. Este Anteprojeto foi elaborado por uma Comissão de Juristas designada pela própria Câmara e aguarda apresentação oficial por parte de um parlamentar para se tornar um Projeto de Lei.

Por fim, é relevante destacar também que a supervisão administrativa será conduzida diretamente pela Administração Pública, seja através de suas entidades policiais, seja por intermédio da Autoridade Nacional de Proteção de Dados (ANPD), com atribuições definidas pelo art. 55-J[33] da LGPD. A ANPD, sendo um órgão

[33] Art. 55-J. Compete à ANPD: (Incluído pela Medida Provisória nº 869, de 2018)
I - zelar pela proteção dos dados pessoais;
II - editar normas e procedimentos sobre a proteção de dados pessoais;
III - deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos;
IV - requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais;
V - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei;
VI - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
VII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;
VIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal;
IX - difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança;
X - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores;
XI - elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
XII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
XIII - realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD;
XIV - realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da

federal vinculado à Presidência da República, terá a responsabilidade de estabelecer regulamentos e supervisionar procedimentos relacionados à salvaguarda de informações pessoais

2.5 As câmeras pelo mundo

Atualmente, é possível afirmar que a maioria dos países incorpora de maneira institucionalizada o sistema de reconhecimento facial em suas operações. Apesar da ausência de estudos conclusivos que comprovem inequivocamente os benefícios dessa tecnologia, observa-se uma disseminação generalizada das câmeras em âmbito global.

A discussão sobre a viabilidade do emprego de tecnologias de reconhecimento facial tem sido objeto de debate em escala internacional. Enquanto alguns países já as implementam de fato, em outros, a possibilidade de utilização continua em fase de testes. Por outro lado, existem nações que apenas teorizam sobre essa questão, sem efetuar experimentos concretos.

Um dos países que enfrentou mais questionamentos em relação ao uso dessas tecnologias é os Estados Unidos da América, onde elas já foram efetivamente empregadas. Entretanto, alguns estados norte-americanos estabeleceram restrições ao seu uso.

A China é um dos países onde a incorporação das tecnologias de reconhecimento facial já integra o dia a dia de seus habitantes. Com um contingente que supera 200 milhões, as câmeras de monitoramento estão distribuídas por todo o território nacional, tendo como propósito monitorar a população e garantir a conformidade com as leis e os padrões sociais. Esse sistema visa prevenir crimes violentos, identificar indivíduos suspeitos, criminosos foragidos e até mesmo detectar estudantes que estejam dormindo nas salas de aula, entre outras circunstâncias[34].

---

administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica;
XV - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e,
XVI - elaborar relatórios de gestão anuais acerca de suas atividades.

[34] LENTINO, Amanda. “This Chinese facial recogniton start-up can identify a person in seconds”. CNBC Disruptor 50, 2019, disponível em

Por sua vez, na Rússia, a utilização da inteligência artificial se destacou ao mapear indivíduos afetados pelo COVID-19 e monitorar o cumprimento das medidas de quarentena, analisando o movimento dos infectados. Em territórios belgas e marroquinos, a tecnologia de reconhecimento facial foi proibida, visto que ambos os países entenderam que sua implementação poderia infringir direitos individuais e representar um risco para a população.

35

O uso do reconhecimento facial urbano varia consideravelmente em diferentes países ao redor do mundo, gerando debates complexos sobre segurança, privacidade e liberdades individuais. Na China, essa tecnologia é amplamente empregada para fins de segurança pública, controle de tráfego e até mesmo monitoramento de comportamento social, suscitando críticas por sua potencial violação da privacidade e práticas de vigilância em massa.

Nos Estados Unidos, a adoção do reconhecimento facial varia conforme

https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-upcan-id-a-person-in-seconds.html consultado em: 1 ago. 2023.

[35] Já na Imagem: https://direitodigitalcast.com/o-mapa-da-tecnologia-de-reconhecimento-facial-no-mundo/

estados e cidades, com algumas implementações para auxiliar agências de aplicação da lei na identificação de suspeitos, enquanto outras regiões estabelecem regulamentações mais rigorosas ou proibições temporárias devido a preocupações éticas e de privacidade.

Na União Europeia, o Regulamento Geral de Proteção de Dados (GDPR) estabelece normas estritas sobre o processamento de dados pessoais, abordando também informações coletadas por meio do reconhecimento facial. Além disso, outros países têm adotado abordagens variadas, com alguns usando essa tecnologia em aeroportos ou pontos de entrada, enquanto outros resistem devido a preocupações éticas e legais[36].

2.7 RESPOSTAS AO RECONHECIMENTO FACIAL

Durante um longo período, a privacidade foi frequentemente negligenciada, mas à medida que a preocupação com a proteção de dados pessoais ganhou destaque por meio de regulamentações internacionais, emergiram iniciativas coordenadas pela sociedade civil. Estas buscam abordar o crescente emprego do reconhecimento facial por ações como a busca por regulamentação apropriada, a imposição de moratórias em sua utilização ou até mesmo a sua completa proibição.

A noção de moratória implica na suspensão temporária do uso do reconhecimento facial em um contexto específico, permitindo aos reguladores tempo para desenvolver estratégias que evitem abusos no emprego dessas tecnologias. Nesse sentido, o Conselho de Direitos Humanos da ONU recomendou, em 2020, que os países estabelecessem uma moratória no uso de tecnologia de reconhecimento facial em eventos de caráter pacífico, até que as autoridades competentes demonstrassem conformidade com os padrões de privacidade e proteção de dados, além da ausência de problemas significativos de precisão e impactos discriminatórios.

O racismo estrutural está profundamente interligado a essa questão em diversos níveis, abrangendo desde o design dos algoritmos, que considera a

[36] Big Brother Watch, “Stop Facial Recognition”, disponível em https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/. Acesso em: 3 ago. 2023

estrutura facial branca como o padrão e qualquer desvio desse padrão é considerado uma exceção. Além disso, o racismo desempenha um papel central na decisão de onde instalar essas câmeras de vigilância. Por exemplo, no Rio de Janeiro, observamos o cercamento inicial de Copacabana através do reconhecimento facial, tendo historicamente servido para restringir o acesso de jovens negros, principalmente aqueles provenientes das periferias da cidade. Além disso, observamos o uso de câmeras em favelas para exercer controle sobre essas populações.

O que também merece destaque é o modo como as forças policiais conduzem abordagens. É importante reconhecer que o reconhecimento facial está diretamente relacionado a abordagens policiais e detenções. É amplamente conhecido que a maioria das pessoas abordadas pela polícia, muitas vezes de forma violenta, são jovens negros. No Rio, por exemplo, 63% das pessoas abordadas pela polícia são negras, e esses encontros frequentemente resultam em situações de violência. O encarceramento também é impactado por essa dinâmica. O Brasil tem uma das maiores populações carcerárias do mundo, com taxas crescentes. No entanto, esse aumento no encarceramento não corresponde a melhorias na segurança pública; pelo contrário, estamos testemunhando a implementação do reconhecimento facial como uma nova estratégia que parece reforçar a aposta no encarceramento como solução para os problemas de segurança pública no país.

De maneira geral, tanto a moratória quanto o banimento estão alinhados com o princípio da precaução. No âmbito da proteção de dados, esse princípio é aplicado em situações em que as finalidades e os usos dos dados pessoais não são claros. De forma abrangente, esse princípio fundamenta-se na ideia de que, diante de incertezas e evidências limitadas, os proponentes devem tomar medidas precautórias para evitar riscos, podendo até mesmo ser necessário proibir atividades potencialmente arriscadas até que seja possível demonstrar que elas não apresentam riscos ou que os riscos envolvidos são aceitáveis.

Um relatório de inteligência ressaltou que sistemas de reconhecimento facial foram empregados para identificar manifestantes que protestavam contra o assassinato de George Floyd. No entanto, em resposta às pressões da sociedade, a cidade de Minneapolis proibiu a utilização desse sistema, e empresas fornecedoras de tecnologia como IBM e Microsoft cessaram a venda desses sistemas para as

forças policiais.

