UNIVERSIDADE DO ESTADO DA BAHIA – UNEB
DEPARTAMENTO DE EDUCAÇÃO – DEDC – *CAMPUS* VIII
CURSO DE BACHARELADO EM DIREITO

RAFAELA DAYLANE DE OLIVEIRA DA SILVA

REGULAMENTAÇÃO DO RECONHECIMENTO FACIAL NO BRASIL:

Aspectos legais para a proteção de dados biométricos

PAULO AFONSO

2025

RAFAELA DAYLANE DE OLIVEIRA DA SILVA

Regulamentação do reconhecimento facial no Brasil:

Aspectos legais para a proteção de dados biométricos

Trabalho de Conclusão de Curso – TCC apresentado à Universidade do Estado da Bahia (UNEB) como pré-requisito parcial para a conclusão do Curso de Bacharelado em Direito.

Orientador: Dr. Ivandro Pinto de Menezes

PAULO AFONSO

2025

DECLARAÇÃO DE AUTORIA

Eu, Rafaela Daylane de Oliveira da Silva, declaro para os devidos fins que o Trabalho Monográfico, intitulado "**Regulamentação do reconhecimento facial no Brasil:** Aspectos legais para a proteção de dados biométricos" é de minha autoria e está a Universidade Estadual da Bahia - Campus VIII - Paulo Afonso - BA, autorizada a divulgá-lo, mantendo cópia na biblioteca, sem ônus referente a direitos autorais, por se tratar de exigência para conclusão do Curso de Bacharelado em Direito. Saliento também que a cópia total ou parcial deste trabalho pode ser efetivada desde que citada a fonte e a autoria.

Paulo Afonso/BA, 19 de março de 2025.

_____

RAFAELA DAYLANE DE OLIVEIRA DA SILVA

RAFAELA DAYLANE DE OLIVEIRA DA SILVA

REGULAMENTAÇÃO DO RECONHECIMENTO FACIAL NO BRASIL:

Aspectos legais para a proteção de dados biométricos

Trabalho de Conclusão de Curso apresentado ao Colegiado do Curso de Bacharelado em Direito, da Universidade do Estado da Bahia – *Campus* VIII, como parte dos requisitos à obtenção do título de Bacharel(a) em Direito.

Aprovada em 19 de Março de 2025.

BANCA EXAMINADORA

_____

Dr. Ivandro Pinto de Menezes

Orientador

_____

Me. Carlos Henrique Alves Limeira

Examinador

_____

Me. José Ivaldo de Brito Ferreira

Examinador

Dedico este trabalho àqueles que, com paciência e sabedoria, me guiaram e apoiaram nesta jornada, sempre me desafiando a ir além do que eu pensava ser possível.

AGRADECIMENTOS

Agradeço, primeiramente, à Deus e pelo dom da vida, que me permitiu chegar até aqui e finalizar essa monografia.

Agradeço ao professor Dr. Ivandro Menezes por ter aceitado ser meu orientador, pela paciência e compreensão.

Agradeço à minha família materna e paterna, pelo suporte diário desde o início da graduação até aqui. Vocês foram essenciais em todas as etapas da graduação. Serei eternamente grata por ter vocês comigo.

Agradeço à Lucas Figueiredo, por ter sido meu apoio desde a escolha do tema do meu TCC até sua finalização. Obrigada por ter contribuído tanto com seu conhecimento em Direito Digital, pelo suporte emocional e pela motivação para que eu concluísse.

Agradeço à Igor Vitorino, amigo e ex aluno do curso de Direito da UNEB. Por todos os momentos de troca diária, conversas, conselhos, apoio e suporte durante a construção desse trabalho.

Agradeço à Paulo Roberto, meu amigo e colega de turma da faculdade. Pelo apoio, conversas, motivação e suporte durante a faculdade até a conclusão da graduação.

Agradeço às minhas amigas Raiane Timóteo e Nathalya Mariana, por terem sido meu apoio emocional durante a faculdade e construção deste trabalho. Vocês fizeram com que essa jornada fosse menos árdua.

Agradeço à Elton Oliveira, amigo, por todo apoio recebido, motivação e admiração ao escutar sobre meu tema e discussões importantes.

Agradeço a todos que contribuíram, de alguma forma, com esse trabalho.

"Sempre considerei as ações dos homens como as melhores intérpretes dos seus pensamentos."

(John Locke)

RESUMO

Diante dos desafios e riscos inerentes na proteção de dados biométricos, a regulamentação do reconhecimento facial no Brasil torna-se necessária, bem como sugestões de diretrizes para equilibrar inovação tecnológica e proteção de direitos fundamentais. A ausência de normas específicas pode gerar violações de direitos fundamentais, como a privacidade e a não discriminação. Nesse cenário, este estudo tem como objetivo geral avaliar e propor diretrizes para uma regulamentação adequada do reconhecimento facial no Brasil. Para tanto, são examinados os aspectos legais, sociais e éticos da tecnologia, com ênfase na sua relação com a Lei Geral de Proteção de Dados, bem como uma análise do panorama da regulamentação internacional. A metodologia adotada inclui pesquisa bibliográfica, documental, descritiva e exploratória, envolvendo a consulta de doutrinas, artigos científicos, teses, legislações e relatórios técnicos. Os resultados demonstram que a falta de regulamentação específica para o reconhecimento facial no Brasil representa um risco significativo para os direitos dos cidadãos, podendo levar a abusos e discriminação algorítmica. Conclui-se que é essencial a criação de um arcabouço normativo que garanta a transparência no uso da tecnologia, mitigue vieses discriminatórios e assegure a proteção de dados biométricos, alinhando-se às melhores práticas internacionais e aos princípios da LGPD.

Palavras-chave: Reconhecimento Facial. Proteção de Dados. Regulamentação. Privacidade. Discriminação Algorítmica.

ABSTRACT

Given the challenges and risks related to the protection of biometric data, the regulation of facial recognition in Brazil becomes necessary, as well as suggestions for guidelines to balance technological innovation and the protection of fundamental rights. The absence of specific regulations can lead to transparency of fundamental rights, such as privacy and non-discrimination. In this scenario, this study has the general objective of evaluating and proposing guidelines for the adequate regulation of facial recognition in Brazil. To this end, the legal, social and ethical aspects of the technology are examined, with an emphasis on its relationship with the General Data Protection Law, as well as an analysis of the international regulatory landscape. The methodology adopted includes bibliographic, documentary, descriptive and exploratory research, involving the consultation of doctrines, scientific articles, theses, legislation and technical reports. The results demonstrate that the lack of specific regulation for facial recognition in Brazil represents a significant risk to the rights of citizens, and may lead to abuse and algorithmic discrimination. It is concluded that it is essential to create a regulatory framework that guarantees transparency in the use of technology, mitigates discriminatory biases and ensures the protection of biometric data, in line with international best practices and the principles of the LGPD.

Keywords: Facial Recognition. Data Protection. Regulation. Privacy. Algorithmic Discrimination.

SUMÁRIO

1. INTRODUÇÃO

Os avanços tecnológicos, inclusive da Inteligência Artificial, trouxeram novas ferramentas para identificação e controle social, a exemplo do reconhecimento facial. Esta tecnologia tem sido utilizada de forma ampla em setores públicos e privados e tem gerado debates sobre sua legalidade, segurança e impactos sobre os direitos fundamentais, especialmente no que se refere à privacidade e à proteção de dados pessoais. No Brasil, o uso crescente desta tecnologia levanta questões jurídicas relevantes, especialmente no que diz respeito à proteção de dados biométricos, que são informações sensíveis conforme a Lei Geral de Proteção de Dados.

Diante desse cenário, este trabalho tem como tema a regulamentação do reconhecimento facial no Brasil, com foco nos aspectos legais para a proteção de dados biométricos. Trata-se de um estudo inserido no campo do Direito, mais especificamente na área do Direito Digital e da Proteção de Dados Pessoais, com abordagem interdisciplinar, considerando também aspectos da área da Tecnologia da Informação, computação e direitos fundamentais.

O problema de pesquisa que norteia este estudo é: quais são os desafios e as possíveis soluções jurídicas para regulamentar o reconhecimento facial no Brasil, garantindo a proteção de dados biométricos e dos direitos fundamentais? A hipótese levantada é que a ausência de uma regulamentação específica gera riscos à privacidade e pode levar ao uso indiscriminado da tecnologia, tornando essencial a criação de diretrizes normativas que assegurem transparência, consentimento informado e fiscalização adequada.

O objetivo geral deste estudo é avaliar e propor diretrizes para uma regulamentação adequada do reconhecimento facial no Brasil. Para alcançar esse objetivo, foi estabelecido os seguintes objetivos específicos: contextualizar o uso da tecnologia de reconhecimento facial e sua base tecnológica, abordando conceitos como algoritmos, inteligência artificial e aprendizado de máquina, a fim de fornecer suporte técnico à análise jurídica; Avaliar as lacunas jurídicas relacionadas ao uso do reconhecimento facial no Brasil, com foco na proteção de dados biométricos e nos direitos fundamentais, à luz das normas de proteção de dados existentes.; Identificar os riscos e controvérsias associados ao uso do reconhecimento facial, como viés algorítmico, vigilância em massa e impactos sobre direitos fundamentais; Analisar e

relacionar as normas de proteção de dados existentes no Brasil e no cenário internacional, examinando a LGPD e outras legislações aplicáveis, além de realizar um comparativo com regulamentações internacionais; Propor diretrizes para a regulamentação do reconhecimento facial no Brasil, a fim de equilibrar inovação tecnológica e proteção dos direitos individuais.

