DIREITO & POLÍTICA

Direito e Política, vol. 20, n. 3, 2025

A APLICAÇÃO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA BRASILEIRA E SEUS DESAFIOS

Cinthia Obladen de Almendra Freitas

Devilson da Rocha Sousa

Heloísa Daniela Nora

Contextualização: O uso da tecnologia de reconhecimento facial vem sendo apregoado no Brasil como uma ferramenta de suma importância para a segurança pública, seja no que se refere à proteção dos cidadãos e à prevenção de crimes, seja quanto a identificação e localização de pessoas procuradas pela estrutura policial. Apesar de todos os supostos benefícios advindos do seu emprego, a introdução dessa tecnologia no cotidiano da segurança pública brasileira tem gerado diversas críticas, em especial por conta do alegado viés discriminatório da tecnologia, que estaria direcionada majoritariamente para grupos tradicionalmente marginalizados e criminalizados, e, ainda, pela violação a direitos e liberdades fundamentais a partir de fiscalização massiva e ostensiva por parte de instituições do Estado.

Objetivos: Este artigo tem como objetivo analisar como se dá o funcionamento da tecnologia de reconhecimento facial, a fim de responder à seguinte pergunta: quais são os principais problemas resultantes do uso da tecnologia de reconhecimento facial na segurança pública brasileira e como superá-los?

Método: A pesquisa utilizou metodologia hipotético-dedutiva com revisão e levantamento bibliográfico.

Resultado: Como resultado, ficou demonstrado que a utilização da tecnologia de reconhecimento facial no Brasil se dá de forma desordenada, pouco transparente e apresenta significativas falhas, fatores estes que servem para evidenciar tanto seu desacordo com os direitos fundamentais quanto a premente necessidade de regulação em nível federal.

Palavras-chave: Defensoria Pública; Acesso à Justiça; Tutela das Vulnerabilidades; Liberdade Substantiva; Abordagem das Capacitações.

DEFENSORÍA PÚBLICA Y SU MISIÓN CONSTITUCIONAL: UN ENFOQUE DESDE LAS VULNERABILIDADES Y LAS CAPACIDADES HUMANAS

Contextualización: La Defensoría Pública desempeña un papel fundamental en la promoción del acceso a la justicia, especialmente para personas en situación de vulnerabilidad. Basado en la teoría de las capacidades de Amartya Sen, este estudio explora cómo la institución va más allá de la asistencia técnico-jurídica, desempeñando funciones extrajudiciales, educativas y estratégicas para abordar distintos tipos de vulnerabilidad y reducir las desigualdades estructurales.

Objectivos: Este artículo tiene como objetivo analizar el papel constitucional de la Defensoría Pública en la ampliación de las libertades sustantivas, considerando la diversidad de vulnerabilidades que afectan el acceso a la justicia.

Método: La investigación es de carácter bibliográfico y adopta un enfoque deductivo, partiendo de premisas generales para llegar a una conclusión específica. El estudio se centró en doctrinas jurídicas y estudios académicos que analizan la relación entre la Defensoría Pública, las vulnerabilidades y el acceso a la justicia.

Resultados: El estudio demuestra que la Defensoría Pública desempeña un papel esencial en la democratización del acceso a la justicia. Al adoptar una concepción amplia de las vulnerabilidades, la institución contribuye a la construcción de una sociedad más justa y equitativa, consolidándose como un instrumento indispensable para la promoción de la ciudadanía y la superación de las desigualdades.

Palabras clave: Defensoría Pública; Acceso a la Justicia; Tutela de las Vulnerabilidades; Libertad Sustantiva; Enfoque de las Capacidades.

PUBLIC DEFENDER'S OFFICE AND ITS CONSTITUTIONAL MISSION: AN APPROACH FROM VULNERABILITIES AND HUMAN CAPABILITIES

Contextualization: The Public Defender's Office plays a fundamental role in promoting access to justice, especially for individuals in vulnerable situations. Based on Amartya Sen's capabilities theory, this study explores how the institution goes beyond legal assistance, performing extrajudicial, educational, and strategic functions to address different forms of vulnerability and reduce structural inequalities.

Objectives: This article aims to analyze the constitutional role of the Public Defender's Office in expanding substantive freedoms, considering the various vulnerabilities that affect access to justice.

Methodology: The research is bibliographic in nature and adopts a deductive approach, starting from general premises to reach a specific conclusion. The investigation focused on legal doctrines and academic studies that examine the relationship between the Public Defender's Office, vulnerabilities, and access to justice.

Results: The study demonstrates that the Public Defender's Office is essential in democratizing access to justice. By adopting a broad conception of vulnerabilities, the institution contributes to building a more just and equitable society, consolidating itself as an indispensable tool for promoting citizenship and overcoming inequalities.

Keywords: Public Defender's Office; Access to Justice; Protection of Vulnerabilities; Substantive Freedom; Capabilities Approach.

INTRODUÇÃO

O reconhecimento facial tem sido promovido como uma solução inovadora para questões de segurança pública, prometendo uma forma eficaz de identificar e localizar pessoas procuradas, bem como prevenir crimes. No Brasil, por exemplo, o Estado da Bahia tem adotado a tecnologia para realizar o monitoramento de espaços públicos durante eventos de grande porte, integrando-a às estratégias de vigilância e segurança pública. No entanto, a rápida expansão dessa tecnologia no contexto brasileiro tem levantado preocupações significativas sobre sua eficácia, impacto ético, integridade dos bancos de dados utilizados, eficácia dos algoritmos de identificação além de sua conformidade com os direitos fundamentais, como a privacidade e a liberdade individual. Para isso, este artigo investiga o uso da tecnologia de reconhecimento facial na segurança pública brasileira, examinando seus benefícios e desafios, bem como as questões críticas relacionadas ao viés discriminatório e à falta de regulamentação.

Após a demonstração de um contexto histórico, é possível perceber a rápida evolução da tecnologia, embalada por bancos de imagens, cada vez mais numerosos – entretanto, também é possível identificar suas inúmeras facetas, limitações e falhas técnicas que parecem persistir ao longo do tempo. O que se verifica inicialmente é que a eficácia do reconhecimento facial está atrelada a qualidade das imagens capturadas, precisão na extração das características e confiabilidade dos algoritmos utilizados.

Entretanto, o que se percebe é que, por mais que siga um ritmo acelerado de desenvolvimento, ainda existem falhas que persistem. Muitas vezes, sua utilização não leva em consideração os riscos inerentes à tecnologia, como seu enviesamento, racismo, falsos positivos e o impacto direto na intimidade e privacidade dos cidadãos. Por conta desse cenário, é necessário entender as preocupações éticas e legais que se relacionam a esse meio, demonstrando, inclusive, como a falta de regulamentação adequada leva a uma abordagem fragmentada e inconsistente no uso dessa tecnologia, resultando em riscos para os direitos dos cidadãos.

Diante desse cenário, por meio de metodologia hipotético-dedutiva com revisão e levantamento bibliográfico, analisa-se o funcionamento desta tecnologia, a fim de responder à seguinte pergunta: quais são os principais problemas resultantes do uso da tecnologia de reconhecimento facial na segurança pública brasileira e como superá-los? A hipótese desenvolvida foi a de que a adoção indiscriminada e não regulamentada da tecnologia de reconhecimento facial no Brasil contribui para falhas operacionais, a criação de “vieses raciais” e restrições desproporcionais aos direitos individuais. O objetivo geral da pesquisa é demonstrar que a tecnologia em si não é responsável pelos casos de discriminação, mas que sua má utilização pode levar a esse caminho. Como resultado, ficou demonstrado que a utilização da tecnologia de reconhecimento facial no Brasil se dá

de forma desordenada, pouco transparente e apresenta significativas falhas, fatores estes que servem para evidenciar tanto seu desacordo com os direitos fundamentais quanto a premente necessidade de regulação em nível federal.

1. A TECNOLOGIA DE RECONHECIMENTO FACIAL E SEU MODO DE OPERÇÃO

As tecnologias de reconhecimento facial são parte de um processo tecnológico que visa a identificar pessoas a partir de técnicas computacionais, analisando características faciais e criando representações matemáticas[1]. Essa área de pesquisa tecnológica se encaixa no campo do aprendizado de máquina, também conhecido como *machine learning*, um subcampo da ciência da computação que evoluiu a partir de pesquisas em reconhecimento de padrões. O objetivo principal do *machine learning* é permitir que uma máquina aprenda e identifique padrões a partir de dados inseridos nela, ajustando seus modelos conforme as informações são fornecidas.

As primeiras pesquisas de um sistema de reconhecimento facial semiautomatizado tiveram início em 1963, com o matemático Woodrow Wilson Bledsoe[2]. O pesquisador e sua equipe trabalharam em um experimento que verificava se computadores eram capazes de reconhecer e identificar rostos humanos diferentes[3]. O experimento, de forma resumida, dependia do *input*[4] de um operador que escaneava pessoas e tentava mapear suas características[5].

Entretanto, após 13 meses de pesquisa, o computador não foi capaz de reconhecer sequer um rosto[6]. As dificuldades relatadas pelo pesquisador em seu relatório[7] foram,

[1] Chamadas de "vetores de características". Por exemplo: ao processar uma imagem de um rosto humano para o reconhecimento facial, são extraídas características, como a posição de boca, nariz, olhos, etc., para formar um vetor numérico que represente essa face.

[2] Mais conhecido como "Woody". Em 1960, fundou sua própria empresa em Palo Alto, Califórnia: *Panoramic Research Incorporated*.

[3] A pesquisa envolvendo reconhecimento facial inspirou-se no sistema de Alphonse Bertillon, o criminologista que criou a antropometria judicial.

[4] A palavra "*input*" significa "entrada". Nesse caso, o *input* seria o fornecimento de informações para a máquina.

[5] BLEDSOE, Woodrow Wilson. **Proposal for a Study to Determine the Feasibility of a Simplified Face Recognition Machine.** Panoramic Research Inc. Palo Alto, California, 1963. Disponível em: https://archive.org/details/firstfacialrecognitionresearch/FirstReport/page/n5/mode/2up. Acesso em: 15 abr. 2024.

[6] RAVIV, Shaun. **The Secret History of Facial Recognition**. **Wired**, 21 de janeiro de 2020. Disponível em: https://www.wired.com/story/secret-history-facial-recognition/. Acesso em: 15 abr. 2024.