Na Argentina, a campanha ConMiCaraNo, em colaboração com seus parceiros, obteve uma vitória significativa no final de 2022: a Justiça reconheceu a ilegalidade do sistema de reconhecimento facial empregado para identificar pessoas em fuga, ordenando a destruição dos registros já coletados pela polícia.

No Brasil, várias iniciativas estão empenhadas na causa de proibir o uso do reconhecimento facial na segurança pública. A mobilização do movimento Sai da Minha Cara, por exemplo, incentivou parlamentares a apresentarem projetos de lei para proibir o reconhecimento facial em espaços públicos. Enquanto isso, a iniciativa “Sem Câmera na Minha Cara!” tem trabalhado para evitar que a prefeitura do Recife (PE) implemente relógios inteligentes com tecnologia de reconhecimento facial pela cidade.

A Campanha Tire Meu Rosto da Sua Mira defende o banimento dessa tecnologia prejudicial que tem se espalhado rapidamente pelo Brasil. Alcançar um banimento ao nível nacional é um desafio à altura das dimensões do nosso país. Por essa razão, acreditamos na colaboração e na disseminação do debate e das iniciativas de proibição em todas as regiões do Brasil. Embora tenhamos um longo caminho pela frente, reconhecemos ser possível um futuro sem reconhecimento facial na segurança pública.

De outra perspectiva, a compreensão das ações das grandes empresas de tecnologia no âmbito do debate político sobre a regulamentação do reconhecimento facial apresenta desafios éticos e sociais, bem como implicações concretas no campo econômico. Além disso, pesquisas em IA têm impacto em três esferas: governo, academia e indústria. Portanto, organizações com vínculos econômicos fortes têm demonstrado preocupações em relação a aspectos comportamentais e éticos.

No contexto brasileiro, a discussão sobre banimento e moratória continua em estágio inicial. Não há no país um movimento ativo que pleiteie o banimento do uso do reconhecimento facial ou a implementação de uma moratória. Recentemente, ativistas e associações civis brasileiras se uniram a diversas outras organizações internacionais para assinar a Carta Aberta pelo Banimento Global de Tecnologias de Reconhecimento Facial e outras formas remotas de reconhecimento biométrico que permitam vigilância em massa, com preconceito e tendenciosa. A iniciativa

#TIREMEUROSTODASUAMIRA é uma mobilização da sociedade civil pelo banimento total do uso das tecnologias digitais de reconhecimento facial na segurança pública no Brasil.

3. APLICAÇÃO NO ÂMBITO CRIMINAL

O uso do reconhecimento facial na segurança pública no contexto do sistema processual penal brasileiro demanda uma análise cuidadosa. É essencial que qualquer implementação dessa tecnologia respeite estritamente os princípios legais estabelecidos pela Constituição Federal e pela legislação vigente, como o Código de Processo Penal e a Lei de Interceptação Telefônica, garantindo que as ações das autoridades estejam nos limites legais.

Além disso, a coleta e o processamento de dados biométricos no reconhecimento facial estão sujeitos à Lei Geral de Proteção de Dados (LGPD). Essa lei estabelece regras rígidas para o tratamento de dados pessoais, incluindo a necessidade de consentimento do titular dos dados. Portanto, o uso dessa tecnologia deve obedecer estritamente às disposições da LGPD, considerando a sensibilidade dos dados envolvidos.

A precisão do reconhecimento facial é outro fator preocupante, que pode levar a falsos positivos e falsos negativos, e o potencial viés dessa tecnologia em relação a grupos raciais específicos. No contexto brasileiro, essa questão assume ainda mais importância dada a diversidade étnica do país.

3.1 TRATAMENTO DE DADOS E INVESTIGAÇÃO CRIMINAL

Apesar da exclusão expressa feita pela LGPD de sua aplicação aos dados tratados para fins exclusivos de segurança pública, a questão demanda uma análise cuidadosa de situações envolvendo dados já processados por órgãos de investigação, relativos a titulares que igualmente necessitam da proteção do direito fundamental para salvaguardar essas informações.

Isso ocorre porque a transformação digital da sociedade desencadeou uma

indústria de dados que permeia várias áreas para aprimorar a eficácia e a eficiência[37]. Essa circunstância alcançou o âmbito do Direito Penal, já que o sistema de justiça criminal expandiu-se em proporção à ampla digitalização das informações.

O conceito de *Big Data* pode ser compreendido a partir de três aspectos principais: volume, variedade e velocidade. Em outras palavras, refere-se a conjuntos enormes de dados provenientes de diversas fontes e com uma velocidade de circulação tão rápida que torna inviável sua gestão apenas por seres humanos, sendo necessários algoritmos para esse fim [38]. Dentre as várias aplicações possíveis dessa tecnologia, talvez os campos mais debatidos sejam o da Segurança Pública e o do sistema de Justiça Criminal.

> O *big data* é, acima de tudo, o componente fundamental de uma nova lógica de acumulação, profundamente intencional e com importantes consequências, que chamo de capitalismo de vigilância. Essa nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado. O capitalismo de vigilância se formou gradualmente durante a última década, incorporando novas políticas e relações sociais que ainda não haviam sido bem delineadas ou teorizadas. Mesmo que o *big data* possa ser configurado para outros usos, estes não apagam suas origens em um projeto de extração fundado na indiferença formal em relação às populações que conformam tanto sua fonte de dados quanto seus alvos finais [39].

No contexto da investigação criminal, é evidente a tendência dos órgãos de investigação de realizar análises de *Big Data* como ponto de partida para iniciar investigações. Nesse sentido, ocorre uma busca ativa e abrangente por palavras-chave específicas, como, por exemplo, a palavra “arma” em uma plataforma de mídia social, é o que aponta pesquisa que analisou os verbos usados nas sentenças e nas denúncias para descrever os supostos atos criminosos em

---

[37] Eficácia se trata de fazer a coisa certa (alcançar objetivos) x eficiência trata-se de fazer a coisa da maneira certa (otimizar recursos).

[38] FUCHS, C., & CHANDLER, D. (2019). Introduction Big Data Capitalism - Politics, Activism, and Theory. In: Chandler, D., & Fuchs, C. (eds.), Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour

[39] ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilizaçãode informação. In: BRUNO, Fernanda [et al.] (Org). Tecnopolíticas da vigilância: perspectivas da margem. São Paulo, Boitempo. 2018, p. 18.

julgamento[40]. Isso representa uma inversão na lógica tradicional do processo penal, em que se parte de um grande volume de dados para identificar indícios de atividade criminosa[41]. No entanto, uma preocupação surge pelo fato de que essa abordagem carece de regulamentação específica no arcabouço jurídico.

Trata-se de vigilância, empregada como ferramenta de investigação para obter a identificação de possíveis adversários ou terroristas, por meio da vigilância constante de toda a população e da coleta indiscriminada e contínua de dados dos usuários de internet. Contudo, essas tecnologias também expõem a população ao risco de abusos por parte das autoridades. Conforme argumentado por Schneier[42], ao possuir uma quantidade suficiente de dados sobre qualquer indivíduo, independentemente de quem seja, é possível incriminá-lo por algum crime, o que significa que qualquer pessoa arrisca ser condenada por violar as leis, caso alguma autoridade opte por mirá-la.

Nesse contexto, essa forma de implementar a vigilância pode ser interpretada de várias perspectivas. Alguns autores sustentam ser uma forma de vigilância inovadora, enquanto outros a consideram um fenômeno de vigilância essencialmente tecnológica. Há também aqueles que afirmam que ela é uma vigilância adaptável, voltada para enfrentar ameaças externas. Por fim, surgem pensadores que argumentam que se trata simplesmente de um produto da era moderna, com todas as suas transformações[43].