Visando alcançar os objetivos traçados, adotou-se um misto das metodologias de pesquisa bibliográfica, documental, descritiva e exploratória, por meio da consulta de artigos científicos, teses, bases de dados acadêmicos, legislações e outras publicações relevantes. Essa abordagem metodológica se mostra essencial para embasar as discussões, análises e conclusões deste estudo, permitindo uma compreensão aprofundada sobre os aspectos legais da regulamentação do reconhecimento facial e a proteção dos dados biométricos.

A pesquisa se justifica pela relevância do tema na atualidade pela crescente implementação do reconhecimento facial sem diretrizes claras, o que pode gerar violações de direitos fundamentais, comprometendo o direito à privacidade, previsto no art. 5º, inciso X da Constituição Federal e a proteção de dados no inciso LXXIX. Além disso, a nível internacional, a União Europeia e os Estados Unidos têm debatido e implementado regulações mais rígidas, enquanto o Brasil ainda discute a necessidade de um modelo regulatório eficaz. Dessa forma, este trabalho busca contribuir para o debate acadêmico e jurídico ao analisar os desafios da tecnologia e sugerir diretrizes para uma regulamentação que equilibre segurança e direitos fundamentais.

O reconhecimento facial é uma ferramenta de identificação biométrica baseada em características faciais individuais, que são consideradas dados sensíveis de acordo com a Lei Geral de Proteção de Dados Pessoais (Brasil, 2018). Apesar do uso envolver dados biométricos, a tecnologia oferece benefícios significativos, como possíveis melhorias na segurança pública e a facilitação da autenticação digital. Entretanto, sua utilização indiscriminada sem critérios normativos claros, pode levar a consequências graves. Neste sentido, entre os principais desafios desse sistema então a coleta massiva de dados sem consentimento, o risco de viés algorítmico que pode gerar discriminação racial e social e a possibilidade de vigilância em massa por parte do Estado e empresas privadas (Buolamwini; Gebru, 2018).

Diante desse cenário, este trabalho busca analisar a necessidade de regulamentação do reconhecimento facial no Brasil, discutindo os desafios e propondo

sugestões para a proteção de dados biométricos. Para isso, são examinados os avanços tecnológicos que permitiram o desenvolvimento dessa ferramenta, os riscos e impactos decorrentes do seu uso, e a abordagem adotada em outros países. Além disso, são analisados os princípios e diretrizes da LGPD e sua aplicabilidade ao reconhecimento facial, bem como os Projetos de Lei em tramitação no Congresso Nacional.

Para uma maior exploração do tema, este trabalho dividiu-se em quatro capítulos. O primeiro abordou o contexto histórico do reconhecimento facial, iniciando com as primeiras pesquisas entre 1960 e 1990 e o avanço das técnicas neste período, assim como os avanços tecnológicos do Big Data, Inteligência Artificial e sua relevância nessa discussão. O reconhecimento facial passou por diversas evoluções desde as primeiras pesquisas. Pioneiros como Woody Bledsoe, Helen Chan Wolf e Charles Bisson desenvolveram sistemas baseados em medições faciais, entretanto, enfrentaram desafios como as variações de iluminação e expressão facial. Na década de 1970, Takeo Kanade introduziu um modelo automatizado em 3D, enquanto, nos anos 1980 e 1990, técnicas como Eigenfaces (PCA) e Fisherfaces (LDA) aprimoraram a precisão da tecnologia. Nos anos 1990, o governo dos EUA investiu na pesquisa e aplicabilidade do reconhecimento facial, impulsionando o desenvolvimento de bancos de dados mais robustos e variados.

Em seguida, entre 2000 e 2020, avanços tecnológicos como Big Data e IA transformaram a tecnologia, permitindo maior precisão e escalabilidade. O Big Data possibilitou o armazenamento massivo de imagens faciais, enquanto a IA, com redes neurais e Deep Learning, aprimorou a identificação e reconhecimento em diferentes condições. Esses avanços colaboraram para que o reconhecimento facial se tornasse uma ferramenta amplamente aplicada em segurança, vigilância e autenticação, mas também levantaram questões sobre privacidade e regulamentação, tema central deste estudo.

No capítulo seguinte, apresentou-se os fundamentos da tecnologia de reconhecimento facial, exemplos concretos de aplicações da ferramenta, áreas onde é utilizada, relação direta entre a tecnologia e os dados biométricos, e os principais desafios decorrentes do uso da tecnologia, como o viés discriminatório do algoritmo e a vigilância em massa. Neste capítulo, o objetivo foi abordar sobre o funcionamento da biometria facial de modo mais detalhado com uso dos dados biométricos para colaborar com a compreensão do tema e para entender as implicações na sociedade.

No último capítulo, houve um olhar voltado para os aspectos legais da regulamentação, incluindo uma seção dedicada também ao panorama da regulamentação internacional, tendo em vista que ainda não há um consenso mundial sobre a tecnologia e os impactos aos direitos fundamentais. Por isso, foi importante analisar o cenário internacional, pensando também em possíveis ‘’modelos’’ ou ‘’exemplos’’ que podem ser discutidos e aplicados no Brasil, levando em consideração as particularidades do contexto brasileiro. Buscou-se também apresentar e realizar uma análise dos Projetos de Lei que abordam o reconhecimento facial em seu texto, de modo a contribuir com sugestões para a regulação.

Ao longo do desenvolvimento deste trabalho, busca-se demonstrar que a ausência de regulamentação específica para o reconhecimento facial no Brasil representa um risco significativo para os direitos fundamentais dos cidadãos. A partir dessa análise fundamentada nos casos concretos apresentados, na argumentação baseada em pesquisas de autores renomados sobre os sistemas de identificação facial, são apresentadas sugestões para um modelo normativo que contemple o equilíbrio entre direitos e tecnologia, transparência quanto ao uso, a mitigação de vieses discriminatórios e a garantia da proteção de dados biométricos, alinhando-se às melhores práticas internacionais e aos princípios estabelecidos pela LGPD.

2. CONTEXTO HISTÓRICO DO RECONHECIMENTO FACIAL

A evolução da tecnologia proporcionou inúmeras mudanças no mundo todo e no que diz respeito ao reconhecimento facial, não seria diferente. Tratando-se de uma técnica que identifica as pessoas através do seu rosto, tem sido amplamente utilizada em diversos setores, tanto na esfera pública quanto no setor privado.

Sendo assim, tendo em vista que o desenvolvimento desse sistema não é atual, é importante analisar sua cronologia, etapas e avanços do seu surgimento, levando em consideração os motivos que provocaram o nascimento dessa tecnologia, os desafios e implicações do uso do reconhecimento facial na sociedade e no caso deste trabalho, a necessidade de regulamentação e a proteção de dados pessoais.

2.1. Primeiras pesquisas nos anos 1960 e 1990

O reconhecimento facial é uma tecnologia cuja origem foi motivada pela identificação de rostos entre as décadas de 1960 e 1990. Segundo Li e Jain (2005), entre as décadas de 1960 e 1970, Woody Bledsoe, Helen Chan Wolf e Charles Bisson foram alguns dos pioneiros na pesquisa sobre reconhecimento facial. Eles criaram sistemas que utilizavam medições como a distância entre os olhos, o comprimento do nariz e o formato do maxilar, comparando esses dados com imagens armazenadas em um banco. Apesar das primeiras técnicas terem sido muito dependentes de intervenção humana, essas abordagens iniciais estabeleceram a base para a automação do reconhecimento facial.

Conforme mencionado por Woodrow Wilson Bledsoe em seus primeiros estudos, ele desenvolveu um programa de computador em 1966, no qual manuseava as dimensões do rosto, como por exemplo, os olhos, nariz, orelha, para ajudar na categorização manual das fotos (Bledsoe, 1966). Entretanto, ele se deparou com alguns empecilhos que dificultavam o reconhecimento facial, como destaca Noé (2021, p. 17):

> [...] neste estudo, Bledsoe foi capaz de evidenciar diferentes problemas que são recorrentes até hoje no reconhecimento facial como: variabilidade de rotação e inclinação da cabeça, intensidade e ângulo de iluminação, expressão facial e envelhecimento.

Posteriormente, em 1973, o pesquisador japonês Takeo Kanade na sua tese de doutorado, desenvolveu um sistema automático que não necessitava de intervenção humana e baseado em um modelo 3D, que reconhecia os rostos e processava a semelhança com aqueles presentes no banco de dados (Kanade, 1973).

Em 1987, os pesquisadores Kirby e Sirovich publicaram um trabalho que tinha como objetivo a utilização da técnica de eigenfaces, baseada na análise de componentes principais (PCA). Basicamente, este procedimento reduz a dimensionalidade das imagens com foco no reconhecimento dos rostos, pois este é o intuito do PCA, a identificação ou extração de padrões variáveis, tornando assim o reconhecimento facial eficiente (Kirby; Sirovich, 1987). Segundo eles, há algumas etapas neste procedimento que consiste em: 1) coleta de dados (imagens que são coletadas), 2) cálculo da média dessas imagens, 3) centralização das imagens, 4) matriz da covariância, 5) cálculo dos autovetores e autovalores e por fim, 6) projeção das imagens.