[7] This recognition problem is made difficult by the great variability in head rotation and tilt, lighting intensity and angle, facial expression, aging, etc. Some other attempts at facial recognition by machine have allowed for little or no variability in these quantities. Yet the method of correlation (or pattern matching) of unprocessed optical data, which is often used by some researchers, is certain to fail in cases where the variability is great. In particular, the correlation is very low between two pictures of the same person with two different head rotations. HISTORYOFINFORMATION. **Woodrow Bledsoe Originates Automated Facial Recognition**. [*S.l.*]: [*s.d.*]. Disponível em: https://www.historyofinformation.com/detail.php?entryid=2495. Acesso em: 30 abr. 2024.

principalmente: problemas com a falta de iluminação adequada e a diversidade e variedade das expressões faciais variáveis, além do impacto do envelhecimento nas características faciais[8]. Outra curiosidade sobre a pesquisa é que as informações obtidas não foram amplamente divulgadas devido ao financiamento da pesquisa ter sido realizado por uma agência de inteligência não identificada[9].

Já em 1965, com a evolução das técnicas de pesquisa, a introdução do sistema *men-machine*[10] e ampliação das bases de dados utilizadas para treinamento e teste, um novo estudo foi iniciado por Bledsoe, dessa vez com um número bem maior de rostos – aproximadamente 2.000. No entanto, mesmo com esses avanços, os pesquisadores enfrentaram desafios semelhantes aos observados em estudos anteriores[11].

Em novembro de 1973, Takeo Kanade publica sua tese de doutorado: *Picture processing system by computer complex and recognition human faces*. Na tese, utilizando uma base de dados com mais de 800 fotografias digitalizadas, propõe um sistema totalmente automatizado capaz de processar imagens de rostos e os reconhecer automaticamente[12]. O trabalho foi inovador na época, por explorar a utilização de técnicas de processamento de imagens e análise de padrões para identificar características faciais e reconhecer rostos, além do desenvolvimento de algoritmos que detectassem e localizassem características faciais de partes específicas, tais como olhos, nariz e boca, a partir das imagens capturadas, sem a necessidade de um operador. Na pesquisa de teste apresentada, 15 de 20 pessoas foram identificadas corretamente.

Alguns anos após os avanços pioneiros de Takeo Kanade, houve outra grande evolução nas tecnologias de reconhecimento facial com o trabalho de Sirovich e Kirby, em 1987[13]. Eles introduziram o método conhecido como *Eigenfaces*, método este expandido em 1991 por Matthew Turk e Alex Pentland[14]. O algoritmo *Eigenfaces* é fundamental na história do reconhecimento facial, pois emprega uma técnica matemática sofisticada para simplificar e efetivar a análise de imagens faciais. Baseando-se na Análise de

[8] O problema enfrentado por Bledsoe é conhecido como A-PIE (*ageing, pose, illumination, expression*).

[9] Há rumores de que a empresa que financiou a pesquisa se chamava *King-Hurley Research Group,* uma empresa de fachada utilizada pela *Central Intelligence Agency* (CIA).

[10] Tinha esse nome pela necessidade de que um operador inserisse as informações (operação homem-máquina).

[11] BLEDSOE, Woodrow Wilson; CHAN, Helen. **A Man-Machine Facial Recognition System-Some Preliminary Results**. Technical Report PRI 19A. Panoramic Research, Inc. Palo Alto: California, 1965.

[12] KANADE, Takeo. **Picture processing system by computer complex and recognition of human faces**. Department of Information Science, Kyoto University, 1973. Disponível em: https://www.ri.cmu.edu/pub_files/pub3/kanade_takeo_1973_1/kanade_takeo_1973_1.pdf. Acesso em: 15 abr. 2024.

[13] SIROVICH, Lawrence; KIRBY, M. Low-dimensional procedure for the characterization of human faces. 1986. **Journal of the Optical Society of Americ a A**, v. 4, n. 3, p. 519-524, 1987. Disponível em: https://www.face-rec.org/interesting-papers/General/ld.pdf. Acesso em: 15 abr. 2024.

[14] TURK, Matthew; PENTLAND, Alex. Eigenfaces for Recognition. **Journal of Cognitive Neuroscience**, Massachusetts Institute of Technology, v. 3, n. 1, 1991. Disponível em: https://www.face-rec.org/algorithms/PCA/jcn.pdf. Acesso em: 15 abr. 2024.

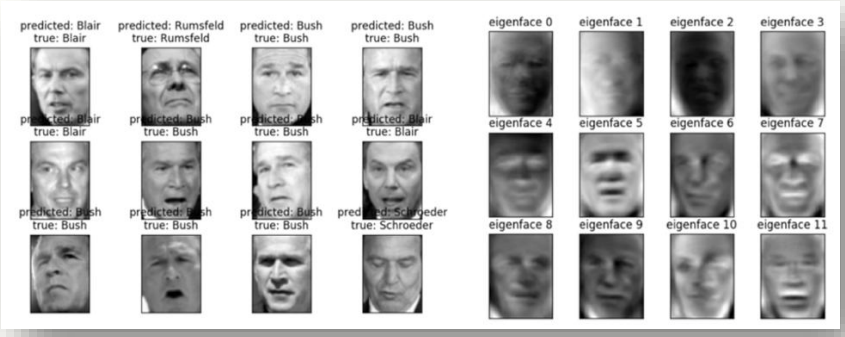
Componentes Principais (PCA), esse algoritmo converte imagens complexas de rostos em um conjunto reduzido de características essenciais. Esse processo não apenas separa as informações mais importantes de cada rosto, mas também facilita uma comparação eficaz e veloz entre diferentes imagens faciais.

O processo envolve, inicialmente, a coleta de um vasto conjunto de imagens faciais, que são então processadas para identificar os *eigenfaces*. Esse conjunto de *eigenfaces* forma uma base para o espaço de faces, no qual cada rosto individual pode ser projetado. Durante o reconhecimento, um rosto desconhecido é projetado nesse mesmo espaço, e sua posição é comparada às dos rostos conhecidos, facilitando a identificação ou a classificação. Ou seja, ele reduz a complexidade das imagens de um rosto para um conjunto menor de características significativas, possibilitando uma comparação mais eficiente e rápida entre as diferentes faces.

A aplicação do algoritmo *Eigenfaces* revolucionou o reconhecimento facial ao proporcionar uma abordagem matematicamente eficiente para o processamento de imagens. O método não apenas reduziu significativamente a quantidade de dados necessários para descrever cada rosto, mas também trouxe uma melhora na velocidade e na precisão do reconhecimento facial em diversos contextos, desde sistemas de segurança até aplicações de mídia social.

O conjunto de imagens abaixo ilustra o processo executado por essa aplicação, mostrando, no lado esquerdo, fotos de pessoas e, no lado direito, seus *eigenfaces*.

Figura 1 – Rostos e seus *eigenfaces*



Fonte: Face Recognition with Eigenfaces[15].

Outro marco no desenvolvimento nas metodologias de reconhecimento facial foi o

[15] DESHPANDE, Mohit. Face Recognition with Eigenfaces – Computer Vision Tutorial. **ZENVA**, 30 de novembro de 2023. Disponível em: https://gamedevacademy.org/face-recognition-with-eigenfaces/. Acesso em: 17 abr. 2024.

surgimento do algoritmo *Fisherface*[16], que pode ser visto como uma versão atualizada do *Eigenface* – por ter menos sensibilidade quanto à variação da iluminação e às expressões faciais das imagens.

Na década de 1990, as pesquisas científicas na área do reconhecimento facial automático se intensificaram, recebendo bastante atenção. O aparecimento de programas como o *Face Recognition Technology* (FERET)[17] impulsionaram a criação de uma base de dados para o teste dos sistemas criados, além de proporcionar uma grande evolução na área. Como resultado, no início dos anos 2000 emergiam as primeiras aplicações comerciais do reconhecimento facial automático. Surge, também, o *Facial Recognition Vendor Test* (FRVT), como uma série de avaliações e testes conduzidos pelo *National Institute of Standards and Technology* (NIST) para avaliar o desempenho de sistemas de reconhecimento facial desenvolvidos por diferentes fornecedores e empresas[18].

Já em 2001, ocorreu outra virada de página no contexto das tecnologias de reconhecimento facial. Paul Viola e Michael Jones criam o primeiro algoritmo capaz de realizar reconhecimento facial por vídeo[19]. Em 2004, esses autores revisitam e aprimoram ainda mais seu algoritmo, focando especialmente na melhoraria da detecção de rostos em ângulos variados, fato este que era uma limitação inicial do modelo. Viola e Jones introduziram melhorias que aumentaram significativamente a capacidade do algoritmo de reconhecer rostos não apenas de frente, mas também em posições parcialmente rotacionadas, facilitando a detecção em um espectro mais amplo de condições reais.

A metodologia introduzida por Viola e Jones, frequentemente referenciada como o "método Viola-Jones", utiliza um *framework* de detecção de objetos baseado em características chamado *Haar-like features*, juntamente a uma abordagem de aprendizado de máquina conhecida como "cascata de classificadores". Esse método destaca-se por sua habilidade em detectar rapidamente rostos em imagens, operando eficientemente, mesmo em condições de baixa resolução ou quando os rostos não estão perfeitamente alinhados com a câmera.

O algoritmo de Viola-Jones tornou-se um padrão na detecção de rostos, viabilizando uma série de aplicações, desde sistemas de segurança e vigilância até

[16] BELHUMEUR, Peter N.; HESPANHA, Joao P.; KRIEGMAN, David J. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 19, n. 7, p. 711-720, jul., 1997. Disponível em: https://cseweb.ucsd.edu/classes/wi14/cse152-a/fisherface-pami97.pdf. Acesso em: 15 abr. 2024.

[17] Lançado pelo *National Institute of Standards and Technology* (NIST) em 1993, um projeto que tinha como objetivo criar um sistema automático de reconhecimento facial voltado para inteligência, segurança e aplicação da lei.

[18] BLACKBURN, Duane M.; BONE, Mike; PHILLIPS, P. Jonathon. **Face Recognition Vendor Test 2000: Evaluation Report**. Defense Advanced Research Projects Agency. National Institute of Justice, 2001.