Em sua essência, a vigilância surgiu inicialmente como um meio de fortalecer o poder do Estado e, hoje, desempenha um papel central no controle social[44]. Como resultado, o *Big Data* amplifica certas tendências de vigilância ligadas à tecnologia da informação e às redes, e está envolvido em configurações novas, mas flexíveis. Isso pode ser compreendido de três maneiras: i) as capacidades do *Big Data*,

[40] CAETANO, Guilherme. Estudo analisa 5 mil processos por tráfico de drogas e mostra que negros são alvo de prisões com baixo número de provas. O Globo, 2023. Disponível em: <https://oglobo.globo.com/brasil/noticia/2023/07/18/estudo-analisa-5-mil-processos-por-trafico-de-drogas-e-mostra-que-negros-sao-alvo-de-prisoes-com-baixo-numero-de-provas.ghtml>. Acesso em: 19 ago. 2023.

[41] CONGRESSO INTERNACIONAL DE DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL, 3, 2020. São Paulo. Disponível em <https://www.youtube.com/watch?v=idQSRq6BaYk&ab_channel=InternetLab>. Acesso em 5 jul. 2023.

[42] SCHNEIER, Bruce. Data and Goliath: the hidden battles to collect your data and control your world. New York. W. W. Norton, 2015. p. 108.

[43] LYON, D. Globalizing surveillance: Comparative and sociological perspectives. Internacional Sociology, 2004, p. 135-149

[44] WILLIAMS, R., & JOHNSON, P. 'Wonderment and dread': Representantios of DNA in ethical disputes about forensic DNA databases. New Genetics and Society, 2004, p. 205-223

incluindo metadados, intensificam a vigilância, expandindo conjuntos de dados interconectados e ferramentas analíticas. A dinâmica de influência existente, a gestão de riscos e o controle ganham velocidade e abrangência por meio de novas técnicas, especialmente análises preditivas, gerando uma avaliação precisa da ameaça criminal através dessa previsão de riscos; ii) o *Big Data* promove uma mudança qualitativa nas práticas de vigilância, resultando em consequências visíveis; e iii) a consideração ética se torna mais urgente como uma forma de crítica[45].

3.2 ADMISSIBILIDADE DA PROVA NO PROCESSO PENAL

A preocupação com os erros judiciários resultou, como um de seus principais efeitos, na criação da presunção de inocência, ou seja, em uma "opção garantista de civilidade[46]". A possibilidade de erros judiciários é inerente ao julgamento, um ato judicial a ser realizado diante da dúvida que se apresenta ao julgador: inocente ou culpado? Por isso, alguns afirmam a inevitabilidade de erros, frequentemente parecendo ignorar a possibilidade democrática de seleção baseada em preferências[47].

Indubitavelmente, o processo penal tem como objetivos primordiais a realização da justiça e a busca pela verdade substancial, assegurando a salvaguarda dos direitos fundamentais dos indivíduos perante o Estado e, adicionalmente, a restauração da estabilidade jurídica. Entretanto, por vezes, a conciliação desses objetivos se torna inatingível. Isso se torna evidente em situações como o reconhecimento facial, onde podemos estar diante de um conflito entre a busca pela verdade material e a garantia dos direitos fundamentais, uma questão particularmente delicada.

A narrativa é moldada por aqueles que conseguem vencer e controlar o discurso. A eliminação das influências relacionadas à raça é uma característica

---

[45] LYON, David. Vigilância líquida: diálogos com David Lyon. Zahar, 2014. p. 5 a 17.

[46] AMARAL, Augusto Jobim do. O dispositivo inquisitivo: entre a ostentação penal e a estética política do processo penal. 2014. 499 f. Tese (Doutorado em Ciências Criminais). Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2014, p. 336

[47] RODRIGUES, Anabela Miranda, "A Inteligência Artificial no Direito Penal …", ob. cit., pp.11-13

constante nos processos históricos do Ocidente, seja ao tentar enfraquecer a identidade racial de figuras históricas negras ou ao apagar a dimensão racial de certos eventos.

> Na historiografia tradicional do constitucionalismo, as revoluções burguesas foram decisivas para a criação de estados nacionais. De igual modo, as guerras de independência nacional são o ponto de partida do constitucionalismo na América Latina. A mediação entre o constitucionalismo europeu, estadunidense e latino americano teria sido efetuada por elites locais com a leitura dos iluministas. Tudo se passa como se as mentes pensantes agissem sobre uma realidade "bruta", moldando, com sua capacidade e inteligência, um novo mundo que nasce com fronteiras jurídicas bem constituídas. Entretanto, o colonialismo e a luta anticolonial foram formados por inúmeros espaços e fluxos hoje esquecidos que transbordam a imagem do mapa e das alegorias presentes na ideia de "recepção teórica" e de "protagonismo das elites".[48]

A emergência de novas tecnologias exerce, efetivamente, um fascínio sobre o âmbito do processo penal. No entanto, dado os conflitos inerentes às finalidades desse processo, é imperativo buscar uma harmonização prática entre elas, enquanto se preserva a efetividade dos interesses em jogo. Quando se aborda a temática do reconhecimento facial, nos deparamos com um embate entre duas das metas do processo penal: por um lado, a busca pela verdade material e, por outro, a proteção dos direitos fundamentais dos cidadãos perante o Estado. Nota-se que esses mecanismos primordialmente almejam alcançar a verdade, a realidade dos fatos, ou seja, fornecer evidência.

> O mesmo se deu nos processos de unificação nacional nos Estados Unidos e na África do Sul. A unidade nacional foi construída com o racismo e não apesar dele. Nos Estados Unidos, a unidade nacional ocorreu tendo a segregação racial como condição de convivência pacífica entre os estados do Sul e do Norte depois da guerra civil e do período da Reconstrução. A Reconstrução dos Estados Unidos pós-guerra civil foi feita sobre o sistema de leis segregacionistas conhecido como Jim Crow. Já na África do Sul, a unidade contraditória que caracteriza toda a nação também valeu-se da incorporação e institucionalização da segregação racial contra a maioria

[48] QUEIROZ, M. V. L. Constitucionalismo brasileiro e o Atlântico negro: a experiência constituinte de 1823 diante da Revolução Haitiana. Rio de Janeiro: Lumen Juris, 2017, p. 10-42.

> negra da população e um regime jurídico conhecido como apartheid, uma mistura macabra de práticas colonialistas-escravistas com nazismo, que vigorou até os anos 1990.[49]

A abordagem academicamente neutra se estende sobre a estrutura normativa do Brasil. Parece haver a presunção de valores morais intrínsecos que se formam automaticamente no subconsciente da sociedade. Sempre que medidas legais de proteção são direcionadas a grupos vulneráveis, surgem vozes que afirmam que tais resultados foram alcançados devido a influências ideológicas. Que cada indivíduo é ideologicamente influenciado para formar opiniões, a partir de sua própria compreensão do mundo e seus interesses, muitas vezes é ignorado. Nesse contexto, a noção de neutralidade parece ser mais uma ilusão do que realidade, possivelmente ocultando as motivações ideológicas subjacentes a cada decisão no âmbito público.

Ao examinar os debates que moldaram a Constituinte de 1823, Marcos Queiroz destaca que o elemento “raça” desempenhou um papel significativo em todo o processo. Isso não é surpreendente, considerando que a Assembleia foi convocada por D. Pedro I quando ainda era Príncipe Regente em 1821, e que transcorreram 67 anos até a promulgação da Lei Áurea em 1888. Essa perspectiva também é enfatizada por Sílvio Almeida.

Estabelecer a fundamentação de provas criminais exclusivamente a partir de registros fotográficos ou em vídeo capturados por sistemas de reconhecimento facial revela-se inadequado, dado que a tecnologia de reconhecimento facial tem evidenciado sua suscetibilidade a erros que podem resultar na condenação injusta de um indivíduo a uma pena severa.

É evidente que a aplicação indiscriminada dessa tecnologia infringe uma série de direitos individuais à privacidade. Muitas pessoas se encontram atualmente detidas injustamente, com o reconhecimento facial servindo como único meio de evidência para embasar suas condenações penais. Contudo, tal reconhecimento é prejudicado por viés racial em sua configuração, e isso perigosamente leva à incriminação de pessoas inocentes.