Em 1991, os pesquisadores Matthew Turk e Alex Pentland aprimoraram o método chamado ‘’Eigenfaces’’, no qual era utilizada uma técnica de Análise de Componentes Principais (PCA), cujo objetivo era separar as fisionomias em elementos essenciais (Turk; Pentland, 1991). A introdução da análise de componentes principais (*Principal Component Analysis* - PCA) representou um marco no campo. Esse método permitiu a redução da complexidade dos dados faciais ao identificar padrões estatísticos em imagens (Turk; Pentland, 1991). A técnica conhecida como *Eigenfaces* tornou o reconhecimento facial mais eficiente e viável, superando limitações anteriores e possibilitando avanços significativos em aplicações práticas.

Logo em seguida, em 1996, colaboradores do governo dos EUA adotaram o reconhecimento facial como um atributo biométrico não agressivo que poderia ser empregado na identificação e localização de pessoas sem a necessidade de sua presença física (Phillips *et al.*, 2000). O algoritmo fisherfaces foi desenvolvido em 1997 pelos pesquisadores Belhumeur, Hespanha e Kriegman. Diferentemente do Eigenfaces, o fisherfaces faz uso da técnica LDA, que assim como o PCA, também reduz a dimensionalidade dos dados (Bissi, 2018).

De acordo com Belhumeur, Hespanha e Kriegman (1997), o fisherfaces possui uma evolução em relação ao algoritmo eigenfaces porque ele extrai componentes principais que separam os indivíduos uns dos outros, sem levar tanto em consideração a iluminação e com foco nas características únicas das pessoas. Corrobora com a explicação dos pesquisadores o que foi mencionado pela Saini (s.d.), ao destacar que o algoritmo eigenfaces não considera como importante todas as partes do rosto, levar em consideração o fator iluminação nesse processo, mantendo os componentes principais e descartando o restante.

Conforme relatado por Raji e Fried (2021), em 1996 foi criado um programa pelo Departamento de Defesa dos EUA e pelo Instituto Nacional de Padrões e Tecnologia (NIST), intitulado FERET (Tecnologia de Reconhecimento Facial), no qual foi investido US$ 6.5 dólares para aperfeiçoar a tecnologia de reconhecimento facial. No começo, havia 2.413 imagens no banco de dados, obtidas a partir de um ensaio fotográfico. Posteriormente, passou-se a ter 14.126 correspondentes a 1.119 pessoas, obtidas através do consentimento de cada um deles (Embratel, 2021).

Embora os avanços tenham sido significativos nessa época, desafios técnicos ainda persistiam. Problemas como baixa resolução de imagens, condições de iluminação inadequadas e variações nas expressões faciais limitavam a eficácia dos sistemas (Jain; Li, 2005). Além disso, a ausência de padronização nos métodos de captura e processamento de dados restringia o uso da tecnologia a ambientes controlados. Essas limitações demonstraram a necessidade de pesquisas contínuas e do aprimoramento de métodos complementares.

Nos anos 2000 surgiu a demanda por mais dados para pesquisas acadêmicas e comerciais, o que acabou provocando o surgimento de novos bancos de dados (Embratel, 2021). De acordo com Raji e Fried (2021), a coleta desses dados (imagens) incluía metadados, como por exemplo, idade, etnia e informações acerca da iluminação. Assim, levando em consideração o desafio de configurar e otimizar sistemas de acordo com o ambiente real, tornou-se necessário a busca por bancos de dados mais diversificados e maiores.

Com o crescente poder computacional e o desenvolvimento de novos algoritmos, a década de 1990 trouxe avanços que tornaram os sistemas de

reconhecimento facial mais precisos. Redes neurais e aprendizado de máquina começaram a ser aplicados, enquanto o armazenamento de dados em larga escala permitiu a construção de bases de dados mais robustas (Brunelli; Poggio, 1993). Nesse período, a tecnologia começou a atrair maior interesse comercial, especialmente em áreas de segurança e vigilância. No geral, o período de 1960 a 1990 foi fundamental para o desenvolvimento do reconhecimento facial como tecnologia moderna. As contribuições dos primeiros pesquisadores e os avanços nos algoritmos estatísticos e computacionais pavimentaram o caminho para inovações futuras, consolidando a base para aplicações amplas e diversificadas que vemos atualmente.

2.2. Avanços tecnológicos: Big Data e Inteligência Artificial

Para abordar o reconhecimento facial, é imprescindível discutir os avanços tecnológicos mais relevantes, como o Big Data e a Inteligência Artificial (IA) que, especialmente entre os anos 2000 e 2020, colaboraram com o aprimoramento em massa e disseminação da tecnologia. Segundo Gupta *et al*., (2014), o Big Data refere-se ao processamento de grandes volumes de dados, sejam eles estruturados ou não estruturados, que são gerados continuamente. Entretanto, o mais relevante não é apenas a quantidade de informações disponíveis, mas a forma como elas são analisadas e utilizadas para extrair insights que possibilitem a tomada de decisões estratégicas e aprimorem a atuação das organizações.

Nesse contexto, o Big Data não só permitiu o armazenamento de grandes volumes de dados e informações, incluindo imagens e dados faciais, como também foi fundamental para o desenvolvimento de sistemas de reconhecimento facial. A IA, por sua vez, contribuiu com o avanço de algoritmos como o machine learning e as redes neurais, permitindo que as máquinas realizassem um mapeamento facial cada vez mais preciso. A interação entre esses dois elementos — o Big Data, que fornece os dados necessários, e a IA, que os processa e analisa — foi decisiva para a evolução do reconhecimento facial, transformando-o de uma fase experimental para uma aplicação em larga escala em diversos setores.

Segundo Mauro (2022), o Big Data facilita a coleta e análise de grandes volumes de dados, possibilitando a geração de informações precisas que são

fundamentais para a criação de modelos preditivos e sistemas de reconhecimento, essenciais para a evolução dos algoritmos de IA aplicados ao reconhecimento facial. A capacidade do Big Data de processar grandes quantidades de dados também impacta diretamente no aprimoramento dos sistemas de identificação facial. Com a disponibilidade de dados mais amplos e diversificados, os algoritmos de IA se tornam mais eficientes, adaptando-se a diferentes condições, como variações de iluminação, ângulos e expressões faciais. Essa melhoria contínua na precisão dos sistemas de reconhecimento facial é crucial para sua aplicabilidade e confiança.

Um exemplo prático de como Big Data é aplicado no reconhecimento facial, é o programa Smart Sampa da Prefeitura de São Paulo. O programa é uma iniciativa voltada para a segurança pública, que vai contar com a instalação de 20 mil câmeras por toda capital em pontos estratégicos, com o objetivo de identificar pessoas em tempo real (Prefeitura Municipal de São Paulo, 2024). Tendo em vista que o sistema de reconhecimento é uma tecnologia que necessita de uma vasta base de dados alimentada, isso demonstra a aplicabilidade e relevância do Big Data na segurança pública.

Além do Big Data, a Inteligência Artificial (IA) é um avanço tecnológico relevante, ao permitir que sistemas e dispositivos aprendam a comparar padrões faciais através de um banco de dados. Vale mencionar que um dos principais componentes da IA aplicados ao reconhecimento facial é o Deep Learning, subárea do machine learning (aprendizado de máquina), que por sua vez faz uso de redes neurais profundas para analisar e processar dados complexos. O Deep Learning se destaca por permitir que redes neurais com múltiplas camadas identifiquem padrões cada vez mais abstratos nos dados, aprimorando a precisão do reconhecimento facial (Goodfellow *et al*., 2016).

As redes neurais artificiais, que são sistemas computacionais inspirados no funcionamento do cérebro humano, são compostas por neurônios artificiais interconectados. Essas redes têm a capacidade de aprender a partir dos dados e ajustar suas conexões internas para melhorar o desempenho em tarefas como reconhecimento de padrões, classificação e previsão, tornando-se uma ferramenta essencial em diversas aplicações da IA (Haykin, 1999).

No caso do reconhecimento facial, as redes neurais são capazes de identificar detalhes sutis e precisos, como a forma da mandíbula, a posição dos olhos e até mesmo as expressões faciais, independentemente de fatores como o ângulo ou a iluminação (Schroff *et al.*, 2015). Essa capacidade das redes neurais garante que os sistemas de reconhecimento facial sejam eficazes e precisos, permitindo sua aplicação em áreas como segurança pública, desbloqueio de celulares e sistemas bancários, identificação de pessoas foragidas etc.

Com o avanço dos métodos de IA, o reconhecimento facial passa a ser utilizado também na análise de comportamentos e previsões futuras, como por exemplo, no caso do metrô de São Paulo, da concessionária ViaQuatro. No episódio em questão, houve uma captação de expressões faciais dos passageiros sem o consentimento, para fins comerciais e publicitários, sendo a prática vedada pela LGPD (Ribas Junior, 2023).

Sendo assim, essa prática possui implicações importantes nas áreas de marketing e segurança, tendo em vista que a IA é utilizada para aperfeiçoar a experiência do usuário e também para a identificação de pessoas suspeitas nos ambientes públicos (LeCun *et al.*, 2015).

No entanto, o uso dos sistemas de identificação facial também traz à tona questões sociais, éticas e legais, especialmente no que diz respeito à coleta de dados sensíveis sem o consentimento explícito dos indivíduos. Esse é um ponto crítico na discussão sobre a regulamentação do reconhecimento facial, especialmente quando se trata da proteção de dados biométricos. No próximo capítulo, serão abordados os principais aspectos do reconhecimento facial, fundamentação tecnológica, funcionamento, a relação com dados biométricos, casos de uso e os desafios éticos e legais envolvendo essa tecnologia.