[19] VIOLA, Paul; JONES, Michael. Rapid Object Detection using a Boosted Cascade of Simple Features. **Conference on Computer Vision and Pattern Recognition**. 2001. Disponível em: https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf. Acesso em: 15 abr. 2024.

interações mais sofisticadas em dispositivos móveis e interfaces de usuário baseadas em reconhecimento facial. A capacidade de processar imagens de vídeo em tempo real abriu portas para inovações em campos, como automação residencial, jogos interativos e sistemas avançados de monitoramento, em que a identificação rápida e precisa de indivíduos se torna crucial.

Em 2007, um marco significativo foi alcançado no campo do reconhecimento facial com a criação do projeto *Labeled Faces in the Wild* (LFW) por uma equipe de pesquisadores liderada por Gary Huang, Vidit Jain e Erik Learned-Miller. Publicado em 2008, o LFW nasceu da compreensão de que as tecnologias de reconhecimento facial poderiam ser aprimoradas significativamente com o acesso a um conjunto de dados que oferecesse uma ampla gama de variabilidade nas condições de imagens faciais. O projeto pioneiro visava a superar as limitações dos conjuntos de dados existentes, que frequentemente contavam com imagens faciais sob condições controladas, limitando a eficácia dos sistemas de reconhecimento facial em ambientes reais[20].

O LFW introduziu um banco de dados sem precedentes, caracterizado por sua natureza "sem restrições". Isso significava que o conjunto de dados incluía imagens capturadas em uma variedade de situações do mundo real, abrangendo diferentes posições, expressões faciais, configurações de fundo e variáveis de qualidade de câmera. Com um total de 13.233 imagens de 5.749 indivíduos diferentes, o LFW proporcionou uma ferramenta inestimável para a pesquisa e desenvolvimento de algoritmos de reconhecimento facial capazes de operar eficientemente em condições dinâmicas e imprevisíveis[21].

A introdução do LFW representou um avanço significativo na pesquisa de reconhecimento facial, facilitando o desenvolvimento de sistemas mais robustos e precisos. Permitiu aos pesquisadores testar e refinar seus algoritmos contra um espectro muito mais amplo de variações faciais do que antes, impulsionando, assim, o progresso em direção a tecnologias de reconhecimento facial que podem ser aplicadas de maneira confiável em uma multiplicidade de cenários do dia a dia. O impacto do LFW no campo foi profundo, estabelecendo um novo padrão para avaliação de desempenho e incentivando a criação de conjuntos de dados semelhantes para impulsionar a inovação contínua na área. Já em meados de 2014, há a introdução do *Deepface,* um sistema de reconhecimento facial criado por um grupo de pesquisadores do Facebook.

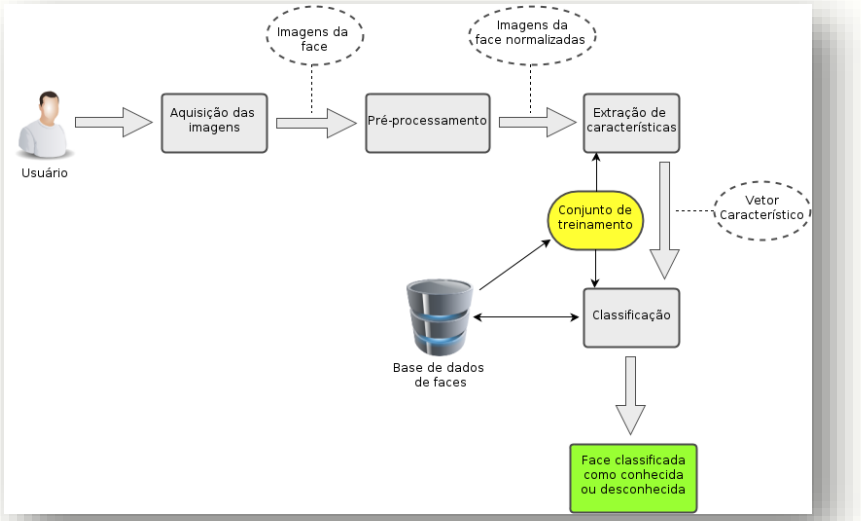
[20] HUANG, Gary B.; RAMESH, Manu; BERG, Tamara; LEARNED-MILLER, Erik. **Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments**. [*S.l.*]: [*s.d.*]. Disponível em: https://cs.brown.edu/courses/cs143/2011/proj4/papers/lfw.pdf. Acesso em: 16 abr. 2024.

[21] HUANG, Gary B.; RAMESH, Manu; BERG, Tamara; LEARNED-MILLER, Erik. **Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments**. [*S.l.*]: [*s.d.*]. Disponível em: https://cs.brown.edu/courses/cs143/2011/proj4/papers/lfw.pdf. Acesso em: 16 abr. 2024.

Essa caminhada histórica demonstra que a tecnologia de reconhecimento facial está diretamente vinculada a dois fatores técnicos primordiais: a capacidade de identificação de padrões de imagens em diferentes cenários ambientais; e ao banco de dados que alimenta o algoritmo de identificação que opera a ferramenta de identificação.

Em paralelo, o processo de identificação, em geral, passa por três fases principais, sendo elas: a detecção das faces e a captura de imagens; a extração de características e sua representação matemática; e, por último, o reconhecimento e a verificação na base de dados. Esse caminho pode ser mais bem compreendido a partir da ilustração abaixo.

Figura 2 – Processo de identificação



Fonte: Arquitetura do Sistema de reconhecimento facial[22].

Portanto, pode-se concluir que a eficácia do reconhecimento facial está diretamente vinculada a vários fatores-chave, dentre os quais a qualidade das imagens capturadas, a precisão na extração de características e a confiabilidade e eficiência dos algoritmos de correspondência utilizados. A qualidade das imagens é fundamental, pois imagens claras e bem definidas fornecem a base para a identificação precisa de características faciais. A extração de características realizada de forma precisa é crucial para diferenciar os indivíduos de maneira eficaz, mesmo em condições variáveis que incluem diferentes expressões faciais, iluminação e ângulos. Por fim, algoritmos de correspondência confiáveis e avançados são necessários para comparar essas características de forma precisa com as de imagens existentes em um banco de dados,

[22] DINIZ, Fabio Abrantes; MENDES NETO, Francisco Milton; LIMA JÚNIOR, Francisco das Chagas Lima Júnior; FONTES, Laysa Mabel Oliveira. RedFace: um sistema de reconhecimento facial baseado em técnicas de análise de componentes principais e autofaces. **Revista Brasileira de Computação Aplicada**, v. 5, n. 1, 2013. Disponível em: https://seer.upf.br/index.php/rbca/article/view/2627. Acesso em: 17 abr. 2024.

permitindo a identificação correta do indivíduo.

Cada um desses componentes desempenha um papel vital na construção de sistemas de reconhecimento facial robustos e confiáveis. O desafio reside não apenas em aprimorar cada elemento individualmente, mas também em garantir sua interoperabilidade eficiente. A integração bem-sucedida desses elementos define a fronteira para o desenvolvimento de tecnologias de reconhecimento facial que podem ser aplicadas de forma segura e eficiente em uma ampla gama de aplicações, desde ferramentas para o mercado de consumo até seu emprego na segurança pública.

2. O CENÁRIO DE APLICAÇÃO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA BRASILEIRA

Segundo Welinder[23], a tecnologia de reconhecimento facial tem como objetivo combinar as habilidades humanas de percepção com a imensa capacidade de armazenamento e processamento dos computadore[24]. Como evidenciado pelo contexto histórico mencionado anteriormente, essa tecnologia não é novidade. Ocorre que a introdução de bancos de dados abertos para treinar algoritmos, como o *Labeled Faces in The Wild*, e o interesse de empresas como o *Facebook* e *Google* impulsionaram seu progresso vertiginosamente nos últimos anos. Um exemplo dessa evolução pode ser observado no fato de que, em 1997, o melhor programa de reconhecimento facial do Departamento de Defesa do Governo Norte-Americano (*US Department of Defense*) tinha uma taxa de erro de 0,54; em 2006, essa taxa caiu para 0,003, uma melhoria de mais de duas ordens de magnitude[25].

No mesmo sentido, de acordo com um relatório do *National Institute of Standards and Technology*[26], que documenta os resultados do reconhecimento facial em quatro bancos de dados com mais de 30,2 milhões de fotos de 14,4 milhões de indivíduos, a precisão e a velocidade dos algoritmos têm melhorado. Todo esse cenário tem contribuído para um emprego massivo desta tecnologia para os mais diversos fins e nos mais diversos

[23] WELINDER, Yana. A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. **Harvard Journal of Law and Technology**, v. 26, n. 1, 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2109108. Acesso em: 19 abr. 2024.

[24] Em inglês, no original: "Face recognition technology aims to combine the superior perception skills of humans with the immense processing power and memory capacity of computers". ACQUISTI, Alessandro; GROSS, Ralph; STUTZMAN, Fred. Face Recognition and Privacy in the Age of Augmented Reality. **Journal of Privacy and Confidentiality**, v. 6, n. 2, 2014, p. 170). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305312. Acesso em: 16 abr. 2024.

[25] Em inglês, no original: "In 1997, the best computer face recognizer in the US Department of Defense's Face Recognition Technology program scored an error rate of 0.54 (the false reject rate at a false accept rate of 1 in 1,000). By 2006, the best recognizer scored 0.026. By 2010, the best recognizer scored 0.003 —an improvement of more than two orders of magnitude in just over 10 years". ACQUISTI, Alessandro; GROSS, Ralph; STUTZMAN, Fred. Face Recognition and Privacy in the Age of Augmented Reality. **Journal of Privacy and Confidentiality**, v. 6, n. 2, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305312. Acesso em: 16 abr. 2024.

[26] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT)**. Part 2: Identification. U.S. Department of Commerce, National Institute of Standards and Technology, 2018. Disponível em: https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf. Acesso em: 15 de jul. 2024.

cenários.

Ocorre que o Centro de Privacidade e Tecnologia da *Georgetown Law*, em um estudo de 2016, argumenta que o reconhecimento facial é inerentemente probabilístico, ou seja, não fornece respostas binárias, mas sim correspondências prováveis. O estudo também destaca que algumas características faciais são melhores indicadores de similaridade do que outras. Muitos algoritmos ajustam seus parâmetros para reconhecer e dar mais peso a características consistentes e discriminativas[27].