É de suma importância ressaltar que o uso do reconhecimento facial no

[49] ALMEIDA, Silvio. Racismo estrutural: Feminismos plurais. São Paulo: Jandaíra, 2019, p. 66-67.

contexto brasileiro visa auxiliar o sistema judiciário no processo de penalização, atuando como um elemento de prova legal. No entanto, as provas devem ser parte de um procedimento justo e democrático. Ao final, uma decisão sólida deve ser baseada em elementos de prova objetivos e legalmente previstos nos autos, e não influenciada por opiniões ou ideologias preconceituosas de terceiros, com o potencial de causar prejuízos e injustiças.

Quando um juiz considera a validade da prova digital como meio de convencimento probatório, é crucial que se atenha à análise jurídica dos fatos e garanta uma compreensão precisa sobre a ocorrência ou não do fato, bem como todas as circunstâncias envolvidas. A prova, em sua essência, é o instrumento que embasa a convicção do julgador em relação a um fato específico[50].

Portanto, recorrer a métodos de convicção, como a prova pericial, serve como uma ferramenta de exame minucioso que contribui para uma aplicação justa da lei, eliminando a margem de erro na identificação do verdadeiro infrator e, ao mesmo tempo, evitando a introdução de viés inconsciente, que se baseia em estereótipos presentes nas percepções individuais. Tais estereótipos podem prejudicar decisões de grande importância. Considerando que podem levar à discriminação, é crucial que se implementem medidas robustas para prevenir e responsabilizar os culpados.

Contudo, é essencial ponderar sobre sua admissibilidade, reforçando a ideia de que a evidência também desempenha um papel crucial na garantia de um processo imparcial, onde a verdade não pode ser obtida por meios ilícitos. Assim como salientado por Amelung, o Estado não pode recorrer a práticas criminosas, pois isso acarretaria numa contradição que poderia minar a legitimidade da pena imposta[51]. Ou seja, “o sistema não pode resolver seus problemas às custas da violação do valor intrínseco da pessoa”[52].

Quando se trata do reconhecimento facial, o propósito desta tecnologia é prestar assistência na identificação de indivíduos. O resultado probabilístico fornecido por este sistema auxiliará as autoridades competentes no avanço das investigações. Nesse sentido, acredita-se que esteja em pauta um meio de obtenção

---

[50] THAMAY, R.; TAMER, M. Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020, p.157-158.
[51] AMELUNG, “Informationsbeherrschungsrechte”, p. 22 junto de ANDRADE, Manuel da Costa, “Sobre as proibições de prova em processo penal”, Gestlegal, 2ª edição, março 2022, p.17.
[52] AMELUNG, Rechtsgüterschutz, p.385 junto de ANDRADE, Manuel da Costa, “Sobre as proibições de prova em processo penal”, ob. cit., p. 124

de evidência, pois por si só, tal tecnologia não será suficiente para convencer as autoridades judiciais nem para fundamentar decisões legais.

Devido à importância de se obter uma compreensão mais aprofundada das tecnologias de reconhecimento facial, é essencial haver a participação de um especialista. Este perito, graças aos seus conhecimentos técnicos e científicos, estará capacitado a avaliar o material probatório coletado e, assim, fornecer uma avaliação fundamentada. Portanto, é crucial que o resultado obtido seja devidamente explicado.

Para que seu uso seja considerado aceitável, é essencial cumprir certos requisitos. Estes requisitos incluem a "ausência de uma proibição normativa explícita" e a "falta de um meio probatório especificamente tipificado para alcançar o mesmo resultado de conhecimento." É importante não confundir a liberdade de apresentação de provas com uma total intercambialidade dos meios de prova. Além disso, é crucial observar que existem meios de prova proibidos exatamente porque não estão previstos na legislação.

No cenário atual, a tecnologia mais uma vez emerge como uma possível solução para os desafios do sistema penal. Isso se aplica não apenas no que diz respeito às testemunhas, mas também aos meios de prova de maneira mais abrangente.

Portanto, a decisão de adotar dispositivos tecnológicos para a realização de identificação facial é motivada por diversos fatores. Um desses fatores é a ocorrência frequente de casos de identificação equivocada de suspeitos por parte de testemunhas, erro que persiste como um dos principais equívocos judiciais há décadas. A princípio, essa abordagem pode parecer crucial e apropriada. Contudo, essa percepção se desfaz facilmente.

Considerando as recentes decisões do Superior Tribunal de Justiça relativas ao reconhecimento pessoal, é necessário reconhecer que, por um lado, as disposições do art. 226[53] do Código de Processo Penal (que incluem a descrição do

[53] Quando houver necessidade de fazer-se o reconhecimento de pessoa, proceder-se-á pela seguinte forma:
I - a pessoa que tiver de fazer o reconhecimento será convidada a descrever a pessoa que deva ser reconhecida;
Il - a pessoa, cujo reconhecimento se pretender, será colocada, se possível, ao lado de outras que com ela tiverem qualquer semelhança, convidando-se quem tiver de fazer o reconhecimento a apontá-la;
III - se houver razão para recear que a pessoa chamada para o reconhecimento, por efeito de intimidação ou outra influência, não diga a verdade em face da pessoa que deve ser reconhecida, a autoridade providenciará para que esta não veja aquela;

suspeito pela testemunha/vítima, a formação de uma linha de identificação com pessoas de características físicas semelhantes, medidas para proteger a testemunha/vítima de ameaças e a elaboração de um registro detalhado de identificação) não podem ser executadas por meio de inteligência artificial. Por outro lado, os algoritmos só podem operar com base em fotos e vídeos (sejam imagens individuais ou agrupadas), resultando em um reconhecimento fotográfico inválido em todas as circunstâncias.

As evidências obtidas durante a investigação acompanham o desenrolar do processo penal, servindo para embasar medidas cautelares e determinar a admissibilidade do caso, porém, não podem constituir a base de uma possível condenação. É necessário reunir evidências na fase processual para fundamentar os acontecimentos e orientar futuras decisões.

Como afirmado por Lopes Junior, “O inquérito seleciona e disponibiliza as fontes de informação relevantes. Sua função reside em indicar quem deve ser ouvido, e não necessariamente o que foi afirmado. O testemunho válido é aquele apresentado em juízo, não o contido no inquérito.”[54] A etapa investigativa é reconhecida como um componente crucial no trajeto do processo penal, delimitando temporariamente sua função. Dada a ausência de uma disposição legal que estabeleça uma presunção de veracidade do inquérito policial e de seus elementos, prevalece amplamente na doutrina e jurisprudência o entendimento de que os atos do inquérito são válidos até que se prove o oposto. Isso resulta na admissão no processo de ações realizadas sem a oportunidade de contraditório e ampla defesa.

3.3 PREDPOL

Devido à persistência de padrões discriminatórios enraizados no colonialismo, os corpos de indivíduos negros são frequentemente culpabilizados por comportamentos que lhes são impostos, especialmente em um contexto de justiça automatizada. Nesse sentido, o uso de *Big Data* na esfera criminal, ao mesmo

IV - do ato de reconhecimento lavrar-se-á auto pormenorizado, subscrito pela autoridade, pela pessoa chamada para proceder ao reconhecimento e por duas testemunhas presenciais.
Parágrafo único. O disposto no no III deste artigo não terá aplicação na fase da aplicação na fase da instrução criminal ou em plenário de julgamento (BRASIL, 1941).

[54] LOPES JUNIOR, Aury. Direito Processual Penal. 14 ed. São Paulo: Saraiva, 2017, p. 185.

tempo que gera uma falsa sensação de segurança, também pode infringir as salvaguardas humanas estabelecidas constitucionalmente[55]). Como resultado desse cenário e considerando a herança cultural carregada de preconceitos raciais, surgem diversas críticas ao sistema de justiça criminal. Esse sistema é percebido como um instrumento de controle social fundamentado em um regime opressivo, contribuindo para a sociedade adotar um temor irracional em relação a indivíduos negros.