3. RECONHECIMENTO FACIAL: FUNDAMENTOS, APLICAÇÕES E DESAFIOS

A tecnologia de reconhecimento facial é amplamente utilizada para identificação e autenticação de indivíduos, sendo aplicada em smartphones, câmeras de segurança, policiamento, etc. Seu desenvolvimento remete à década de 1960, quando as primeiras pesquisas foram voltadas para investigações policiais.

Com o desenvolvimento de algoritmos e o aumento da capacidade computacional, o reconhecimento facial tornou-se mais preciso e acessível, ao mesmo tempo em que suscitou debates éticos e sociais. Dessa forma, é importante entender conceitos introdutórios sobre os sistemas de identificação facial, seu funcionamento, aplicações e contextos, assim como os desafios e implicações decorrentes do uso.

3.1. Fundamentação tecnológica: algoritmos, ia e aprendizado de máquina

Na discussão da regulamentação do reconhecimento facial, torna-se necessário apresentar a fundamentação tecnológica, de modo a facilitar a compreensão do tema e o porquê da necessidade de pensar em regulação e clareza no estabelecimento de critérios para o uso dos sistemas de biometria facial. Algoritmo, inteligência artificial e aprendizado de máquina são conceitos ou áreas que estão intrinsecamente relacionados.

Os algoritmos são essenciais para a execução de tarefas e resolução de problemas. De acordo com Shimabukuro e Lima (2024), o algoritmo é um conjunto limitado de preceitos e comandos que servem como embasamento para a aplicação de uma tarefa ou resolução de um problema. Em outras palavras, o algoritmo é uma sequência lógica de passos que orienta a realização de ações específicas. Nas palavras de Turing (1950), os algoritmos são como "sequências finitas de instruções bem definidas, que, ao serem seguidas, levam à solução de um problema computacional específico". Para exemplificar, no cenário atual do reconhecimento facial, os algoritmos desempenham um papel indispensável porque eles são responsáveis por processar as imagens, identificar padrões e associá-los a dados biométricos armazenados em banco de dados.

Neste sentido, Shimabukuro e Lima (2024) destacam que os algoritmos são treinados para receber uma enorme quantidade de informações e, como

consequência, eles são capazes de descobrir tendências, interpretar informações (processar dados) e entender como atingir um objetivo final em cenários diversos.

Um exemplo prático da utilização dessa tecnologia, foi durante o Carnaval de Salvador-BA em 2024, no qual as câmeras foram instaladas nas entradas da festa e nos pontos estratégicos, com foco na identificação de pessoas foragidas (G1 Bahia, 2024). O caso exemplificativo demonstra o potencial da tecnologia no campo da segurança pública, porém, também coloca em risco questões relacionadas à privacidade e a proteção de dados biométricos, devido ao risco de abuso e uso indevido dos dados coletados. Desse modo, ao mesmo tempo que a tecnologia de reconhecimento facial se mostra como uma ferramenta efetiva, evidencia a necessidade de pensar em regras claras para a proteção de direitos fundamentais.

De acordo com Shimabukuro e Lima (2024) os algoritmos são utilizados de forma variada, entretanto, são frequentemente encontrados em implementações da Inteligência Artificial, códigos de programação, ferramentas de busca e mecanismos de filtragem de redes sociais. Em outras palavras, os algoritmos são usados em todas as atividades que as pessoas estão em contato diariamente, seja ao pesquisar uma notícia, uma música, o perfil de alguém nas redes sociais (Facebook, Instagram, Tik Tok etc.), nos deparamos com os algoritmos guiando nossos passos, escolhas e decisões.

Segundo Shimabukuro e Lima (2024), os algoritmos possuem entradas e saídas, juntamente com variáveis e critérios específicos que orientaram os dados conforme os cenários da tarefa. Dito de outro modo, quando uma pessoa está programando, ela escreve linhas de código para atingir um objetivo, como por exemplo, criar um programa que calcule as médias escolares de um aluno, no qual, o desenvolvedor entrará com instruções que solicitarão dados e retornarão com dados, ou melhor, com o objetivo alcançado. No reconhecimento facial, as ‘’entradas’’ podem ser as imagens capturadas, enquanto a ‘’saída’’ seria a identificação ou validação de uma pessoa em um banco de dados.

A IA está crescendo e sendo utilizada com vários objetivos, como por exemplo: inovação, competitividade entre os setores público e privado, disputas entre os centros tecnológicos, entre outros (Bughin, 2017). Sem dúvidas, a inteligência artificial vem sendo cada vez mais utilizada em diversos setores e com propósitos

diferentes, o que reforça a necessidade de discussão sobre as implicações do uso do reconhecimento facial, uma das aplicações da IA.

Embora seja difícil defini-la, a Inteligência Artificial pode ser descrita como um campo do saber que busca criar mecanismos capazes de realizar operações vistas como racionais ou lógicas se fossem desempenhadas por humanos (Russell; Norvig, 2013 *apud* Melo, 2024). Nesse sentido, o processamento computacional da IA é realizado através do machine learning (aprendizado de máquina) - área da computação cujo objetivo é ensinar à máquina o que ela deve fazer - que permitirá ao sistema aprender a partir das informações fornecidas por um ser humano, permitindo seu desenvolvimento (Melo, 2024). No reconhecimento facial, o machine learning é o suporte para o treinamento de modelos que reconheçam padrões faciais de forma precisa.

O uso de redes neurais convolucionais (CNNs) tem se mostrado crucial para a evolução de tecnologias de reconhecimento facial, especialmente devido à sua habilidade de extrair características complexas de imagens. Essas redes são capazes de processar dados visuais em múltiplas camadas, identificando padrões detalhados que são fundamentais para o reconhecimento preciso (Noé, 2021). Estudos de Krizhevsky, Sutskever e Hinton (2012) e de Schroff, Kalenichenko e Philbin (2015) evidenciam que essas redes conseguem identificar características faciais mesmo diante de variações de iluminação, ângulos ou expressões.

Nota-se que apesar da IA ser vista como solucionadora de problemas, ela não pode ser igualada ao ser humano. Inclusive, ‘’é um sistema que necessita de estímulos’’, como mencionado por Melo (2024), e saber disso nos coloca a pensar na responsabilidade de quem treina esses sistemas.

Como ressaltado por Bughin (2017), a IA está crescendo de forma exponencial, sendo utilizada para inovação, competitividade e disputas tecnológicas. Contudo, essa expansão também traz implicações éticas, sociais e econômicas que podem impactar sociedades democráticas, como no caso do reconhecimento facial. Com isso, é preciso analisar as perspectivas e aspectos legais da regulamentação do reconhecimento facial, com foco no panorama da regulamentação internacional e no Brasil, a fim de observar como outros países estão discutindo as tecnologias emergentes e seus impactos.

A fundamentação tecnológica sobre algoritmos, IA, aprendizado de máquina, é essencial para um entendimento básico como um todo das áreas ou termos que fazem parte do desenvolvimento dessa tecnologia. Embora o embasamento técnico não seja o foco deste trabalho, é importante compreender a relação desses campos e definições entre si, para que o leitor consiga se situar e entender os desdobramentos. Diante disso, observa-se a relevância de regulamentações que contemplem as peculiaridades do tratamento de dados biométricos na tecnologia de reconhecimento facial, tendo em vista que a Era Digital proporciona mudanças significativas para a sociedade e que os avanços devem estar alinhados com os princípios da LGPD.

3.2. Reconhecimento facial e dados biométricos

O reconhecimento facial utiliza dados biométricos em seu tratamento, cujo objetivo é reconhecer uma pessoa através das suas características faciais. Contudo, o seu uso apresenta algumas preocupações éticas, legais e sociais, que serão discutidas posteriormente.

Neoway (2021) traz a definição do reconhecimento facial como um sistema utilizado para reconhecer padrões no rosto de uma pessoa. Faz uso de algoritmos e softwares que realizam uma detecção baseada em formas geométricas e algorítmicas, facilitando a diferenciação entre os rostos. Dependendo do uso, os sistemas podem variar, mas o seu funcionamento básico acontece da seguinte forma:

- *Detecção:* seja por meio de foto, vídeo ou câmera de segurança, o sistema vai identificar as características de uma pessoa, como por exemplo, olhos, nariz e boca.
- *Análise:* depois de detectar, será feita uma análise dessas características que são únicas em cada indivíduo: a abertura dos olhos e distância entre eles, o comprimento do nariz, formato dos lábios, orelhas etc.
- *Conversão em dados:* nesta etapa, ocorre uma transformação das características faciais em dados, sendo armazenadas em um banco de dados. Basicamente, há uma transformação do rosto de uma pessoa em uma fórmula matemática, que acaba gerando uma impressão facial.

- *Correspondência:* quando um sistema de reconhecimento facial é utilizado, há um cruzamento de informações da imagem captada com aquelas que já estão armazenadas.

A tecnologia de reconhecimento facial é utilizada em vários setores. Seu uso vai desde o acesso a aplicativos do Governo Federal, desbloqueio de smartphones, controle de acesso à estabelecimentos, estádios de futebol, investigações criminais, câmeras de segurança em espaços públicos, condomínios etc.