O histórico da tecnologia mostra como a composição do conjunto de treinamento pode influenciar a habilidade de um algoritmo em identificar certos grupos. Algoritmos treinados predominantemente com imagens de uma etnia ou gênero podem ter melhor desempenho para esses grupos. A complexidade da engenharia matemática envolvida, com milhões de variáveis otimizadas durante o treinamento, permite que o algoritmo aprenda, mas também dificulta a interpretação humana de seu comportamento[28].

Isso leva à conclusão de que diferentes fatores técnicos, assim como fatores ambientais, geográficos e sociais, influenciam na operação dessa tecnologia e em seu uso. Fatores internos à tecnologia, como os bancos de dados utilizados para o treinamento e operação da ferramenta de identificação, e fatores externos, como o ambiente onde ela foi treinada e os equipamentos utilizados para sua operação, contribuem significativamente para seu desempenho.

Internamente, a qualidade e a diversidade dos bancos de dados de treinamento são cruciais. Um banco de dados abrangente, com representações adequadas de diferentes etnias, gêneros e idades, melhora a precisão e a imparcialidade do algoritmo. Por outro lado, bancos de dados limitados ou enviesados podem levar a erros e discriminações. Externamente, as condições ambientais, como iluminação, clima e presença de obstáculos, afetam a captura e a qualidade das imagens. Em ambientes bem iluminados e estáveis, os algoritmos tendem a funcionar melhor do que em condições adversas. Além disso, a qualidade dos equipamentos, como a resolução das câmeras e a capacidade de processamento dos computadores, também influencia diretamente o desempenho do reconhecimento facial[29].

---

[27] GEORGETOWN LAW. **The Perpetual Line-up**. Unregulated Face Recognition in America. 2016. Disponível em: https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf Acesso em 15 de jul. 2024.

[28] GEORGETOWN LAW. **The Perpetual Line-up**. Unregulated Face Recognition in America. 2016. Disponível em: https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf Acesso em 15 de jul. 2024.

[29] GEORGETOWN LAW. **The Perpetual Line-up**. Unregulated Face Recognition in America. 2016. Disponível em: https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-

Com o histórico da evolução da tecnologia, foi possível entender, de início, como a composição de um conjunto de treinamento pode influenciar o tipo de rosto que um algoritmo será mais habilidoso em examinar. Se um conjunto de treinamento estiver mais bem treinado para uma determinada etnia ou sexo, pode ser melhor em identificar membros desse grupo em comparação com indivíduos com outras características. A engenharia matemática por trás de um algoritmo de reconhecimento facial pode incluir milhões de variáveis que são otimizadas no processo de treinamento. Essa complexidade é o que permite ao algoritmo aprender, mas também torna muito difícil para que um ser humano examine ou generalize seu comportamento[30].

Esse desafio decorre, principalmente, da natureza complexa e multidimensional das variáveis envolvidas: os algoritmos de reconhecimento facial utilizam uma vasta quantidade de dados e parâmetros que são ajustados e otimizados durante o treinamento e esses dados podem incluir características faciais sutis, como formas, texturas e cores, bem como padrões mais abstratos que representam características específicas de indivíduos. Além disso, a complexidade dos algoritmos de reconhecimento facial pode levar a resultados imprevistos ou enviesados, especialmente quando os conjuntos de treinamento não são representativos da diversidade da população geral.

Tais dados demonstram que, embora a tecnologia de reconhecimento facial seja extremamente útil para diversas atividades cotidianas, seu uso em áreas vinculadas à segurança pública, especialmente na identificação de suspeitos de crimes ou foragidos, apresenta desafios significativos. É possível afirmar que o desenvolvimento dessas atividades não pode se basear exclusivamente ou ter como principal ferramenta essa tecnologia. No contexto da segurança pública brasileira, desde 2011, essa tecnologia vem ganhando terreno significativo, tanto em ações do Governo Federal quanto, e especialmente, nas administrações estaduais, caso dos Estados de São Paulo, Rio de Janeiro, Bahia, Ceará, Amazonas, Amapá, Paraná, Santa Catarina e o Distrito Federal[31].

Essa expansão se dá em múltiplas frentes e diferentes cenários, mas todas elas convergem para os mesmos objetivos: (i) a melhoria nos processos de identificação e detenção de indivíduos suspeitos; (ii) prevenção e combate a atividades criminosas; e (iii) incremento no processo de monitoramento e segurança de espaços públicos.

%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf Acesso em 15 de jul. 2024.

[30] GEORGETOWN LAW. **The Perpetual Line-up**. Unregulated Face Recognition in America. 2016. Disponível em: https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf Acesso em 15 de jul. 2024.

[31] De acordo com informações coletadas junto às administrações estaduais e dados fornecidos por institutos especializados em segurança pública, como o Instituto Igarapé e a *Coding Rights*, atualmente todos os estados brasileiros empregam tecnologia de reconhecimento facial nas áreas de segurança pública. INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil**. Rio de Janeiro, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 15 abr. 2024.

Considerando a ausência de uma definição precisa no Brasil sobre o modo e o contexto de utilização da tecnologia de reconhecimento facial, e levando em conta que o artigo 144 da Constituição Federal[32] estabelece a Segurança Pública como dever do Estado e responsabilidade de todos, além de ser influenciada por decisões recentes do Supremo Tribunal Federal que expandiram as competências dos municípios em questões de Segurança Pública, diversas administrações municipais têm adotado esses sistemas. O que tem dificultado sobremaneira o mapeamento e a definição das formas de emprego dessa tecnologia por parte dos órgãos do Estado.

Dal Magro destaca que a adoção da tecnologia de reconhecimento facial pelos estados brasileiros é promovida como uma estratégia fundamental para melhorar a eficácia na prevenção e combate ao crime, especialmente em regiões extensas, resultando em maior eficiência nas ações de segurança pública[33]. Os benefícios advindos do uso dessa tecnologia em conjunto com bases de dados governamentais e sistemas de monitoramento incluem a identificação ágil de pessoas de interesse, como indivíduos com mandados de prisão ou desaparecidos, sem aumentar a necessidade de forças policiais. Além disso, permite uma gestão mais eficaz e humanizada dos espaços públicos, possibilitando abordagens menos invasivas e mais respeitosas aos direitos dos cidadãos, ao mesmo tempo em que otimiza recursos e minimiza o risco de confrontos diretos.

Devido a esses alegados benefícios e à sua atual vasta gama de aplicações pelos governos estaduais, é importante ressaltar que, apesar de o termo "reconhecimento facial" ser comumente empregado de maneira genérica para se referir a sistemas que identificam ou confirmam a identidade de uma pessoa a partir de uma imagem ou vídeo, existem, de fato, diversas técnicas, fundamentos e aplicações distintas dentro desse domínio, cada uma com características e implicações significativamente diferentes, conforme demonstrado no item anterior, que variam a depender do fim para o qual o sistema será empregado.

Nesse sentido, é fundamental ressaltar ainda que, no domínio da segurança pública, a operação e a eficácia da tecnologia de reconhecimento facial têm se apoiado em dois pilares principais. Primeiro, na capacidade do sistema para precisamente detectar a presença de um rosto em uma imagem ou sequência de vídeo, facilitando a subsequente análise, comparação e identificação de características faciais distintas. E em segundo lugar, na competência do sistema em associar o rosto identificado a perfis existentes em um banco de dados específico, permitindo a identificação rápida e precisa de indivíduos.

[32] BRASIL. **Constituição da República Federativa do Brasil**. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 abr. 2024.

[33] DAL MAGRO, Diogo. Riscos jurídicos de tecnologias de reconhecimento facial na segurança pública para a democracia brasileira. 192fls. 2022. Dissertação (Mestrado em Direito). Faculdade IMED. Passo Fundo, 2022.

Após a identificação de um rosto humano, inicia-se a etapa de reconhecimento em si. Nessa fase, algoritmos e *softwares* específicos do sistema de reconhecimento são utilizados para analisar e comparar o rosto detectado com os registros presentes em um banco de dados de imagens, banco esse que serve como base de operação para a ferramenta de identificação. O propósito desta etapa é estabelecer a identidade dos indivíduos capturados na imagem ou vídeo, por meio de uma análise comparativa das características faciais[34].

Considerando essa forma de operação, é possível afirmar que os sistemas de reconhecimento facial adotados atualmente no cenário da segurança pública brasileira atuam a partir de um processo composto por quatro fases, que, apesar de distintas, atuam de forma complementar uma da outra. A primeira destas fases é caracterizada pela geração de imagens a partir do monitoramento ostensivo de locais estratégicos com o intuito de coletar dados visuais.

Essa etapa, apesar de não estar diretamente vinculada a uma técnica em si, é fundamental para a aquisição das imagens e sequências de vídeo que serão analisadas subsequentemente. Dessa forma, pode afirmar que ela atua como uma etapa de ativação do processo, uma vez que insere os indivíduos ao alcance da tecnologia e assegura que o sistema obtenha os *inputs* visuais necessários para início da fase de identificação[35].

A demanda por esses dados iniciais é que tem justificado a implementação de um monitoramento extensivo e contínuo de espaços públicos por meio de câmeras de vigilância. Esse monitoramento é particularmente evidente em eventos de grande porte e com grande número de pessoas, como jogos de futebol, *shows*, festividades como as do carnaval[36], assim como em locais de grande fluxo, como estações de trem, rodoviárias, vias públicas e aeroportos[37].

Produzidas as imagens, tem-se início a segunda fase, a fase de detecção: é nesse momento que a tecnologia começa a operar propriamente, uma vez que o sistema inicia a

[34] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT)**. Part 3: Demographic Effects. U.S. Department of Commerce, National Institute of Standards and Technology, 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 15 abr. 2024.

[35] BIG BROTHER WATCH. **Face Off:** The lawless growth of facial recognition in UK policing. Big Brother Watch, 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 15 abr. 2024.

[36] Desde 2019, o Estado da Bahia tem adotado a tecnologia de reconhecimento facial para monitorar espaços públicos durante festividades, visando a aprimorar a segurança desses eventos. A tecnologia é promovida como um instrumento essencial na prevenção e no combate à criminalidade, integrando-a às estratégias de vigilância e segurança pública. No entanto, apesar das expectativas em torno de sua eficácia, a taxa de sucesso na identificação de criminosos através dessa ferramenta tem se mostrado notavelmente baixa. Para mais informações, acessar: FALCÃO, Cintia. A ascensão do tecnoautoritarismo. Parte 4. **The Intercept Brasil**, 20 de setembro de 2021. 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: 30 abr. 2024.