O desafio surge quando as novas tecnologias são adotadas como meio de estabelecer um sistema eficaz e de reduzir a criminalidade, uma vez que os algoritmos muitas vezes reproduzem e perpetuam os comportamentos racistas humanos. O uso do Policiamento Preditivo, também conhecido como "*PredPol*"[56]), se destaca como um exemplo do agravamento do racismo algorítmico. Isso ocorre porque, na busca por mitigar riscos e resolver crimes, a inteligência artificial no sistema *PredPol* é empregada para identificar locais com maior probabilidade de ocorrência de crimes e até mesmo analisar pessoas que venham a se tornar vítimas no futuro[57]. Ao final, o policiamento preditivo tecnológico gera classificações baseadas nos níveis de risco associados aos locais.

Entretanto, esse software alimenta um ciclo prejudicial de retroalimentação, tornando crucial avaliar as áreas onde mais dados são gerados e, por consequência, onde a presença policial é mais intensa. Esse fenômeno ocorre porque a maioria das condenações envolve indivíduos que provêm de bairros empobrecidos e pertencem às comunidades negra ou hispânica. Assim, mesmo que o modelo em si não focalize diretamente na pessoa, o resultado prático acaba por fazê-lo[58] . Portanto, ao ser orientada por previsões e não apenas por fatos, a justiça criminal preditiva acaba por carecer de informações consistentes.

Além do *PredPol*, outro software em uso nos Estados Unidos da América para

---

[55] HANNAH-MOFFAT, K. (2019). Algorithmic risk governance: Big Data analytics, race and information activism in criminal justice debates. Theoretical Criminology, 2019, p. 453–470.
[56] derivado do termo em inglês "Predictive Policing"
[57] PERRY, Walter L.; McINNIS, Brian; PRICE, Carter C.; SMITH, Susan; HOLLYWOOD, John S. Predictive Policing: Forecasting Crime for Law Enforcement. Santa Monica, CA: RAND Corporation, 2013. Disponível em: <https://www.rand.org/pubs/research_briefs/RB9735.html>. Acesso em 12 de agosto de 2023.
[58] O'NEIL, Cathy. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça à democracia. 1ª edição. Tradução: Rafael Abraham, Santo André, SP: Ed. Rua do Sabão, 2020. p. 23.

avaliar o risco de réus é o COMPASS [59]. Este modelo, desenvolvido por Tim Brennan, calcula a probabilidade de reincidência do acusado com base principalmente em seu histórico. Ao combinar fatores como nível educacional, idade e antecedentes do réu, o algoritmo avalia o risco associado a um indivíduo específico. Contudo, apesar da divulgação dos critérios utilizados, a operação interna dessa nova tecnologia permanece desconhecida. Isso, por sua vez, impede a certificação da eficácia dos resultados. De fato, inúmeras pesquisas apontam que o COMPASS trata de maneira diferenciada os réus negros, levando a taxas desproporcionalmente altas de previsão de reincidência[60], colocando em risco a liberdade desses indivíduos.

Nesse cenário, é importante salientar que, quando um juiz se baseia em um resultado falso-positivo para determinar a prisão de um acusado, os princípios de contraditório, ampla defesa e busca pela verdade factual são deixados de lado, levando a uma relativização desses princípios fundamentais e ameaça a democracia.

Nesse contexto, a presença arraigada do racismo é confirmada ao analisar os softwares empregados no sistema de justiça criminal. Segundo o *American Civil Liberties Union*, é evidente a desproporcionalidade na categorização de corpos negros como de alto risco, mesmo que não tenham reincidido. Isso ressalta a inviabilidade de condenar alguém, tratando-o como criminoso, unicamente com base em avaliações automáticas. A tecnologia de reconhecimento facial também contribui para a perpetuação de padrões discriminatórios. Em inúmeras ocasiões, fica claro que a máquina não reconhece o corpo negro como parte integrante da sociedade.

Um exemplo impactante é o caso amplamente divulgado da cientista Joy Buolamwini[61], que só conseguia ter seu rosto reconhecido pela máquina quando usava uma máscara branca. A partir desse incidente, pesquisadores do MIT e de Stanford conduziram análises de programas desenvolvidos por grandes corporações e identificaram preconceitos de gênero e raça nas novas tecnologias. Além disso, o estudo questiona o funcionamento das plataformas de mídia social e explora como as novas tecnologias aprendem a realizar tarefas com base em padrões extraídos

[59] Correctional Offender Management Profiling for Alternative Sanctions
[60] SUMPTER, David. Dominados pelos números do Facebokk e Google às fake news: os algoritmos que controlam nossa vida. Rio de Janeiro: Bertrand Brasil, 2019, p. 87.
[61] Pesquisadora do MIT acompanhada no documentário Coded Bias.

dos bancos de dados.

3.4 EXEMPLOS BRASILEIROS

No Brasil, o estado da Bahia implementou o uso do reconhecimento facial para fins de segurança pública em dezembro de 2018[62]. Em setembro de 2020, as autoridades baianas anunciaram que essa ferramenta havia contribuído para a detenção de 194 indivíduos procurados. Entretanto, o sistema enfrentou situações de resultados incorretos, gerando casos de falsos positivos. Há um pouco mais de um ano, um jovem teve uma arma apontada para sua cabeça após ser erroneamente confundido com um suspeito procurado por roubo.

Ocorrências similares também foram registradas no Rio de Janeiro, onde a tecnologia de reconhecimento em tempo real foi testada a partir de 2018. Um desses incidentes ocorreu em Copacabana, quando uma mulher foi levada à delegacia por engano, sendo incorretamente identificada como uma pessoa condenada por homicídio[63]. A verdadeira culpada pelo crime já estava sob custódia.

No Ceará, desde 2019, policiais têm à disposição um aplicativo que possibilita a busca por meio do reconhecimento facial de indivíduos sem identificação durante abordagens[64]. Além disso, sistemas de reconhecimento facial também foram adotados por alguns governos municipais, tais como Vitória, João Pessoa, São José dos Campos (SP), Guarujá (SP), Mesquita (RJ), Blumenau (SC) e Pilar (AL).

O estado de São Paulo está em processo de preparação para adquirir mais de 20 mil novas câmeras, que serão integradas ao sistema denominado Smart

---

[62] “Os novos gastos do governo baiano em tecnologia para segurança pública superam R$ 900 milhões, o que é propagandeado como o “maior investimento da história em segurança pública na Bahia”. LENTES RACISTAS Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial. Intercecpt_Brasil, 2019 Disponível em: https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/>. Acesso em: 13 de agosto de 2023.

[63] Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. G1, 2019. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 13 de agosto de 2023.

[64] Policiais poderão fazer reconhecimento facial de suspeitos nas ruas usando câmera do celular. OPovo, 2019. Disponível em: <https://www.opovo.com.br/noticias/fortaleza/2019/10/10/policiais-poderao-fazer-reconhecimento-facial-de-suspeitos-nas-ruas-usando-camera-do-celular.html> Acesso em: 13 de agosto de 2023.

Sampa. O objetivo desse sistema é aprimorar a segurança na cidade, com um custo anual de 70 milhões de reais[65].

Na versão inicial do edital de licitação do projeto, lançada no final de 2022, o sistema a ser contratado deveria conseguir identificar indivíduos suspeitos com base em características como cor, aparência facial, vestimentas, atributos físicos, entre outras, incluindo a detecção de comportamentos suspeitos, como permanecer em um local por um período prolongado, o que poderia indicar atividades suspeitas.

Em colaboração com diversos setores da sociedade civil e do poder público, a Campanha Tire Meu Rosto da Sua Mira[66] se uniu para conter o avanço do edital. Juntos, conseguiram contestar a primeira versão do edital do Smart Sampa. Contudo, o edital será relançado em breve, e a possibilidade de implantar um robusto sistema de vigilância na maior cidade do país torna-se cada vez provável.

Mesmo ao realizar uma avaliação adequada dos riscos associados à utilização de tecnologias de vigilância por parte do setor público, ainda é necessário que as instituições governamentais assegurem uma prestação de contas adequada aos detentores dos dados, informando como essas tecnologias vêm sendo aplicadas. Essa prestação de contas é principalmente evidenciada através da garantia dos direitos dos titulares dos dados, assim como pela transparência nas ações dos responsáveis pelo processamento.