Neste sentido, para compreender a importância da proteção de dados, é necessário entender o seu conceito e fatores que exigem esse cuidado. A biometria corresponde às características físicas e comportamentais de cada indivíduo (Ebds, 2023). Basicamente, uma pessoa é identificada de forma única e este procedimento também envolve a íris, face, voz etc.

A LGPD classifica os dados biométricos como dados sensíveis e estabelece que o seu uso deve permanecer igual àquele que foi iniciado. Ou seja, se uma empresa utiliza esses dados para evitar possíveis fraudes, estes não devem ser usados em outras finalidades, exceto se o titular for informado e autorizar (Ebds, 2023).

Sendo assim, o art. 5° da Lei n° 13.709/2018, traz a definição de dados pessoais como uma ‘’informação relacionada à pessoa natural identificada ou identificável’’ (Brasil, 2018). De acordo com Marcondes (2024), são exemplos de dados pessoais: nome, RG, endereço de e-mail, telefone celular etc. A lei também estabelece o conceito de dados sensíveis vinculado a uma pessoa natural, como aqueles dados que indicam origem racial ou étnica, convicção religiosa, filiação em partido político, dado genético ou biométrico etc (Brasil, 2018).

A discussão em torno da tecnologia de reconhecimento facial envolve dados biométricos, que também são considerados sensíveis. Desta forma, o seu uso implica necessariamente em proteger esses dados e lidar com os desafios éticos e legais. Ao levarmos em consideração que a LGPD estabelece diretrizes e princípios, é de extrema importância analisar a sua relevância.

A Lei Geral de Proteção de Dados Pessoais, influenciada pela GDPR (Regulamento Geral da Proteção de Dados), entrou em vigor em 18 de setembro de

2020 (Serpro, 2020). Tanto a LGPD quanto a GDPR têm em comum a adoção de princípios semelhantes, como a necessidade, a transparência e a finalidade, que regulam o tratamento de dados pessoais, com o objetivo único de proteger os dados pessoais em um mundo cada vez mais digitalizado e possibilitar a responsabilização daqueles que realizam operações de tratamento dos dados.

O conceito de dado pessoal, presente no art. 5°, inciso I da LGPD abrange toda ‘’informação relacionada a pessoa natural ou identificável’’ (Brasil, 2018). Em seguida, observa-se que esse conceito é ampliado no art. 5°, inciso II, com o conceito de dado sensível sendo estabelecido como ‘’dado pessoal de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural’’ (Brasil, 2018).

Os dados biométricos são considerados dados sensíveis e recebem um tratamento especial da legislação por tratar-se de dados que representam a identidade única do indivíduo. Nesse sentido, é importante destacar que o reconhecimento facial é uma tecnologia que realiza o processamento de dados biométricos, que exigem cuidados adicionais em decorrência de eventuais impactos em relação aos direitos fundamentais como privacidade e a não discriminação.

Com isso, por se tratar de características únicas dos indivíduos, é importante regulamentar a tecnologia de reconhecimento facial que utiliza esses dados e assim, garantir que direitos fundamentais sejam respeitados e que os riscos sejam mitigados.

Estes são os riscos atrelados ao reconhecimento facial na ausência de regulamentação específica: violações à privacidade das pessoas, uso indevido dos dados, discriminação algorítmica, vigilância em massa e exposição a falhas de segurança.

O uso da tecnologia de reconhecimento facial implica necessariamente em uma operação que trata dados biométricos. Portanto, é importante pensar em diretrizes que possam ajudar na regulamentação desta tecnologia emergente.

O art.6° da LGPD orienta que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os demais princípios (Brasil, 2018). Neste sentido, são princípios estabelecidos em lei: princípio da finalidade, da adequação, da

necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Com isso, é preciso destacar os princípios mais pertinentes ao reconhecimento facial.

De acordo com o princípio da finalidade, art. 6°, inciso I, os tratamentos precisam possuir propósitos legítimos, específicos e que sejam informados ao titular de dados (Brasil, 2018). Assim, a coleta de dados biométricos no contexto do reconhecimento facial, só pode ser realizada se possuir uma finalidade específica, a exemplo da autenticação, segurança pública, sendo proibido o uso discriminação dos dados ou sem o consentimento do indivíduo.

Segundo o princípio da adequação, art. 6°, inciso II, o tratamento será compatível com as finalidades informadas ao titular dos dados (Brasil, 2018). Em outras palavras, o objetivo é evitar que dados coletados para um propósito, sejam utilizados para outras intenções.

Conforme o princípio da necessidade, art. 6°, inciso III, há uma limitação do tratamento de dados ao mínimo necessário, de acordo com sua finalidade, sem excessos (Brasil, 2018). Isto significa que, deve-se evitar o uso imoderado dos dados biométricos nos casos de identificação facial.

Já o princípio da transparência, previsto no art. 6°, inciso VI, impõe que haja clareza de informação e acessibilidade à forma como seus dados estão ou serão tratados (Brasil, 2018). No contexto do reconhecimento facial, as empresas ou órgãos que implementam a tecnologia devem dar acesso às informações acerca da finalidade do uso dos dados, responsáveis pelo tratamento, bem como as medidas de segurança adotadas.

O princípio da segurança, art. 6°, inciso VII, estabelece que é necessária a utilização de medidas técnicas e administrativas para a proteção de dados contra eventuais acessos não autorizados ou situações imprevistas (Brasil, 2018). Ou seja, em sistemas de reconhecimento facial, é preciso que haja uma garantia de proteção de dados biométricos, com o intuito de reduzir os riscos de vazamento de dados ou o seu uso de forma indevida.

Por fim, o princípio da não discriminação, previsto no art. 6°, inciso IX, destaca a impossibilidade de realizar tratamentos de dados com fins discriminatórios (Brasil, 2018). Este é um dos princípios mais relevantes na discussão sobre o uso do

reconhecimento facial, tendo em vista os vieses presentes nos algoritmos, provocando assim, perpetuação de preconceitos existentes na sociedade, afetando minorias étnicas ou raciais.

Os princípios da LGPD servem para orientar o tratamento de dados pessoais, especificamente em questão, dos dados biométricos. Com isso, a legislação procura equilibrar o uso da tecnologia com a garantia de direitos fundamentais, inclusive, ao estabelecer como fundamento a autodeterminação informativa, prevista no art. 2°, inciso I, reforçando o direito de cada indivíduo sobre seus dados pessoais (Brasil, 2018).

Desta forma, sendo o reconhecimento facial uma tecnologia emergente e que também vêm sendo muito aplicada em outros países, torna-se indispensável analisar como outros países estão discutindo e regulamentando, bem como as lições e aprendizados que podem ajudar no cenário brasileiro.

3.3. Casos de uso no Brasil

O reconhecimento facial tem sido implementado no Brasil desde 2011, tanto no setor público, quanto no privado (Instituto Igarapé, s.d.). Sua implementação abrange desde o acesso ao aplicativo GOV (Governo Federal), desbloqueio de smartphones, controle de acesso a estabelecimentos e condomínios, estádios de futebol, investigações criminais, monitoramento por câmeras de segurança em espaços públicos, até o setor de transportes e educação. Todavia, apesar de seu crescimento acelerado, a falta de regulamentação específica gera preocupações quanto à privacidade, transparência quanto ao uso e possíveis violações de direitos fundamentais. A seguir, serão apresentados exemplos práticos do uso da tecnologia, bem como suas implicações.

O maior uso da tecnologia está concentrado na segurança pública, sendo utilizada por forças policiais e órgãos governamentais para monitoramento e identificação de indivíduos. Como menciona Bento (2024), a Bahia é o Estado com maior número de prisões pelo uso da tecnologia implementada em 2019 e desde então, 1.942 foragidos da Justiça foram capturados. Segundo dados da Secretaria de Segurança Pública do Estado, 25% dos identificados eram procurados por crimes de roubo, 21% por homicídios, 13% por tráfico de drogas e 5,7% por estupro.

Em São Paulo, a prefeitura lançou o programa Smart Sampa, que utiliza reconhecimento facial para identificação de foragidos, desaparecidos e suspeitos de crimes como furtos e assaltos (CartaCapital, 2022). No entanto, pesquisadores e instituições ligadas aos Direitos Humanos demonstraram preocupação com o viés discriminatório dos algoritmos e a ausência de consentimento para o uso dos dados coletados.

O reconhecimento facial também vem sendo aplicado nos Estádios de Futebol, pensando na segurança de eventos esportivos. Em parceria com a Secretaria de Segurança Pública de São Paulo, o estádio Allianz Parque adotou a tecnologia no projeto "Muralha Paulista", que já resultou na prisão de 52 foragidos e na identificação de 56 pessoas que descumpriram medidas judiciais (Cnn Brasil, 2024).

O uso segue as instruções previstas na Lei Geral do Esporte, Lei n° 14.597/2023, no qual a biometria facial passará a ser obrigatória em 2025 nos estádios com capacidade para 20 mil pessoas (Nunes e Sousa, 2024). Nesse sentido, a medida tem como objetivo combater a prática de cambismo e também para facilitar a entrada dos torcedores nas catracas.

Um levantamento da revista Consultor Jurídico revelou que, mesmo sem regulamentação, pelo menos quatro estados brasileiros já realizaram mais de 1,7 mil prisões utilizando reconhecimento facial. Além disso, não há transparência quanto à taxa de erros da tecnologia, especialmente no que diz respeito à identificação de pessoas negras e pardas, aumentando o risco de abordagens indevidas e injustas (Tajra, 2024).