[37] HUREL, Louise Marie. Reconhecimento facial: regular, banir ou punir? **Insight Inteligência**, Rio de Janeiro, v. XXI, n. 84, p. 112-118, jan./fev./mar. 2019. Disponível em: https://insightinteligencia.com.br/pdfs/84.pdf. Acesso em: 16 abr. 2024.

busca pela identificação de um rosto humano nas imagens fornecidas. Após essa identificação, segue-se, então, a terceira fase, a de reconhecimento, quando, após identificar o rosto, o sistema gera uma representação numérica única, baseada em posição, tamanho, contorno e demais características faciais. Após esse processo, tem-se início a quarta e última fase, a etapa de comparação, na qual a representação numérica gerada pelos sistemas na fase anterior é submetida a um processo de comparação com outras representações faciais presentes em um banco de dados alimentado pelas forças policiais[38].

Embora o processo de funcionamento da tecnologia de reconhecimento facial possa parecer simples, inovador e de aplicação imediata – razões pelas quais talvez os governos estaduais venham adotando a tecnologia como uma das principais ferramentas no combate à criminalidade –, seu uso no Brasil enfrenta diversas preocupações, desconfianças e críticas. Essa resistência é particularmente forte entre entidades defensoras dos Direitos Humanos e organizações da sociedade civil.

Esse cenário deve-se a uma série de problemas identificados ao longo dos últimos anos, que incluem desde falhas técnicas inerentes à ferramenta até a falta de controle adequado, gestão deficiente[39] e conhecimento insuficiente no uso da tecnologia por parte dos agentes estatais. Tais problemas não só têm comprometido a eficácia dos benefícios alegados pelos governos, como também têm gerado danos significativos aos direitos e às garantias individuais dos cidadãos, em especial as da população negra e periférica dos grandes centros urbanos, que são os principais alvos de erros da tecnologia, conforme apontam Santos *et al*[40].

Nesse sentido, e para ilustrar os problemas relacionados ao reconhecimento facial, é importante destacar o estudo comparativo realizado por Nunes[41] sobre o uso dessa tecnologia no Estado do Rio de Janeiro. A pesquisa analisou dados do uso de reconhecimento facial ao redor do estádio do Maracanã e revelou que, apesar de o governo ter declarado a tecnologia como um sucesso no combate ao crime e na

[38] INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil**. Rio de Janeiro, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 15 abr. 2024.

[39] Existem casos de uso da tecnologia, como na Bahia, em que parte do sistema de monitoramento pode ser instalada nos celulares dos próprios policiais. Isso significa que eles podem usar essas ferramentas mesmo fora do ambiente de trabalho sem grandes dificuldades. O problema se agrava ainda mais, porque, além dos dados biométricos, esses sistemas permitem acesso a informações sobre veículos, impressões digitais, registros criminais, dados demográficos, gênero e localização, inclusive de crianças e adolescentes.

[40] SANTOS, Lucas Gabriel de Matos; COSTA, Arthur Barbosa da; DAVID, Jessica da Silva; PEDRO, Rosa Maria Leite Ribeiro. Reconhecimento facial: tecnologia, racismo e construção de mundos possíveis. **Psicologia & Sociedade**, Rio de Janeiro, v. 35, 2023. Disponível em: https://www.scielo.br/j/psoc/a/wJFV8yjBBr7cYnm3q6SXDjF/#. Acesso em: 16 abr. 2024.

[41] NUNES, Pablo. **Um Rio de câmeras com olhos seletivos:** uso de reconhecimento facial pela polícia fluminense. Rio de Janeiro: CESeC, 2022. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 19 abr. 2024.

identificação de suspeitos, a taxa de erros era significativamente alta. Os dados mostraram que 63% das pessoas detidas no dia de uso da ferramenta foram identificadas incorretamente.

Já Brandão apresenta dados que mostram que as tecnologias de reconhecimento facial usadas atualmente na segurança pública têm uma taxa de sucesso na identificação que varia entre 60% e 90%[42]. Isso indica que, mesmo nas melhores condições e no cenário mais favorável, uma parte significativa das pessoas ainda pode ser erroneamente identificada, levando a abordagens e até mesmo a prisões ilegais. Esses resultados evidenciam as limitações do reconhecimento facial e sugerem uma preocupação significativa com os riscos de erro e a consequente injustiça no uso dessa tecnologia.

Por conta desse cenário, pode-se identificar que três são os fatores que geram as maiores críticas quanto ao uso dessa tecnologia na segurança pública: (i) incertezas sobre a eficácia da ferramenta na identificação precisa de suspeitos, o que levanta dúvidas sobre a confiabilidade da tecnologia; essa questão é crítica, pois erros de identificação podem ter consequências graves para indivíduos erroneamente identificados; (ii) o viés algorítmico que permeia o processo de identificação, frequentemente citado como racismo algorítmico; esse problema aponta para uma discriminação inerente nos algoritmos usados na tecnologia, que tende a afetar desproporcionalmente indivíduos de certos grupos raciais, em especial, a população negra; e (iii) o impacto desproporcional sobre os direitos dos cidadãos, marcado por uma vigilância intensiva e contínua que suscita preocupações acerca de violações da privacidade e restrições à liberdade individual.

Devido a esse contexto e aos impactos adversos observados, especialmente em relação a abordagens indevidas e até mesmo à prisão de cidadãos inocentes, mesmo com a confiança demonstrada por alguns governos estaduais, há uma mobilização crescente em setores da sociedade civil organizada contra o uso dessa tecnologia. Santos *et al.* apontam que essas preocupações alimentam a oposição ao reconhecimento facial, evidenciando a necessidade de um escrutínio mais rigoroso e de regulamentações mais claras para prevenir injustiças e proteger direitos fundamentais[43]. A pressão por parte de grupos da sociedade civil visa a assegurar que a implementação da tecnologia respeite princípios democráticos e direitos humanos.

---

[42] BRANDÃO, Rodrigo. Tecnologias de reconhecimento facial na administração pública brasileira: Desafios técnicos e sociais para o uso responsável da tecnologia. *In*: DUARTE, Daniel Edler; CEIA, Eleonora Mesquita (org.). **Tecnologia, Segurança e Direitos:** os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. p. 115-140.

[43] SANTOS, Lucas Gabriel de Matos; COSTA, Arthur Barbosa da; DAVID, Jessica da Silva; PEDRO, Rosa Maria Leite Ribeiro. Reconhecimento facial: tecnologia, racismo e construção de mundos possíveis. **Psicologia & Sociedade**, Rio de Janeiro, v. 35, 2023. Disponível em: https://www.scielo.br/j/psoc/a/wJFV8yjBBr7cYnm3q6SXDjF/#. Acesso em: 16 abr. 2024.

Esse movimento intensificou as críticas ao uso dessa tecnologia, levando-as para além da simples busca por melhorias no processo de emprego. As críticas têm culminado na argumentação de que a tecnologia é completamente inútil para os propósitos iniciais. Além disso, há a preocupação de que sua implementação possa se tornar uma ferramenta de opressão estatal e de violação dos direitos dos cidadãos, reforçando o argumento de que seu uso deveria ser totalmente proibido na área da segurança pública. Essa posição já começou a influenciar a elaboração de legislações estaduais, como no caso dos Estados de São Paulo, Rio de Janeiro, Rio Grande do Sul e Sergipe, que buscam impedir o emprego, total ou parcial, desta tecnologia nas áreas da segurança pública[44].

Diante desse cenário e levando em conta complexidades, desafios e oportunidades associados ao tema do reconhecimento facial, torna-se essencial uma compreensão mais aprofundada dos problemas associados e da real utilidade dessa tecnologia para a segurança pública. Uma análise detalhada é necessária para garantir que, de um lado, os problemas inerentes ao reconhecimento facial sejam identificados e analisados e, de outro, possam ser traçados, caso possível, mecanismos normativos necessários à sua minoração.

3. O CENÁRIO DE EMPREGO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NO BRASIL

Conforme destacado anteriormente, a tecnologia de reconhecimento facial tem sido alvo de críticas, devido às falhas operacionais observadas, ao potencial viés racial que supostamente incorpora e à desproporção entre as restrições que impõe aos direitos fundamentais dos cidadãos, especialmente no que tange ao direito à privacidade e à intimidade, e os benefícios trazidos. Essas preocupações acarretam significativas implicações jurídicas que necessitam de uma análise cuidadosa para assegurar a eventual continuidade do emprego da tecnologia, em conformidade com os princípios de direitos humanos e a legislação vigente e, ainda, para afastar eventuais incompreensões.

Assim, e para abordar adequadamente a problemática associada à tecnologia de reconhecimento facial, é fundamental realizar uma análise aprofundada das causas subjacentes a cada um desses três principais fatores críticos. O primeiro e o segundo desses fatores, as falhas no processo de identificação de indivíduos e o suposto viés racial

[44] Para mais informações sobre os projetos de Lei em questão, conferir: SOARES, Nicolau. Reconhecimento facial na segurança pública é "nova aposta no encarceramento", diz especialista. **Brasil de Fato**, 29 de junho de 2022. Disponível em: https://www.brasildefato.com.br/2022/06/29/reconhecimento-facial-na-seguranca-publica-e-nova-aposta-no-encarceramento-diz-especialista. Acesso em: 15 abr. 2024. No mesmo sentido: CODING RIGHTS. Parlamentares de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos. **Coding Rights**, 21 de junho de 2022. Disponível em: https://codingrights.org/project-item/parlamentares-de-todas-as-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do-reconhecimento-facial-em-espacos-publicos/. Acesso em: 30 abr. 2024.

das ferramentas, estão intimamente relacionados a três questões técnicas específicas: (a) qualidade das imagens capturadas; (b) integridade, diversidade e confiabilidade do(s) banco(s) de dados que alimenta(m) a ferramenta; e (c) eficácia do *software* encarregado de correlacionar as imagens obtidas com as existentes nos bancos de dados.

O primeiro desses pontos, a qualidade das imagens capturadas, está diretamente relacionado com a precariedade dos sistemas de monitoramento empregados. Como observado, as imagens que servem para início da análise, o que representa a primeira etapa do processo de reconhecimento facial, são fundamentais para a correta operação e funcionamento da ferramenta. Ocorre que, atualmente, não há nenhuma normativa a nível federal ou estadual que oriente esse aspecto técnico. Assim, o que se percebe são estados e municípios investindo pesadamente em sistemas de reconhecimento facial sofisticados e utilizando câmeras de monitoramento com capacidade de captura de imagens de baixíssima qualidade, o que acaba impactando diretamente na eficiência da tecnologia.