O princípio do livre acesso, conforme estipulado pela LGPD, tem como intuito garantir aos titulares a capacidade de consultar de maneira fácil e gratuita os detalhes relativos ao processo e à duração do tratamento de seus dados pessoais, bem como ter acesso completo a esses dados. A qualidade dos dados, por sua vez, é assegurada para preservar a precisão e atualização dos dados, garantindo que sejam congruentes com a finalidade do tratamento. Além disso, o princípio da transparência assegura que os titulares recebam informações claras, precisas e de fácil acesso sobre o tratamento de seus dados, bem como a identificação dos agentes responsáveis por tal tratamento.

---

[65] Prefeito assina contrato para o início do Smart Sampa, maior programa de videomonitoramento da cidade com até 40 mil câmeras. Secretaria Especial de Comunicação da Prefeitura de São Paulo, 2023. Disponível em: <https://www.capital.sp.gov.br/noticia/prefeito-assina-contrato-para-o-inicio-do-smart-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras-2> Acesso em: 14 de agosto de 2023.

[66] Mobilização da sociedade civil pelo banimento total do uso das tecnologias digitais de Reconhecimento Facial na Segurança Pública no Brasil

Além desses princípios, a LGPD também concede aos titulares direitos específicos para solidificar a proteção de seus dados, delineados nos artigos 17 a 22 da legislação.

No entanto, a consulta indica que a adoção não ponderada de tecnologias de vigilância por parte da Administração Pública é evidenciada pela falta de prestação de contas no que diz respeito à utilização desses sistemas. Isso abrange a ausência de compilação de dados estatísticos consolidados relacionados às atividades de tratamento de dados pessoais.

Entre as autoridades investigadas, são poucas as que fornecem canais que facilitem as solicitações de acesso ou correção dos dados em tratamento. E mesmo quando tais canais são disponibilizados, muitas vezes não se mostram suficientemente acessíveis aos titulares dos dados.

A título de exemplo, durante o carnaval de Salvador em 2020, onde uma multidão de 11,7 milhões de pessoas, incluindo adultos e crianças, estava presente, o uso das mais de 80 câmeras equipadas com tecnologia de Radiofrequência (RF) contribuiu para a identificação e captura de 42 indivíduos foragidos. Desses casos, 13 estavam envolvidos com tráfico de drogas, 14 eram procurados por roubo, 3 por furto, 2 relacionados a homicídios, entre outros[67].

No Rio de Janeiro, durante a Copa América de 2019, a Polícia Militar afirmou que a utilização da tecnologia de Radiofrequência nas proximidades do Estádio do Maracanã possibilitou a execução de mais de 63 mandados de prisão. Entretanto, a notícia destacou também dois casos de resultados incorretos. No primeiro caso, uma pessoa suspeita foi erroneamente confundida com um indivíduo que já estava sob custódia por um crime. No segundo caso, um homem foi detido por alguns dias antes de o erro ser identificado.

Num primeiro olhar, a detenção de 42 foragidos através do uso da tecnologia no Carnaval de Salvador parece ser um sucesso. Porém, quando se considera que isso foi alcançado por meio da coleta de informações de uma multidão de 11,7 milhões de pessoas — correspondendo a mais de 278.000 vezes o número de detidos —, surgem questionamentos sobre se os benefícios proporcionados pela

[67] Reconhecimento facial ajuda a capturar 42 foragidos no Carnaval de Salvador. CanalTech, 2020. Disponível em: <https://canaltech.com.br/seguranca/reconhecimento-facial-ajuda-a-capturar-42-foragidos-no-carnaval-de-salvador-161020/> Acesso em 14 ago. 2023.

tecnologia realmente superam os riscos que ela impõe à privacidade das multidões submetidas à vigilância estatal em larga escala[68].

Essa prestação de contas poderia ser concretizada através da garantia da execução dos direitos dos titulares, permitindo que eles solicitem as informações diretamente ao controlador, ou através da divulgação de dados estatísticos pelas próprias autoridades em seus sites institucionais.

Importante ressaltar que a disponibilização desses dados é crucial para a validação do próprio processo de tratamento. Isso ocorre porque, considerando que o principal argumento para a utilização das tecnologias analisadas reside na alegada melhoria da eficiência alcançada pelo emprego do videomonitoramento e do reconhecimento biométrico facial, é imperativo que essa alegação de considerável eficácia seja respaldada por dados que efetivamente demonstrem os resultados obtidos com a identificação de indivíduos, em relação à substancial intrusão na privacidade e proteção dos dados individuais[69].

3.4.1 Smart Sampa

A Prefeitura de São Paulo lançou um edital visando adquirir um sistema de monitoramento capaz de identificar indivíduos suspeitos com base em determinadas características, incluindo a cor da pele. O projeto intitulado Smart Sampa tem como meta a instalação de 20 mil câmeras até 2024, requerendo um investimento de aproximadamente R$ 70 milhões por ano.

O programa Smart Sampa planeja empregar a tecnologia de reconhecimento facial, a qual é notavelmente “pouco precisa” no contexto da segurança pública. Em oposição à iniciativa, o vereador Celso Giannazi (PSOL) caracteriza o Smart Sampa como um “projeto de grande risco” que pode agravar a disparidade social. Todos

[68] Relatório “Vigilância automatizada: uso de reconhecimento facial pela Administração Pública no Brasil”. Lapin, 2021. Disponível em: <https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/> Acesso em: 14 ago. 2023.

[69] Estudados 151 casos de uso de FRT foram identificados em 4 estados federais. Em 42 desses casos, havia dados sobre identidade racial. Destes 42, 38 dos indivíduos rastreados eram negros. Rede de Observatórios da Segurança. Retratos da Violência. 2019. Disponível em: <https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeirorelatorio_20_11_19.pdf>. Acesso em: 15 ago. 2023.

compartilham o desejo por segurança e por uma cidade mais segura, mas não à custa da limitação das liberdades individuais e dos direitos de imagem das pessoas. Após a realização da audiência, os membros da Comissão Extraordinária de Direitos Humanos e Cidadania da Câmara Municipal comprometeram-se a elaborar um requerimento oficial dirigido à Prefeitura de São Paulo, solicitando informações sobre o progresso da implementação da plataforma, bem como sobre eventuais estudos ou iniciativas de monitoramento por meio de câmeras e reconhecimento facial.

A versão inicial do edital foi publicada em novembro de 2022, onde se afirmava que “a pesquisa deve abordar diferentes tipos de características como cor, aparência facial e outras características”, e também indicava que a identificação do comportamento seria baseada em situações de “vadiagem” e no tempo de permanência do suspeito em um local[70].

Numa reação a isso, o IDEC (Instituto Brasileiro de Defesa do Consumidor) e outras 50 organizações manifestaram-se contra o edital. Em resposta às críticas, a prefeitura decidiu suspender o processo de licitação para a contratação do sistema, para dissipar quaisquer dúvidas sobre a gestão do programa. O prefeito afirmou que a administração municipal reconhece a possibilidade de empregar a tecnologia nas políticas de segurança pública preventiva, contanto que se corrijam erros anteriores e se respeitem as leis e direitos individuais.

Após quatro meses de suspensão, em abril de 2023, o conteúdo do edital foi parcialmente alterado e o Tribunal de Contas do Município (TCM) permitiu a retomada do processo de aquisição das câmeras. No entanto, em 18 de maio, o pregão foi novamente suspenso por uma liminar do juiz Luis Manuel Fonseca Pires, que expressou preocupações quanto à possibilidade de ameaça aos dados pessoais dos cidadãos, o que poderia violar a Lei Geral de Proteção de Dados (LGPD). Além disso, Pires destacou o número significativo de especialistas e estudiosos que preveem o risco de perpetuação do racismo estrutural no uso desse sistema.