No transporte público, o reconhecimento facial também vem sendo utilizado para controle de acesso e combate a fraudes. Na cidade de Ilhéus-Bahia, por exemplo, a tecnologia foi implementada desde 2012 para monitorar o uso de cartões de gratuidade e evitar fraudes (Barbosa Sobrinho *et al.*, 2024). De acordo com levantamento do Instituto Igarapé para identificar os principais setores que começam a empregar o uso do reconhecimento facial, foi visto que a educação, transporte, controle de fronteiras e segurança pública aparecem como as principais áreas de uso.

Ainda na esfera de transporte público, em maio de 2021, a empresa ViaQuatro, responsável pela administração da Linha 4 do Metrô de São Paulo, foi condenada por coletar expressões faciais dos passageiros sem consentimento. O

caso gerou grande repercussão, reforçando a importância de regras mais claras sobre a privacidade dos usuários (Neoway, 2021).

Na Educação, a tecnologia de reconhecimento facial também chegou às escolas brasileiras, gerando tanto benefícios quanto preocupações. O município de Jaboatão dos Guararapes foi pioneiro na implementação do reconhecimento facial na educação pública, adotando a tecnologia para controle de frequência dos alunos. O sistema permite que a presença dos estudantes seja registrada automaticamente por meio da biometria facial, eliminando a necessidade da chamada tradicional. Cinco escolas da rede municipal já utilizam a ferramenta (G1 Pernambuco, 2017).

Mesmo sem regulação, muitos estados continuam prendendo inúmeras pessoas através do uso do reconhecimento facial, é o que aponta o levantamento feito pela revista eletrônica Consultor Jurídico, de acordo com Tajra (2024, p.1):

> [...] nas secretarias estaduais de Segurança mostra que quatro estados brasileiros já prenderam mais de 1,7 mil pessoas utilizando o reconhecimento facial, ainda que não exista uma regulamentação para esse mecanismo. Outros estados informam que usam o sistema, mas não dizem quantas pessoas prenderam usando a tecnologia, e há algumas unidades da federação que ainda estudam a implementação das câmeras para fins policiais.

Os casos apresentados demonstram que o reconhecimento facial já está consolidado em diversas áreas no Brasil, com destaque para a segurança pública. No entanto, o uso da tecnologia ainda ocorre sem uma regulamentação específica, o que gera preocupações quanto à privacidade, à transparência e aos riscos de discriminação algorítmica. Como aponta Tajra (2024), a falta de transparência nos dados dificulta a avaliação da taxa de erros da tecnologia, especialmente em relação à população negra e parda.

Apesar do crescimento acelerado, a ausência de normas claras para a implementação do reconhecimento facial aumenta o risco de violações de direitos fundamentais. Assim, é fundamental que haja uma regulamentação específica, garantindo que o uso da tecnologia ocorra de forma ética, segura e proporcional aos interesses da sociedade.

3.4. Desafios no uso do reconhecimento facial: Viés discriminatório e Vigilância em Massa

A ausência de regulamentação adequada coloca em risco direitos fundamentais, como a privacidade, a liberdade de expressão e a não discriminação, permitindo que sistemas sejam desenvolvidos e aplicados sem transparência e fiscalização. Além disso, o uso de bases de dados com baixa representatividade pode resultar em discriminação algorítmica, enquanto a falta de restrições ao uso dessa tecnologia pelo Estado abre caminho para vigilância em massa e controle social. Diante desses desafios, é essencial compreender as implicações do viés algorítmico e da vigilância em massa - dois dos principais desafios atrelados ao uso da tecnologia - garantindo que a regulamentação acompanhe os avanços tecnológicos sem comprometer liberdades individuais.

O uso da tecnologia para monitorar populações negras dispõe de precedentes históricos, como a "Lei das Lanternas" de 1713, em Nova York, que obrigava pessoas escravizadas com mais de 14 anos a carregar lanternas à noite para serem facilmente identificadas por brancos. Apesar dos avanços tecnológicos, o reconhecimento facial ainda carrega associações com práticas discriminatórias que perpetuam desigualdades sociais (Nkonde, 2019).

Estudos e análises de sistemas de reconhecimento facial das empresas IBM, Microsoft e Face++ (empresa chinesa) demonstraram que sistemas de reconhecimento facial apresentaram maior precisão para homens brancos, porém, taxas de erro significativamente mais altas para mulheres negras, chegando a até 35%, enquanto a precisão para homens brancos é superior a 99% (Buolamwini; Gebru, 2018).

No documentário *Coded Bias* (2020) na Netflix, Joy Buolamwini, uma das principais pesquisadoras da área, percebeu que o software não reconhecia sua face até que ela usasse uma máscara branca, o que evidenciou uma falha crítica: os dados que alimentam esses sistemas são majoritariamente compostos por imagens de rostos brancos e masculinos, o que inviabiliza a identificação precisa de pessoas negras e outros grupos sub-representados. A falta de representatividade nas bases de dados compromete a eficácia e a justiça dos algoritmos e isso pode ser evidenciado

no erro de identificação de figuras públicas como Oprah Winfrey, Michelle Obama e Serena Williams.

Neste sentido, em uma entrevista concedida por Silvana Bahia, diretora executiva do Olabi e cofundadora da PretaLab, à EBC Rádios, ela destaca que a tecnologia não é neutra, pois reflete as escolhas e preconceitos de seus criadores, o que pode levar à perpetuação de desigualdades sociais através de sistemas de inteligência artificial (Ebc, 2020).

No contexto brasileiro, temos alguns casos que mostram na realidade o viés discriminatório e as falhas que ocorrem nos sistemas. Na ocasião de um campeonato de futebol na capital de Aracaju-Sergipe, um jovem foi identificado erroneamente com uma pessoa foragida (CartaCapital, 2022). Após ter sido levado para as acomodações da Polícia Militar e apresentar documentos pessoais, foi constatado que houve uma falha de identificação no sistema.

Outro caso ocorreu na festa de São João em Salvador – Bahia, no ano de 2022, na qual um homem negro também foi identificado como foragido. Neste último caso, o rapaz ainda permaneceu preso por 26 dias. Na época, a Secretaria de Segurança Pública alegou que o sistema detectou 95% de similaridade entre as duas pessoas (CartaCapital, 2022). Na prática, casos como esses reforçam a necessidade de regulamentação, tendo em vista que os danos causados por falhas tecnológicas, não são facilmente reparáveis, mesmo com indenizações morais.

Joy Buolamwini, conforme apontado por Monteiro (2024), reflete sobre o desafio de eliminar vieses em sistemas de inteligência artificial, afirmando que, embora se fale em se livrar dos vieses, isso só seria possível se pudéssemos “nos livrar dos humanos”. Ela argumenta que, como os sistemas de IA são projetados e treinados por pessoas, os preconceitos humanos acabam sendo refletidos nessas tecnologias. Dessa forma, a IA nunca será completamente isenta de vieses, pois ela carrega o valor e as escolhas dos indivíduos que a criam. Buolamwini destaca que o objetivo não deve ser tornar a IA "equalitária", mas, sim, ser mais específicos sobre como reduzir danos, identificar quem se beneficia com a tecnologia e quem sofre as consequências negativas dela.

Na chamada "era da vigilância", como discute Oliveira (2021), a sociedade em massa pode ser compreendida como uma sociedade na qual todos os tipos de

atividades virtuais, sejam as sociais, institucionais, negociais, que possuam alguma relevância, envolvem a coleta e o monitoramento de dados com finalidade decisória, para diminuição de riscos, classificação de grupos sociais e fins de autoridade. De acordo com Zuboff (2020), o capitalismo de vigilância estabelece uma nova forma de poder, no qual poucas empresas detêm o controle sobre amplas quantidades de dados e a capacidade de influenciar a sociedade.

George Orwell em sua obra intitulada "1984", retrata uma sociedade no qual o Estado monitora constantemente seus cidadãos por meio do "Grande Irmão" (Big Brother), um sistema de vigilância totalitário que restringe liberdades individuais (Orwell, 2009). A crescente implementação da tecnologia de reconhecimento facial pode ser vista como um reflexo dessa distopia, tendo em vista que na medida em que amplia o controle estatal, reduz a privacidade dos indivíduos.

O reconhecimento facial, utilizado para vigilância em massa, exemplifica a aplicação contínua dessa tecnologia, sem ou com pouca intervenção humana, o que afeta diretamente a privacidade dos cidadãos (Melo, 2024). No entanto, essa prática tem sido aceita passivamente pela sociedade, muitas vezes sob a ilusão de maior segurança pública, embora a proteção real contra riscos seja incerta e, frequentemente, ineficaz (Rodotà, 2003). Ou seja, na chamada era da vigilância, as pessoas são monitoradas o tempo inteiro e esse monitoramento envolve a coleta de dados pessoais, que agora passam a ser a principal motivação para a concretização da vigilância.

A relação entre segurança e tecnologia tem sido fortalecida, fazendo com que muitas pessoas estejam dispostas a abrir mão de direitos básicos para se sentirem mais protegidas (Melo, 2024). Contudo, como alertam Bauman e Lyon (2013), as novas tecnologias não necessariamente protegem contra ameaças reais, mas sim contra "riscos nebulosos", cuja definição é vaga e subjetiva. Nesse contexto, o crime não desaparece, apenas se desloca para áreas não monitoradas, enquanto a vigilância contínua cria a ilusão de falsa segurança.