Além disso, há, no Brasil, uma variedade de sistemas que geram e compartilham imagens e vídeos entre si, sem, contudo, manter um padrão consistente de qualidade nas representações. Atualmente, não há sequer uma normativa que possa dar as referências quanto às questões mínimas do processo de captura de imagens, tais como nível de luminosidade ou captura da face em mais de um ângulo, aspectos fundamentais no processo. Essa falta de padronização dificulta a integração entre os sistemas e compromete a precisão do reconhecimento facial, o que também aumenta a probabilidade de erros, já que a qualidade das imagens pode variar significativamente de um sistema para outro, prejudicando a eficácia geral do processo de reconhecimento.

No que diz respeito ao banco de dados – um dos aspectos mais críticos de qualquer sistema de reconhecimento facial utilizado no contexto da segurança pública –, os problemas vão desde questões técnico-informáticas até desafios jurídicos.

Considerando que os bancos de dados são essenciais para o funcionamento da tecnologia, na medida em que armazenam imagens e informações que são usadas para identificar pessoas, a qualidade e a diversidade de suas informações pode afetar significativamente a precisão e a eficiência do processo de identificação. Além disso, dados desatualizados ou de baixa qualidade podem resultar em falsos positivos e negativos, prejudicando a eficácia do sistema e levando a erros de identificação[45].

E, assim como ocorre nos sistemas de monitoramento, atualmente não existe legislação nacional que aborde direta ou indiretamente o tema dos bancos de dados

[45] BRANDÃO, Rodrigo. Tecnologias de reconhecimento facial na administração pública brasileira: Desafios técnicos e sociais para o uso responsável da tecnologia. *In*: DUARTE, Daniel Edler; CEIA, Eleonora Mesquita (org.). **Tecnologia, Segurança e Direitos:** os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. p. 115-140.

utilizados em ferramentas de reconhecimento facial. Isso faz com que questões técnicas-chave, como métodos de coleta, abrangência e formas de armazenamento dos dados biométricos associados a essa técnica, bem como aspectos legais, como as formas e os períodos de atualização, as hipóteses de compartilhamento dos dados e sua integração entre diferentes forças policiais e órgãos públicos, sejam tratados de maneira inconsistente pelos diversos entes estatais — União, Estados e Municípios.

Além disso, essa falta de normatização leva a uma abordagem fragmentada, em que cada entidade estatal pode adotar políticas próprias, resultando em práticas diversas e, por vezes, conflitantes. Sem diretrizes claras a nível nacional, torna-se difícil garantir uma abordagem padronizada, consistente e segura das ferramentas de reconhecimento facial, o que gera potenciais riscos para os cidadãos. Sobre essa questão, Hurel aponta que, sem uma normatização unificada, há o risco de práticas inadequadas de coleta e armazenamento, bem como de compartilhamento indiscriminado, sem critérios ou controle entre diferentes entes estatais, o que pode abrir caminho para abusos de poder e violação dos direitos fundamentais à privacidade e à intimidade dos cidadãos[46].

Tais questões ganham ainda mais relevância quando observado que a ausência de controle e a falta de atualização das informações e de diversidade nos bancos de dados representam problemas significativos no contexto do reconhecimento facial, na medida em que, sem atualização regular, os bancos de dados biométricos podem conter informações desatualizadas ou errôneas, comprometendo a precisão dos sistemas de reconhecimento facial, fato que tem ocorrido corriqueiramente no Brasil[47].

Por sua vez, conforme apontam Grother, Ngan e Hanaoka[48], a falta de diversidade compromete a eficiência dos sistemas de reconhecimento facial. Os autores destacam que, se os dados usados para treinar algoritmos de reconhecimento facial não refletirem uma ampla gama de características demográficas, como raça, idade e gênero, isso pode resultar em vieses e discriminação. Além disso, algoritmos de reconhecimento facial tendem a ser menos precisos quando aplicados a pessoas de cor, mulheres e minorias, quando aspectos

[46] HUREL, Louise Marie. Reconhecimento facial: regular, banir ou punir? **Insight Inteligência**, Rio de Janeiro, v. XXI, n. 84, p. 112-118, jan./fev./mar. 2019. Disponível em: https://insightinteligencia.com.br/pdfs/84.pdf. Acesso em: 16 abr. 2024.

[47] Diversos têm sido os casos noticiados pela imprensa nos quais indivíduos foram reconhecidos e chegaram até a ser presos por conta de informações desatualizados nos bancos de dados que alimentam a ferramenta. Para mais informações conferir: GRINBERG, Felipe; ARAÚJO, Vera. Mulher identificada por reconhecimento facial em Copacabana é solta após erro em sistema ser constatado. **O Globo**, 04 de janeiro de 2024. Disponível em: https://oglobo.globo.com/rio/noticia/2024/01/04/mulher-identificada-pelo-sistema-de-reconhecimento-facial-em-copacabana-e-liberada-apos-ser-constatado-que-mandado-de-prisao-estava-no-sistema-por-erro.ghtml. Acesso em: 30 abr. 2024. No mesmo sentido: CARMO, Wendal. Erros em série expõem fragilidade do reconhecimento facial como ferramenta de combate ao crime. **Carta Capital**, 19 de abril de 2024. Disponível em: https://www.cartacapital.com.br/tecnologia/erros-em-serie-expoem-fragilidade-do-reconhecimento-facial-como-ferramenta-de-combate-ao-crime/. Acessos em: 30 abr. 2024.

[48] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT)**. Part 3: Demographic Effects. U.S. Department of Commerce, National Institute of Standards and Technology, 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 15 abr. 2024.

particulares desses grupos não são observados, o que aumenta o risco de identificação incorreta e tratamento desigual.

Esses vieses podem levar a consequências negativas, como maior probabilidade de falsos positivos para grupos sub-representados na base de dados de treinamento, resultando em práticas discriminatórias e desigualdade na aplicação da tecnologia[49].

Ou seja, não é dizer que a ferramenta em si possua algum viés discriminatório ou determine suas ações a partir de um aspecto de *tirocínio* policial[50], como apontado por alguns críticos da tecnologia. O problema da discriminação algorítmica reside em como as ferramentas são treinadas e nos bancos de dados que as alimentam. Se a ferramenta for treinada com dados enviesados ou que não representam adequadamente a diversidade racial do local onde vai ser empregada, ela pode refletir esses vieses no seu funcionamento, resultando em respostas discriminatórias ou imprecisas. Nesse caso, mesmo algoritmos sofisticados podem apresentar diferenças de desempenho quando usados em grupos demográficos distintos ou que não reflitam a realidade do país[51].

Por fim, e ainda em relação aos bancos de dados, Hurel destaca a falta de transparência na sua formação[52]. Segundo a autora, muitas vezes, os indivíduos sequer sabem que seus dados estão sendo coletados e compartilhados para a alimentação e operação de bancos de dados que alimentarão ferramentas de reconhecimento facial. Tal prática pode levar a uma vigilância em massa e a riscos para os direitos fundamentais, como a privacidade, a intimidade e até a liberdade de expressão[53]. A falta de transparência e de consentimento explícito dos cidadãos em relação à coleta e ao uso de seus dados biométricos é uma preocupação central nessa temática, pois cria um ambiente propício para o abuso de poder e a invasão da esfera pessoal, comprometendo a confiança do público nas instituições e no uso responsável da tecnologia.

Já no que se refere à eficácia do *software* encarregado de correlacionar as imagens

[49] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT)**. Part 3: Demographic Effects. U.S. Department of Commerce, National Institute of Standards and Technology, 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 15 abr. 2024.

[50] O Relatório do Fórum Brasileiro de Segurança Pública aponta que os operadores da justiça criminal, em especial policiais, alegam ter a capacidade de identificar, apenas olhando para determinada pessoa, um conjunto de informações relevantes para a tomada de decisões. Essa habilidade seria conhecida como "tirocínio". BRASIL. Conselho Nacional de Justiça. **Relatório Analítico Propositivo**. Justiça Pesquisa. Direitos e Garantias Fundamentais Audiência de Custódia, Prisão Provisória e Medidas Cautelares: Obstáculos Institucionais e Ideológicos à Efetivação da Liberdade como Regra. Distrito Federal: CNJ, Poder Judiciário, 2018.

[51] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT)**. Part 3: Demographic Effects. U.S. Department of Commerce, National Institute of Standards and Technology, 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 15 abr. 2024.

[52] HUREL, Louise Marie. Reconhecimento facial: regular, banir ou punir? **Insight Inteligência**, Rio de Janeiro, v. XXI, n. 84, p. 112-118, jan./fev./mar. 2019. Disponível em: https://insightinteligencia.com.br/pdfs/84.pdf. Acesso em: 16 abr. 2024.

[53] HUREL, Louise Marie. Reconhecimento facial: regular, banir ou punir? **Insight Inteligência**, Rio de Janeiro, v. XXI, n. 84, p. 112-118, jan./fev./mar. 2019. Disponível em: https://insightinteligencia.com.br/pdfs/84.pdf. Acesso em: 16 abr. 2024.

obtidas nos monitoramentos com as existentes nos bancos de dados, cumpre destacar que, diferentemente do alegado por algumas administrações estaduais, a exemplo do Governo da Bahia, nenhuma tecnologia de reconhecimento facial está imune a falhas[54].

Isso significa dizer que, mesmo que a ferramenta opere a partir de um sistema de monitoramento que tenha alto grau de qualidade na captura das imagens e que interaja com um banco de dados altamente balanceado que reflita bem a diversidade da sociedade em que está operando, apresentará limitações que podem refletir em erros como falsos negativos, não identificando alguém que deveria ser identificado, ou falsos positivos, identificando alguém que não deveria identificar[55].

Um exemplo que ilustra as limitações dos *softwares* de reconhecimento facial empregados na segurança pública podem ser encontrado no sistema usado pela polícia de Londres, a Scotland Yard, a partir de 2019, elogiado por sua eficiência e precisão. Segundo dados da própria polícia, o sistema, considerado um dos mais avançados do mundo, teve uma taxa de sucesso de aproximadamente 70% na identificação de suspeitos, com uma taxa de falhas muito baixa, gerando apenas um alerta falso a cada mil verificações[56].