Posteriormente, em 23 de maio, a prefeitura de São Paulo e a Secretaria de Segurança Urbana conseguiram remover o embargo ao projeto por meio de uma liminar concedida pela desembargadora Paola Lorena, do Tribunal de Justiça de São

[70] Edital da prefeitura de São Paulo prevê sistema de câmeras que identifica cor e ‘vadiagem’. CartaCapital, 2022. Disponível em: <https://www.cartacapital.com.br/sociedade/edital-da-prefeitura-de-sao-paulo-preve-sistema-de-cameras-que-identifica-cor-e-vadiagem/> Acesso em: 15 ago. 2023.

Paulo (TJSP). Lorena argumentou que “não há evidências de que a implementação do videomonitoramento reforce eventuais discriminações sociais e raciais, uma vez que não é possível determinar a origem ou imparcialidade dos artigos e reportagens jornalísticas”. Em uma sessão realizada na última segunda-feira (29), o pregão eletrônico teve a participação de 12 empresas interessadas em fornecer o sistema de videomonitoramento para a prefeitura da cidade. A proposta mais vantajosa apresentada foi de 9,2 milhões por mês para a implementação do serviço, cumprindo todos os requisitos estabelecidos no edital. Caso a oferta seja confirmada, a empresa vencedora poderá acumular aproximadamente 552 milhões de reais ao longo de 60 meses.

4. CONCLUSÃO

Apesar das vantagens trazidas pelas inovações tecnológicas, surgem diversos problemas decorrentes delas no âmbito da justiça. Isso ocorre porque essas novas tecnologias refletem a visão de seus criadores e, a partir disso, começam a tomar decisões de maneira autônoma por meio de mecanismos de aprendizado de máquina.

Consequentemente, a inserção das novas tecnologias no contexto criminal tem se mostrado arriscada, já que métodos de avaliação de risco para prever reincidência, e até mesmo a emissão de sentenças, são percebidos como atividades automatizadas. Além disso, com o uso das novas tecnologias, a administração da justiça, em certos casos, é influenciada por previsões geradas por máquinas, em detrimento de considerações exclusivas sobre os fatos. Nesse cenário, a falta de controle resultante da adoção das novas tecnologias no contexto judicial se torna evidente no momento em que a habilidade de análise e interpretação dos casos é diminuída, ficando a cargo da máquina.

Dessa discussão também surgiu a preocupação com até onde o Poder Público e a iniciativa privada devem atuar, no que se refere ao manejo de informações pessoais dos indivíduos, especialmente no contexto das cidades inteligentes e seguras.

Além disso, mesmo que os aprimoramentos sejam realizados ao máximo nos sistemas de previsão de comportamento e prevenção de crimes, por meio do refinamento das operações de análise de dados e dos mecanismos de vigilância em larga escala, essa mesma estrutura, concebida com boas intenções, poderia ser explorada para atender aos interesses políticos de um grupo específico detentor do poder. Ao possibilitar a identificação rápida e fácil de indivíduos associados a uma determinada religião ou alinhados com certa orientação política, tais ferramentas poderiam facilitar a perseguição de dissidentes políticos e outros segmentos da sociedade considerados indesejáveis pelas autoridades governantes. Isso não apenas representaria uma ameaça direta aos direitos fundamentais e às liberdades civis da população, mas também comprometeria os princípios fundamentais do Estado Democrático de Direito.

Nesse contexto, sob a justificativa de prevenir a ocorrência de crimes, poderia ser estabelecido um regime de vigilância que apresenta uma série de desvantagens, como mencionado anteriormente. Além disso, tal regime não demonstra eficácia em cumprir seu propósito. Adicionalmente, visando antecipadamente neutralizar uma ameaça abstrata, poderiam ser promulgadas medidas legais que criminalizam preparativos para delitos, o que acabaria por restringir garantias processuais, desconsiderar princípios fundamentais do sistema jurídico e até mesmo inverter os procedimentos do sistema penal.

Na ausência de precauções adequadas, a utilização de tecnologias de reconhecimento facial automatizado pode contribuir significativamente para a perpetuação do racismo nas estruturas sociais do Brasil. Portanto, é imperativo, em primeiro lugar, garantir a transparência nos sistemas de auditoria dos algoritmos de aprendizado, visando identificar possíveis preconceitos discriminatórios e desenvolver soluções para mitigar essa possibilidade.

Além disso, é crucial promover uma mudança na abordagem da política de segurança pública, particularmente na distribuição de recursos orçamentários destinados a investimentos na área de tecnologia e aperfeiçoamento dos dispositivos tecnológicos utilizados pelas forças policiais federais e civis. Com efeito, conforme demonstrado, a adoção de câmeras de alta resolução e qualidade pode desempenhar um papel fundamental na redução da margem de erro durante a aplicação do reconhecimento facial automatizado.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Silvio. **Racismo estrutural: Feminismos plurais**. São Paulo: Jandaíra, 2019, p. 66-67.

ACHIUME, Tendayi. **Racial discrimination and emerging digital technologies: a human rights analysis: report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance**. United Nations Digital Library, Genebra, 18 jun. 2020. Disponível em: https://digitallibrary.un.org/record/3879751.

AMARAL, Augusto Jobim do. **O dispositivo inquisitivo: entre a ostentação penal e a estética política do processo penal**. 2014. 499 f. Tese (Doutorado em Ciências Criminais). Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2014, p. 336

AMELUNG, Rechtsgüterschutz, p. 385 junto de ANDRADE, Manuel da Costa, "**Sobre as proibições de prova em processo penal**", ob. cit., p. 124

AMELUNG, "Informationsbeherrschungsrechte", p. 22 junto de ANDRADE, Manuel da Costa, "**Sobre as proibições de prova em processo penal**", Gestlegal, 2ª edição, março 2022, p.17

ANDRADE, Manuel da Costa, "**Sobre as proibições de prova em processo penal**", Gestlegal, 2ª edição, março 2022.

BAN FACIAL RECOGNITION. Ban Facial Recognition. Disponível em: https://www.banfacialrecognition.com. Acesso em: 4 out. 2021.

BEUTIN, Lyndsey. **Racialization as a Way of Seeing: The Limits of Counter-Surveillance and Police Reform**. 2017.

Big Brother Watch, "**Stop Facial Recognition**", disponível em https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/. Acesso em: 3 ago. 2023

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-BRASIL. Ministério da Justiça e Segurança Pública. **Polícia Federal implementa nova Solução Automatizada de Identificação Biométrica**. Polícia Federal. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica. Acesso em: 21 de agosto de 2023.

CAETANO, Guilherme. **Estudo analisa 5 mil processos por tráfico de drogas e mostra que negros são alvo de prisões com baixo número de provas**. O Globo,

2023. Disponível em: https://oglobo.globo.com/brasil/noticia/2023/07/18/estudo-analisa-5-mil-processos-por-trafico-de-drogas-e-mostra-que-negros-sao-alvo-de-prisoes-com-baixo-numero-de-provas.ghtml. Acesso em: 19 ago. 2023.

CARNEIRO, Sueli. **Racismo, sexismo e desigualdade no Brasil** / Sueli Carneiro. São Paulo: Selo Negro, 2011 p. 86

Cathy O'Nei autora do livro: **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça à democracia**. 1ª edição. Tradução: Rafael Abraham, Santo André, SP: Ed. Rua do Sabão, 2020.

CHNEIER, Bruce. **Data and Goliath: the hidden battles to collect your data and control your world**. New York. W. W. Norton, 2015. p. 108.

CODED BIAS. Direção: Shalini Kantayya. Produção: Shalini Kantayya. Co-Produção: Sabine Hoffman. China, Estados Unidos, Gra Bretênia: 7ª Emire Media, 2020. Streaming

COSTA, Eduarda; REIS, Carolina. **LGPD Penal: o que foi feito até aqui e quais são os próximos passos? LAPIN**. Disponível em: https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos. Acesso em: 19 de agosto de 2023.

DAVIS, Angela. **A liberdade é uma constante**. Trad. Heci Regina Candiani. 1ª ed. São Paulo: Boitempo, 2018

ELECTRONIC FRONTIER FOUNDATION (EFF). Face Recognition. 2017. Disponível em: https://www.eff.org/pages/face-recognition. Acesso em: 5 ago. 2023.
FALCÃO, Cíntia. L**ENTES RACISTAS Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial**. Intercecpt_Brasil, 2019 Disponível em: https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/>. Acesso em: 13 ago. 2023.