Esse cenário remete ao conceito do panóptico, proposto por Jeremy Bentham em 1785 e posteriormente analisado por Michel Foucault (1975), no qual indivíduos não sabem quando estão sendo observados, o que os leva a se comportar como se estivessem sendo vigiados constantemente. O reconhecimento facial representa uma evolução desse modelo, permitindo a supervisão automatizada e

contínua, sem que os indivíduos percebam diretamente o monitoramento (Smanio, 2021). Essa lógica, aplicada à sociedade contemporânea, demonstra como a aceitação da vigilância massiva se tornou um mecanismo de controle social.

A crescente adoção dessas tecnologias levanta debates sobre privacidade, liberdade e poder. Santos (2023) argumenta que a vigilância contínua molda comportamentos e limita a espontaneidade dos cidadãos, tornando-os mais passivos e menos questionadores. Além disso, a coleta e análise de dados biométricos vão além da identificação de pessoas, envolvendo também a interpretação de emoções e expressões faciais, o que amplia as possibilidades de controle e manipulação da população (Rodotà *apud* Oliveira, 2021).

Empresas de tecnologia, por sua vez, exploram esses dados como recursos privados, muitas vezes sem o devido consentimento dos indivíduos, intensificando as preocupações com a privacidade e a autonomia pessoal (Zuboff, 2020).

Outro fator relevante nesse debate é o uso do medo como instrumento de controle. A indústria da segurança e a economia baseada na vigilância alimentam uma sensação permanente de perigo, justificando o monitoramento massivo sob o argumento da proteção pública (Batista, 2016). Nesse contexto, as pessoas acabam cedendo sua privacidade em troca de uma promessa de segurança que, na prática, nem sempre se concretiza (Smanio, 2022).

Aliás, o estado constante de vigilância afeta a liberdade de expressão e o anonimato, especialmente em contextos de protestos e manifestações políticas, como por exemplo, nas manifestações pacíficas de 2020 nos EUA contra o assassinato de George Floyd e a violência racial, onde o FBI empregou o reconhecimento facial para identificar participantes, causando danos duradouros à liberdade dos envolvidos, tanto no momento quanto posteriormente, devido ao medo da coleta de dados sensíveis.

A normalização da vigilância digital representa um risco significativo para a democracia. Han (2018) alerta que essa forma de monitoramento cria uma ilusão de liberdade, quando na verdade possibilita a manipulação psicológica e o controle social. Assim, torna-se essencial discutir e implementar regulamentações eficazes antes que a tecnologia de reconhecimento facial se torne onipresente e irreversível (Hartzog, 2018).

Sem medidas que limitem o uso indiscriminado dessas ferramentas, há o risco de aprofundamento das desigualdades sociais e da restrição das liberdades individuais, impactando diretamente os direitos fundamentais da população (Melo, 2024). Nesse sentido, Lyon (2003) também reforça e alerta que "as tecnologias de vigilância, incluindo o reconhecimento facial, estão cada vez mais sendo utilizadas para monitorar e gerenciar populações, mas sempre há o risco de abusos que comprometem a democracia e os direitos individuais". Esse risco é evidente em aplicações utilizadas para monitorar as pessoas com a justificativa da segurança pública, nos eventos festivos de carnaval etc., que embora demonstrem o potencial de uma tecnologia efetiva, também levantam preocupações sobre vigilância massiva e falta de transparência no uso de dados.

Indo além da limitada coleta de dados, as emoções do ser humano não estão fora da vigilância. Conforme aponta Rodotà, 2003 *apud* Oliveira (2021), as vozes são analisadas para saber se um indivíduo está falando a verdade, expressões faciais, memórias são sondadas em busca de fatos passados etc. Em um cenário de vigilância, o corpo eletrônico passa a dar destaque para o corpo humano, entretanto, este passa a ser utilizado como ‘’cobaia’’ para experimentos tecnológicos e sendo ‘’invadido’’ de todas as formas para fins de coleta de dados.

Diante desse cenário, é primordial questionar o impacto da vigilância digital e buscar mecanismos para garantir que sua utilização respeite os princípios democráticos e os direitos humanos. Senão, estaremos caminhando para uma sociedade na qual o controle e a manipulação prevalecerão sobre as liberdades individuais, comprometendo a autonomia dos cidadãos e a própria estrutura do Estado de Direito.

4. ASPECTOS LEGAIS DA REGULAMENTAÇÃO

A discussão sobre os aspectos legais da regulamentação e da proteção de dados biométricos no Brasil é relevante por estarmos vivenciando uma Era Digital marcada por tecnologias emergentes, a exemplo do reconhecimento facial, uma aplicação da Inteligência Artificial.

Embora a identificação facial seja muito utilizada no Brasil, especialmente com seu uso concentrado na segurança pública, não há regulamentação específica para essa tecnologia. Com isso, apesar do Marco Legal da Proteção de Dados (LGPD), a lei n° 13.709/2018, dispor de objetivos para a proteção dos dados pessoais, atualmente não há legislação específica que regulamenta a tecnologia de reconhecimento facial.

Desse modo, este capítulo tem como objetivo abordar a LGPD, explicar o seu impacto no tratamento de dados pessoais e na sua aplicação ao reconhecimento facial, analisar e comparar regulamentações internacionais, discutir a ausência de disposição normativa para o uso e riscos da tecnologia, assim como apresentar diretrizes para legislação futura.

4.1. Panorama da regulamentação internacional

A tecnologia de reconhecimento facial é um tema considerado ‘’complexo’’ e que ainda está em discussão, tanto no Brasil, como a nível internacional. Com isso, os países ainda estão formulando suas leis para regulamentação. Ou seja, o cenário atual dá ênfase para restrições e proibições, destacando a ausência de regulamentação ou construção de normativas para equilibrar a tecnologia com a proteção de direitos fundamentais.

Como mencionado por Oliveira (2021), em San Francisco (EUA), a norma Ordinance NO. 107-19 ganha destaque por tratar da regulação do reconhecimento facial para fins de vigilância, em uma localização que engloba o Vale do Silício, no qual estão presentes as gigantes da tecnologia, como: Apple, google, microsoft e Tesla. Neste sentido, houve uma restrição do uso pela polícia e agências públicas, entretanto, apesar da proibição, a medida não impactou no uso pessoal ou comercial, de acordo com Gomes (2019). Além disso, o que motivou a regulação está ligada

diretamente ao viés discriminatório do algoritmo vigilância em massa por parte do governo.

De acordo com Oliveira (2021), a norma Ordinance de San Francisco foi promulgada em junho de 2019 e é uma legislação que trata da regulação da tecnologia de reconhecimento facial para fins de vigilância no maior município que engloba o Vale do Silício, no qual estão localizadas as gigantes da tecnologia: Apple, Google, Microsoft e Tesla.

A norma aprovada pelo Conselho de Supervisores da Cidade, é semelhante à uma lei municipal no Brasil, a única diferença é que a lei segue as especificidades dos EUA. Basicamente, a ementa traz as seguintes diretrizes: os departamentos das cidades devem apresentar uma Política de Tecnologia de Vigilância aprovada pelo Conselho de Supervisores baseada nas políticas desenvolvidas pelo Comitê de Tecnologia da Informação (COIT) e um relatório de Impacto da Vigilância ao Conselho (City and County of San Francisco, 2019).

Além disso, cada departamento da cidade que já possui algum equipamento ou serviços de tecnologia de vigilância, deve apresentar ao conselho uma proposta que regule o uso da tecnologia de vigilância. O responsável pelas decisões referentes ao tratamento de dados (controlador), precisa auditar anualmente o uso dos equipamentos ou serviços, além da conformidade de uso, de acordo com uma Política de Tecnologia de Vigilância aprovada, bem como o fornecimento de relatório ao Conselho (City and County of San Francisco, 2019). Resumidamente, o uso das tecnologias de vigilância é direcionado à aprovação, pelo Conselho de Supervisores da Cidade, de uma Política de Tecnologia para vigilância.

Como mencionado anteriormente por Oliveira (2021), a Política de Vigilância é elaborada pelo COIT, após o departamento interessado na implementação da tecnologia, sujeitar ao órgão o Relatório de Impacto da Vigilância. Vale ressaltar que a aprovação da Política de Tecnologia só acontecerá se os efeitos positivos superarem os efeitos negativos. Os direitos e liberdades serão protegidos e a política será utilizada de forma imparcial, evitando preconceitos e discriminações.

Consta na Ordinance que, historicamente, as tecnologias de vigilância foram utilizadas com fins de intimidação e opressão de grupos e comunidades, incluindo aqueles definidos por raça, etnia, origem etc, ademais, o uso do

reconhecimento facial intensifica injustiças raciais, além de manter os indivíduos intimidados pelo monitoramento estatal (City and County of San Francisco, 2019). Ou seja, a regulação mostra-se como uma lei extremamente importante, com diretrizes específicas e detalhadas, que reforça o reconhecimento de vieses discriminatórios no algoritmo que corrobora com preconceitos históricos e que, de certa forma, precisa ser combatido e direitos individuais precisam continuar sendo assegurados.

Além dos EUA, a Europa também tem buscado elaborar suas próprias leis e ampliar o debate sobre a Inteligência Artificial que acaba influenciando no Reconhecimento Facial, por ser uma aplicação da IA. Neste sentido, é válido analisar como a União Europeia está colaborando com a discussão.