Mesmo uma taxa de 70% já seria motivo de muitas críticas e desconfianças, no entanto uma pesquisa realizada por pesquisadores da Universidade de Essex, usando métrica diferente, revelou uma realidade mais preocupante. O estudo constatou que, durante as testagens, o sistema conseguiu apenas oito identificações corretas em um total de 42 realizadas, indicando que 81% das pessoas foram identificadas erroneamente como suspeitas de crimes que não cometeram. Esses falsos positivos ressaltam a necessidade de uma análise mais cuidadosa e critérios rigorosos para avaliar a eficácia dos sistemas de reconhecimento facial, bem como a importância de abordar os riscos associados à sua utilização[57].

Diante dessas evidências, e mesmo em um cenário em que as inconsistências

---

[54] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT)**. Part 3: Demographic Effects. U.S. Department of Commerce, National Institute of Standards and Technology, 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 15 abr. 2024.

[55] BRANDÃO, Rodrigo. Tecnologias de reconhecimento facial na administração pública brasileira: Desafios técnicos e sociais para o uso responsável da tecnologia. *In*: DUARTE, Daniel Edler; CEIA, Eleonora Mesquita (org.). **Tecnologia, Segurança e Direitos:** os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. p. 115-140.

[56] ROBINSON, Martin. Hundreds of innocents face being grabbed in the street by police as Scotland Yard admits new facial recognition system gives false alerts one in every thousand faces — as it introduces cameras to spot criminals in London's busiest public places. **Daily Mail**, 24 de janeiro de 2020. Disponível em: https://www.dailymail.co.uk/news/article-7924733/Scotland-Yard-introduces-facial-recognition-cameras-hunt-watchlist-2-500-suspects.html. Acesso em: 20 abr. 2024.

[57] FUSSEY, Pete; MURRAY, Daragh. **Independent report on the London Metropolitan Police Service's trial of live facial recognition technology**. Human Rights Centre – University of Essex. The Human Rights, Big Data and Technology Project, 2019. Disponível em: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf. Acesso em: 20 abr. 2024.

anteriores, como a qualidade do monitoramento e dos bancos de dados, sejam resolvidas, o uso da tecnologia de reconhecimento facial como uma das principais ferramentas das forças policiais no que se refere à identificação de indivíduos não é recomendado. Ainda assim, muitos governos estaduais e municipais têm adotado essa prática, ignorando os riscos associados a vieses, falsos positivos e falsos negativos e violações de direitos, o que tem contribuído para uma crescente repulsa contra a tecnologia em diversos setores da sociedade, além de críticas quanto à desproporção entre as restrições que a tecnologia impõe aos direitos fundamentais dos cidadãos e os reais benefícios alcançados.

Quanto a esse último aspecto, o da proporcionalidade, é importante destacar, primeiramente, que no Brasil a tecnologia de reconhecimento facial tem sido empregada, como já destacado, a partir de uma lógica de monitoramento contínuo e extensivo, o que acaba gerando uma intervenção desproporcional na vida privada dos indivíduos, na medida em que não há nenhum controle externo ou transparência sobre os termos e as condições desses monitoramentos, o que resulta, segundo dados das secretarias estaduais, em um número significativo de detecções ilegais, e o aumento de processos discriminatórios, como evidencia o relatório do uso desta tecnologia pela polícia do Rio de Janeiro[58].

É fundamental ressaltar que a constante observação cria um ambiente de controle e monitoramento que limita a liberdade de expressão e reprime comportamentos espontâneos, formando uma espécie de panóptico digital. Essa configuração é similar ao conceito apresentado por Bentham, segundo o qual uma torre central de observação permitiria monitorar a todos, o tempo todo. Na obra de Boff, Fortes e Freitas[59], essa noção de monitoramento é descrita como um "panóptico eletrônico", indicando um modelo em que o controle é exercido por meio da tecnologia.

Nesse modelo de *panspectron*[60], a coleta de informações é ampla e o poder não se concentra apenas em uma torre de observação, e sim está disperso e generalizado em cada sistema, dispositivo ou processo tecnológico capaz de gerar dados continuamente, ou seja, em cada uma das forças de segurança que utilizam essa tecnologia.

Esse ambiente de vigilância constante resulta em um sistema no interior do qual os direitos de privacidade, intimidade e liberdade de expressão são reduzidos e o comportamento é rigidamente controlado, impactando a capacidade das pessoas de

[58] NUNES, Pablo. **Um Rio de câmeras com olhos seletivos:** uso de reconhecimento facial pela polícia fluminense. Rio de Janeiro: CESeC, 2022. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 19 abr. 2024.

[59] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

[60] *Panspectron* é o termo utilizado para descrever a transformação da sociedade moderna em uma espécie de panóptico digital, em que o controle e a vigilância são exercidos por meio do espectro total de informações e dados disponíveis sobre os indivíduos.

expressarem-se livremente. Assim, a questão do controle e do monitoramento por meio da tecnologia de reconhecimento facial levanta preocupações éticas sobre a centralização do poder e as implicações para a sociedade moderna, ressaltando a necessidade de uma discussão crítica sobre os limites da vigilância e as garantias de direitos individuais.

Nesse mesmo sentido, de vigilância constante proporcionada por novas tecnologias, Byung-Chul Han destaca que, nesse novo cenário, as pessoas acabam sendo submetidas a uma exposição constante de informações, o que permite que aqueles que controlam a infraestrutura de informação moldem a percepção e o comportamento dos indivíduos de maneira invisível, ao mesmo tempo que contribuem para uma cultura de transparência forçada, em que os cidadãos são incentivados a se expor e compartilhar dados pessoais, ainda que inconscientemente, enquanto as estruturas de poder permanecem opacas e não transparentes[61].

Assim, o que se observa é que esse fenômeno de vigilância intensiva, contínua e exacerbada, propiciada pela tecnologia de reconhecimento facial, aliado à falta de controle e de normas que sejam capazes de direcionar e limitar o uso desta tecnologia, coloca em risco os próprios direitos fundamentais de privacidade e intimidade, e alguns direitos individuais, como o de autonomia e liberdade individual, em proporção significativamente conflitante com aquelas autorizadas pela Constituição brasileira, ainda mais quando observados os benefícios e os resultados atingidos pela tecnologia.

Quanto a esse aspecto, Doneda, Sarlet e Mendes ressaltam a necessidade de uma abordagem equilibrada e proporcional para qualquer limitação dos direitos fundamentais à privacidade e à intimidade, uma vez que esses direitos, além de serem direitos fundamentais em espécie, são componentes essenciais de outros direitos fundamentais[62]. Isso significa que qualquer restrição a eles deve ser rigorosamente justificada, pois a Constituição brasileira estabelece critérios estritos para sua limitação.

Com base nisso, é razoável afirmar que o modelo atual de uso da tecnologia de reconhecimento facial está em completo desacordo com a Constituição, não apenas pelas limitações impostas à privacidade e à intimidade, mas também pela desproporcionalidade entre as medidas tomadas pelos poderes públicos e os resultados até então obtidos. Isso evidencia a necessidade de uma reavaliação do uso dessa tecnologia e uma reestruturação de suas bases, o que passa necessariamente por sua normatização a nível federal.

[61] HAN, Byung Chul. **Infocracia**: Digitalização e a crise da democracia. Tradução de Gabriel S. Philipson. Petrópolis: Vozes, 2022.

[62] DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel. **Estudos Sobre Proteção de Dados Pessoais**. São Paulo: Expressa, 2022.

CONSIDERAÇÕES FINAIS

Há um longo histórico de busca por métodos de melhoria da segurança pública no Brasil. Com a inserção da tecnologia nesse meio, criou-se uma expectativa geral de que as tecnologias de reconhecimento facial seriam a resposta definitiva para resolver os desafios de segurança pública do país, em especial no que se refere à identificação de suspeitos e criminosos e o monitoramento de amplas áreas. No entanto, a realidade por trás dessa promessa é mais complexa e falha do que parece à primeira vista.

Como ficou evidenciado, o uso da tecnologia de reconhecimento facial na segurança pública brasileira apresenta vários desafios e preocupações que necessitam de atenção cuidadosa. A implementação dessa tecnologia tem ocorrido de maneira desordenada e com pouca transparência, apresentando falhas técnicas que comprometem sua eficiência. Além disso, a ausência de regulamentação federal clara e a falta de controle sobre os bancos de dados biométricos levam a uma clara limitação na plena disposição de alguns direitos fundamentais, como a privacidade e a intimidade.

Outro aspecto crítico é o viés algorítmico, não propriamente da tecnologia em si, como restou comprovado, mas das bases de dados que servem para seu treinamento e operação, o que resulta em taxas mais altas de falsos positivos para determinados grupos raciais, especialmente a população negra, o que contribui para práticas discriminatórias e impactos desproporcionais na segurança pública. Esses problemas causam detenção de indivíduos inocentes e tratamento desigual, gerando sérias preocupações éticas e legais.

A necessidade de uma regulamentação equilibrada para o uso do reconhecimento facial, com diretrizes claras que assegurem uma aplicação ética e justa da tecnologia a nível federal se faz mais que necessária, uma vez que a atual manutenção do estado de coisas gera uma ofensa direta aos direitos fundamentais. Ademais, é importante observar que o modelo atual apresenta uma desproporcionalidade entre as restrições impostas aos direitos fundamentais e os benefícios obtidos, aspecto que destaca ainda mais a importância de uma reavaliação para alinhar o uso da tecnologia aos princípios constitucionais. Portanto, é essencial promover uma refundação dos termos e práticas de emprego da tecnologia de reconhecimento facial na segurança pública, a fim de proteger os direitos dos cidadãos e evitar práticas discriminatórias.

REFERENCIAS DAS FONTES CITADAS

ACQUISTI, Alessandro; GROSS, Ralph; STUTZMAN, Fred. Face Recognition and Privacy in the Age of Augmented Reality. **Journal of Privacy and Confidentiality**, v. 6, n. 2, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305312. Acesso em: 16 abr. 2024.

BELHUMEUR, Peter N.; HESPANHA, Joao P.; KRIEGMAN, David J. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 19, n. 7, p. 711-720, jul. 1997. Disponível em: https://cseweb.ucsd.edu/classes/wi14/cse152-a/fisherface-pami97.pdf. Acesso em: 15 abr. 2024.