FIDALGO, Sónia, "**A utilização de inteligência artificial no âmbito da prova digital — direitos fundamentais (ainda mais) em perigo**", ob. cit., p. 142.

FUCHS, C., & CHANDLER, D.. **Introduction Big Data Capitalism - Politics, Activism, and Theory**. In: Chandler, D., & Fuchs, C. (eds.), **Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour,** 2019

HANNAH-MOFFAT, K. **Algorithmic risk governance: Big Data analytics, race and information activism in criminal justice debates**. Theoretical Criminology, 2019, p. 453–470.

HARTMANN PEIXOTO, Fabiano; MARTINS DA SILVA, Roberta Zumblick. **Inteligência artificial e Direito**. v. 1. Curitiba: Alteridade Editora, 2019 - p. 21

HERCOG, A.; MELO, P. V. **O racismo que estrutura as tecnologias digitais de informação e comunicação**. Brasil de fato, 2019. Disponível em: https://www.brasildefato.com.br/2019/12/03/artigo-or-o-racismo-que-estrutura-astecnologias-digitais-de-informacao-e-comunicacao. Acesso em 13 ago. de 2023.

HOLSTON, James. **A Cidade Modernista: uma crítica de Brasília e sua utopia/ James Holston**; Tradução Marcelo Coelho.- São Paulo: Companhia das Letras, 1993, p 23.

LAMA, José Pérez de; SANCHEZ-LAULHE, José. **Consideraciones a favor de un uso más amplio del término tecnopolíticas. Sobre la necesidad de la crítica y las políticas del conocimiento y las tecnologías**. In: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldiserra Carvalho. Algoritarismos. São Paulo: Tirant lo Blach, 2020.

LENTINO, Amanda. "**This Chinese facial recogniton start-up can identify a person in seconds**". CNBC Disruptor

LOPES JUNIOR, Aury. **Direito Processual Penal**. 14 ed. São Paulo: Saraiva, 2017, p. 185.

LUCENA, Pedro Henrique Capelari de. **VIÉS E RACISMO NO POLICIAMENTO**
LYON, D. Globalizing surveillance: Comparative and sociological perspectives. Internacional Sociology, 2004, p. 135-149

LYON, David. **Vigilância líquida: diálogos com David Lyon.** Zahar, 2014. p. 5 a 17.

MAGRANI, Eduardo. **A Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018

MANTELLO, Peter. **The machine that ate bad people. Big Data & Society**. Dez. 2016. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/2053951716682538. Acesso em: 05 agosto de 2023.

MARASCIULO, Marília**, "Reconhecimento facial: prós e contras da tecnologia que veio para ficar"**, GALILEU, junho de 2020, disponível em https://revistagalileu.globo.com/Tecnologia/noticia/2020/06/reconhecimento-facial-pros-econtras-da-tecnologia-que-veio-para-ficar.html. Acesso em 18 ago. 2023.

MAYBIN, S. **Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA.** 2016. Disponível em: https://www.bbc.com/portuguese/brasil-37677421. Acesso em 9 ago. 2023.

MILLS, Charles. **The Racial Contract**. Nova York: Cornell University, 1997.

MOROZOV, Evgeny. ***Bit tech:* a ascensão dos dados e a morte da política**. São Paulo: Ubu, 2018. p 28.

NOBLE, S. ROBERTS, S. T. **Elites tecnológicas, meritocracia e mitos pós-raciais**

no Vale do Silício.6 Vol. 22 Nº 1 - janeiro/abril 2020. Revista Fronteiras - estudos midiáticos.

NOBLE, Safiya Umoja. **Algorithms of oppression: how search engines reinforce racism.** NYU Press, 2018 p. 29.

NUNES, P. **Algoritmo e racismo nosso de cada dia: Reconhecimento facial aposta no encarceramento e pune preferencialmente população negra**. Folha de São Paulo, 02 de Jan de 2021. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/. Acesso em 5 ago. 2023.

NUNES, Pablo. **EXCLUSIVO: LEVANTAMENTO REVELA QUE 90,5% DOS PRESOS POR MONITORAMENTO FACIAL NO BRASIL SÃO NEGROS.** Intercept_Brasil, novembro de 2021. Disponível em: https://www.intercept.com.br/2019/11/21/presos-monitoramento-facial-brasil-negros/. Acesso em: 13 ago. 2023.

NUNES, Pablo. **O algoritmo e racismo nosso de cada dia: Reconhecimento facial aposta no encarceramento e pune preferencialmente população negra.** Piauí, 2 jan. 2021. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-eracismo-nosso-de-cada-dia. Acesso em: 13 ago. 2023.

Nunes, Pablo. **Um Rio de olhos seletivos [livro eletrônico]: uso de reconhecimento facial pela polícia fluminense** / Pablo Nunes, Mariah Rafaela Silva, Samuel R. de Oliveira. – Rio de Janeiro : CESeC, 2022

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça à democracia.** 1ª edição. Tradução: Rafael Abraham, Santo André, SP: Ed. Rua do Sabão, 2020. p. 23.

OLIVEIRA, Samuel. **Sorria, você está sendo filmado!**: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

PERRY, Walter L.; McINNIS, Brian; PRICE, Carter C.; SMITH, Susan; HOLLYWOOD, John S. **Predictive Policing: Forecasting Crime for Law Enforcement.** Santa Monica, CA: RAND Corporation, 2013. Disponível em: <https://www.rand.org/pubs/research_briefs/RB9735.html>. Acesso em 12 ago. 2023.

QUEIROZ, M. V. L. **Constitucionalismo brasileiro e o Atlântico negro: a experiência constituinte de 1823 diante da Revolução Haitiana**. Rio de Janeiro: Lumen Juris, 2017, p. 10-42.

Relatório **Vigilância Automatizada: uso de reconhecimento facial pela Administração Pública**. Laboratório de Políticas Públicas e Internet: 2021.

RODRIGUES, Anabela Miranda, **"A Inteligência Artificial no Direito Penal"**,

Almedina, 2022, pp. 11-59.

SILVA, Tarcizio. **Dos autômatos e robôs às redes difusas de agência no racismo algorítmico**. In: TAVARES, A. R. Vestígios do Futuro: 100 Anos de Isaac Asimov. Rio de Janeiro: Editora Etheria, 2020.

SILVA, Tarcizio. **Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código**. Disponível em: bighttps://lavits.org/wp-content/uploads/2019/12/Silva-2019-LAVITSS.pdf. Acesso em: 10 ago. 2023.

SILVA, Tarcizio. **Racismo Algorítmico: Inteligência artificial e discriminação nas redes digitais.** São Paulo: Edições Sesc SP, 1ª ed. 2022. n.p. [E-book].

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais.** São Paulo: Edições Sesc São Paulo, 2017 — p. 38.

SUMPTER, David. **Dominados pelos números do Facebook e Google às fake news: os algoritmos que controlam nossa vida**. Rio de Janeiro: Bertrand Brasil, 2019, p. 87.

THALES. **Biometrics: authentication & identification** (definition, trends, use cases, laws and latest news) — 2020 review. 2020.

THAMAY, R.; TAMER, M. **Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie**. São Paulo: Thomson Reuters Brasil, 2020, p.157-158

WILLIAMS, R., & JOHNSON, P. **'Wonderment and dread': Representantios of DNA in ethical disputes about forensic DNA databases**. New Genetics and Society, 2004, p. 205-223

ZUBBOF, Shoshana. **A Era do Capitalismo de Vigilância.** 1 ed. Editora Intrínseca, 2021. p.18

ZUBOFF, Shoshana. **Big Other: capitalismo de vigilância e perspectivas para uma civilizaçãode informação**. In: BRUNO, Fernanda [et al.] (Org). Tecnopolíticas da vigilância: perspectivas da margem. São Paulo, Boitempo. 2018. pp. 17-68.