BIG BROTHER WATCH. Face Off: The lawless growth of facial recognition in UK policing. **Big Brother Watch**, 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 15 abr. 2024.

BLACKBURN, Duane M.; BONE, Mike; PHILLIPS, P. Jonathon. **Face Recognition Vendor Test 2000**: Evaluation Report. Defense Advanced Research Projects Agency. National Institute of Justice, 2001.

BLEDSOE, Woodrow Wilson. **Proposal for a Study to Determine the Feasibility of a Simplified Face Recognition Machine**. Panoramic Research Inc. Palo Alto, California, 1963. Disponível em: https://archive.org/details/firstfacialrecognitionresearch/FirstReport/page/n5/mode/2up. Acesso em: 15 abr. 2024.

BLEDSOE, Woodrow Wilson; CHAN, Helen. **A Man-Machine Facial Recognition System-Some Preliminary Results**. Technical Report PRI 19A. Panoramic Research, Inc. Palo Alto: California, 1965.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRANDÃO, Rodrigo. Tecnologias de reconhecimento facial na administração pública brasileira: Desafios técnicos e sociais para o uso responsável da tecnologia. *In*: DUARTE, Daniel Edler; CEIA, Eleonora Mesquita (org.). **Tecnologia, Segurança e Direitos**: os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022, p. 115-140.

BRASIL. Conselho Nacional de Justiça. **Relatório Analítico Propositivo**. Justiça Pesquisa. Direitos e Garantias Fundamentais Audiência de Custódia, Prisão Provisória e Medidas Cautelares: Obstáculos Institucionais e Ideológicos à Efetivação da Liberdade como Regra. Distrito Federal: CNJ, Poder Judiciário, 2018.

BRASIL. **Constituição da República Federativa do Brasil**. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 abr. 2024.

CODING RIGHTS. Parlamentares de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos. **Coding Rights**, 21 de junho de 2022. Disponível em: https://codingrights.org/project-item/parlamentares-de-todas-as-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do-reconhecimento-facial-em-espacos-publicos/. Acesso em: 30 abr. 2024.

DAL MAGRO, Diogo. Riscos jurídicos de tecnologias de reconhecimento facial na segurança pública para a democracia brasileira. 192fls. 2022. Dissertação (Mestrado em Direito). Faculdade IMED. Passo Fundo, 2022.

DESHPANDE, Mohit. Face Recognition with Eigenfaces – Computer Vision Tutorial. **ZENVA**, 30 de novembro de 2023. Disponível em: https://gamedevacademy.org/face-recognition-with-eigenfaces/. Acesso em: 17 abr. 2024.

DINIZ, Fabio Abrantes; MENDES NETO, Francisco Milton; LIMA JÚNIOR, Francisco das Chagas Lima Júnior; FONTES, Laysa Mabel Oliveira. RedFace: um sistema de reconhecimento facial baseado em técnicas de análise de componentes principais e autofaces. **Revista Brasileira de Computação Aplicada**, v. 5, n. 1, 2013. Disponível em: https://seer.upf.br/index.php/rbca/article/view/2627. Acesso em: 17 abr. 2024.

DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel. **Estudos sobre Proteção de Dados Pessoais**. São Paulo: Expressa, 2022.

FALCÃO, Cintia. A ascensão do tecnoautoritarismo. Parte 4. **The Intercept Brasil**, 20 de setembro de 2021. 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: 30 abr. 2024.

FUSSEY, Pete; MURRAY, Daragh**. Independent report on the London Metropolitan Police Service's trial of live facial recognition technology**. Human Rights Centre – University of Essex. The Human Rights, Big Data and Technology Project, 2019. Disponível em: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf. Acesso em: 20 abr. 2024.

GEORGETOWN LAW. **The Perpetual Line-up**. Unregulated Face Recognition in America. 2016. Disponível em: https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf Acesso em 15 de jul. 2024.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT)** – Part 3: Demographic Effects. U.S. Department of Commerce, National Institute of Standards and Technology, 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 15 abr. 2024.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test (FRVT)** – Part 2: Identification. U.S. Department of Commerce, National Institute of Standards and Technology, 2018. Disponível em: https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf. Acesso em: 15 de jul. 2024.

HAN, Byung Chul. **Infocracia**: Digitalização e a crise da democracia. Tradução de Gabriel S. Philipson. Petrópolis: Vozes, 2022.

HISTORYOFINFORMATION. **Woodrow Bledsoe Originates Automated Facial Recognition**. [S.l.]: [s.d.]. Disponível em: https://www.historyofinformation.com/detail.php?entryid=2495. Acesso em: 30 abr. 2024.

HUANG, Gary B.; RAMESH, Manu; BERG, Tamara; LEARNED-MILLER, Erik. **Labeled Faces in the Wild**: A Database for Studying Face Recognition in Unconstrained Environments. [S.l.]: [s.d.]. Disponível em: https://cs.brown.edu/courses/cs143/2011/proj4/papers/lfw.pdf. Acesso em: 16 abr. 2024.

HUREL, Louise Marie. Reconhecimento facial: regular, banir ou punir? **Insight Inteligência**, Rio de Janeiro, v. XXI, n. 84, p. 112-118, jan./fev./mar. 2019. Disponível em: https://insightinteligencia.com.br/pdfs/84.pdf. Acesso em: 16 abr. 2024.

INSTITUTO IGARAPÉ. Reconhecimento Facial no Brasil. Rio de Janeiro, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 15 abr. 2024.

KANADE, Takeo. Picture processing system by computer complex and recognition of human faces. **Department of Information Science**, Kyoto University, 1973. Disponível em: https://www.ri.cmu.edu/pub_files/pub3/kanade_takeo_1973_1/kanade_takeo_1973_1.pdf. Acesso em: 15 abr. 2024.

NUNES, Pablo. **Um Rio de câmeras com olhos seletivos**: uso de reconhecimento facial pela polícia fluminense. Rio de Janeiro: CESeC, 2022. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 19 abr. 2024.

RAVIV, Shaun. The Secret History of Facial Recognition. **Wired**, 21 de janeiro de 2020. Disponível em: https://www.wired.com/story/secret-history-facial-recognition/. Acesso em: 15 abr. 2024.

ROBINSON, Martin. Hundreds of innocents face being grabbed in the street by police as Scotland Yard admits new facial recognition system gives false alerts one in every thousand faces — as it introduces cameras to spot criminals in London's busiest public places. **Daily Mail**, 24 de janeiro de 2020. Disponível em: https://www.dailymail.co.uk/news/article-7924733/Scotland-Yard-introduces-facial-recognition-cameras-hunt-watchlist-2-500-suspects.html. Acesso em: 20 abr. 2024.

SANTOS, Lucas Gabriel de Matos; COSTA, Arthur Barbosa da; DAVID, Jessica da Silva; PEDRO, Rosa Maria Leite Ribeiro. Reconhecimento facial: tecnologia, racismo e construção de mundos possíveis. **Psicologia & Sociedade**, Rio de Janeiro, v. 35, 2023. Disponível em: https://www.scielo.br/j/psoc/a/wJFV8yjBBr7cYnm3q6SXDjF/#. Acesso em: 16 abr. 2024.

SIROVICH, Lawrence; KIRBY, M. Low-dimensional procedure for the characterization of human faces. 1986. **Journal of the Optical Society of America A**, v. 4, n. 3, p. 519-524,

1987. Disponível em: https://www.face-rec.org/interesting-papers/General/ld.pdf. Acesso em: 15 abr. 2024.

SOARES, Nicolau. Reconhecimento facial na segurança pública é "nova aposta no encarceramento", diz especialista. **Brasil de Fato**, 29 de junho de 2022. Disponível em: https://www.brasildefato.com.br/2022/06/29/reconhecimento-facial-na-seguranca-publica-e-nova-aposta-no-encarceramento-diz-especialista. Acesso em: 15 abr. 2024.

TURK, Matthew; PENTLAND, Alex. Eigenfaces for Recognition. **Journal of Cognitive Neuroscience**, Massachusetts Institute of Technology, v. 3, n. 1, 1991. Disponível em: https://www.face-rec.org/algorithms/PCA/jcn.pdf. Acesso em: 15 abr. 2024.

VIOLA, Paul; JONES, Michael. Rapid Object Detection using a Boosted Cascade of Simple Features. **Conference on Computer Vision and Pattern Recognition**. 2001. Disponível em: https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf. Acesso em: 15 abr. 2024.

WELINDER, Yana. A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. **Harvard Journal of Law and Technology**, v. 26, n. 1, 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2109108. Acesso em: 19 abr. 2024.

COMO CITAR

FREITAS, Cinthia Obladen de Almeida; SOUSA, Devilson da Rocha; NORA, Heloísa Daniela. A aplicação da tecnologia de reconhecimento facial na segurança pública brasileira e seus desafios. **Revista Direito e Política**. Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, vº 20, nº3, 3º quadrimestre de 2025. Disponível em: https://periodicos.univali.br/index.php/rdp - ISSN 1980-7791. DOI: https://doi.org/10.14210/rdp.v20n3.p563-591

SOBRE OS AUTORES:

Cinthia Obladen de Almeida Freitas
Mestre em Engenharia Elétrica e Informática Industrial pela Universidade Tecnológica Federal do Paraná (1990) e Doutora em Informática pela Pontifícia Universidade Católica do Paraná (2001). Professora Titular do Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Membro da Comissão de Direito Digital e Proteção de Dados da OAB/PR. Membro da Diretoria do Instituto Nacional de Proteção de Dados (INPD).

Devilson da Rocha Sousa
Doutorando em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR) com bolsa CAPES. Mestre em Direito Constitucional Contemporâneo pela Universidade de Santa Cruz do Sul (UNISC) com bolsa/taxa CAPES, modalidade II e Mestre em Direito da União Europeia pela Universidade do Minho (UMINHO) - Portugal. Especialista em Direito Constitucional e em Direito Público. Graduado pelo Centro Universitário Franciscano do Paraná (FAE) 2017. Pesquisador nas áreas de Ciência Política, Direito Constitucional e Novas Tecnologias. Advogado.

Heloísa Daniela Nora
Mestranda pelo Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Paraná (PUCPR), bolsista CAPES

Received: 07/07/2025
Approved: 11/11/2025

Recebido em: 07/07/2025
Aprovado em: 11/11/2025