Na Europa, as movimentações para o banimento da tecnologia de reconhecimento facial na segurança pública já vêm acontecendo há algum tempo, e isto pode ser observado com a preparação para a implementação da IA em 2010, quando documentos foram lançados com o objetivo de regulamentá-la (Comissão Europeia, 2018).

Neste sentido, em 2018, a Comissão Europeia enviou um comunicado aos órgãos para que analisassem a tecnologia, estabelecendo diretrizes que posteriormente serviriam como embasamento para as legislações específicas sobre IA (Cepej, 2018).

Em seguida, foi lançada uma carta europeia de Ética sobre o uso da IA em Sistemas Jurídicos e seu ambiente, no qual foram adotados princípios como ‘’respeito aos direitos fundamentais’’, ‘’não-discriminação’’ e ‘’transparência’’, que devem ser observados pelos agentes públicos e privados (Cepej, 2018).

Neste seguimento, também foi publicado um artigo pela Agência dos Direitos Fundamentais da União Europeia, com o título ‘’Tecnologia de Reconhecimento Facial’’: considerações de direitos fundamentais no contexto da aplicação da lei’’, no qual foi reforçada a preocupação com a implementação da tecnologia em decorrência do potencial em afligir direitos mínimos ou a possibilidade de serem substituídos e ofuscados (União Europeia, 2019).

Posteriormente, o Comitê Europeu lançou as diretivas 3/2019 para a Proteção de Dados, no qual o objetivo era analisar a proteção de dados em relação ao uso de videomonitoramento. Foi tratado na diretiva que o uso de

videomonitoramento impacta diretamente na forma como as pessoas se comportam, afetando a privacidade e o direito de seguir a vida no anonimato de uma forma que não sejam levantadas suspeitas sobre algo ilícito que uma pessoa tenha feito ou culpabilidade (European Data Protection board, 2020). Com isso, o objetivo da diretiva é de que as ações que ferirem direitos, devem ser fundamentadas, analisadas e reavaliadas periodicamente.

Em 2020, a Comissão Europeia lançou o ‘’livro branco sobre inteligência artificial’’, definindo condutas mais precisas baseadas na estratégia lançada em 2018. O intuito foi pensar em equilibrar o uso da tecnologia em decorrência de sua importância, levando em consideração as implicações éticas e humanas (Comissão Europeia, 2020).

Logo após, em 2021, a Comissão propôs um novo regulamento sobre a IA, no qual buscaram estabelecer uma tecnologia neutra, criação de regras para os sistemas que apresentam altos riscos para direitos fundamentais, além de buscar incentivar códigos de conduta para os sistemas com pouco ou nenhum risco (Comissão Europeia, 2021).

O regulamento trouxe a definição dos níveis de risco para a IA sendo: inadmissíveis, de risco alto, limitado e mínimo. Dessa forma, o título II, art.5° diz que os sistemas de identificação biométrica com monitoramento ao vivo em espaços públicos para fins policiais são considerados inadmissíveis (Comissão Europeia, 2021).

Os sistemas considerados de alto nível, dizem respeito à potencialidade de prejudicar a segurança das pessoas ou os direitos fundamentais. Sendo assim, os sistemas de identificação remota, embora não sejam proibidos, precisam passar pelos requisitos rigorosos, tais como: gestão de risco, qualidade dos dados, documentação e registro, transparência e divulgação de informações aos usuários, supervisão humana e solidez, bem como a avaliação antes de entrar no mercado, criação e uso (Melo, 2024).

O regulamento não deixou de receber críticas, pois não trouxe a definição de algoritmos e dados, seus diferentes tipos, além de ser muito amplo e não abarcar todos os casos e situações específicas. Segundo Melo (2024), em decorrência das possíveis lacunas no regulamento e de pontos que não ficaram bem esclarecidos,

foram aprovadas algumas mudanças no texto em junho de 2023. Ao que tudo indica, houve um maior banimento da tecnologia, de acordo com o art. 5° que proíbe o uso da IA para fins de identificação biométrica à distância em tempo real em espaços públicos (Melo, 2024).

4.2. Panorama na regulamentação Brasil: Uma análise dos Pls 12/2015, 1515/2022, 3.069/2022 e 2.338/2023

Analisar o panorama da regulamentação da tecnologia de reconhecimento facial no Brasil é essencial para estabelecer uma base para compreensão do contexto atual de uso e controle da tecnologia. Além disso, é importante analisar os projetos de lei que estão sendo elaborados ou tramitando atualmente para entender como estamos avançando no debate e no âmbito legislativo. Basicamente, a análise contribuirá para nortear o leitor, para o levantamento de pontos positivos e negativos dos projetos. Ademais, é imprescindível destacar como direitos fundamentais podem ser afetados diante dos desafios apresentados pelo uso da tecnologia, oferecer uma visão do que já foi regulamentado, dos autores e desafios envolvidos, além de mostrar a relevância da atuação de diferentes áreas ou órgãos (Judiciário, Legislativo e ANPD).

O reconhecimento facial vem sendo utilizado de forma ampla no Brasil, como, por exemplo, na segurança pública, em eventos festivos, serviços financeiros, na educação etc. Entretanto, o seu uso vem crescendo e, consequentemente, tem gerado debates sobre a necessidade de uma regulamentação específica para garantir a proteção de direitos fundamentais.

Apesar de a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) estabelecer princípios gerais para o tratamento de dados pessoais, incluindo a biometria, não há no ordenamento jurídico brasileiro uma legislação específica que regule detalhadamente o uso do reconhecimento facial.

A ausência de normatização específica gera desafios que necessitam de diretrizes claras para a implementação da tecnologia de forma ética e segura, principalmente para os cidadãos, que podem ter seus direitos violados sem mecanismos eficazes de proteção.

Analisando o cenário brasileiro, vários projetos têm sido apresentados no Congresso Nacional para regulamentar o uso da tecnologia, como por exemplo o PL 12/2015. O projeto, de autoria do ex-deputado Lucas Vergílio, dispõe sobre a utilização de sistemas de verificação biométrica e dá outras providências (Brasil, 2015).

Os principais objetivos são referentes à regulamentação da utilização dos sistemas, com ênfase na proteção de dados biométricos e na garantia de direitos dos titulares. Com isso, pode ser observado que no art. 1° há um destaque para o estabelecimento de normas gerais para os sistemas de verificação pensando na substituição dos meios de segurança tradicionais, bem como na segurança das informações dos indivíduos. Além disso, o art. 4° diz que ‘’o armazenamento dos dados biométricos somente ocorrerá por meio do consentimento inequívoco de seu titular, expressa ou tacitamente, ressalvadas as exceções de interesse público, e terá como finalidade a confirmação da identidade do seu titular’’.

O PL dispõe acerca dos sistemas de identificação biométrica, com foco na proteção de dados e na segurança dos indivíduos. O referido PL, em seu art. 2º, traz uma definição sobre os sistemas biométricos. Discorre ainda a respeito do consentimento do titular para o armazenamento de dados biométricos, exceto em casos de interesse público (art., 4°), da garantia dos direitos do titular (art. 7°), da segurança e armazenamento dos dados (art. 4°, § 1 e 2), das penalidades por infrações (art. 7°) e da regulamentação técnica (art. 5° ao 7°).

O PL aborda de forma geral os sistemas, mas não aborda especificamente o reconhecimento facial, como pode ser verificado no art. Art. 2º:

> Art. 2. Para efeitos desta Lei considera-se como sistema de verificação biométrica o método automatizado pelo qual a identidade de um indivíduo é verificada, comparando-se dados biométricos deste indivíduo com um ou mais modelos biométricos armazenados no dispositivo do sistema de verificação.

Pode ser observado uma ambiguidade nas definições, tendo em vista que essa descrição é ampla e não especifica quais tipos de dados biométricos são incluídos (por exemplo, impressões digitais, reconhecimento facial, íris etc.). Portanto, essa generalidade pode permitir interpretações variadas sobre quais tecnologias e práticas seriam cobertas pela lei, pois apesar da definição abrangente, pode não ser

suficiente para englobar todos os aspectos do reconhecimento facial e suas aplicações.

Um ponto controverso do PL é o art. 4°, que trata do consentimento do indivíduo para o armazenamento dos dados. A exigência de consentimento inequívoco pode ser questionável em contextos no qual a coleta de dados é realizada sem o conhecimento do usuário ou em situações de exceção de interesse público, criando brechas para o uso indevido desses dados.

A eficácia do PL depende da capacidade das autoridades de fiscalizar e aplicar regras estabelecidas. Entretanto, o projeto não faz menção à órgãos fiscalizatórios, o que nos leva a observar que pode haver incertezas sobre quem deve monitorar e garantir a conformidade com a lei.

Outro ponto controverso do PL é o contraste entre o interesse público e a privacidade. Embora a necessidade de equilibrar o interesse público com a privacidade ainda seja um dos maiores desafios na discussão, é importante buscar um equilíbrio que, de fato, resguarde direitos fundamentais. Por fim, apesar do projeto tratar de pontos importantes, a rápida evolução da tecnologia pode dificultar sua aprovação, sendo necessário que novos ajustes sejam feitos para que possa adequar-se às novas aplicações tecnológicas e englobar desafios que não foram previstos no momento da sua elaboração.

Avançando um pouco, o PL 1515/2022 foi proposto pelo Deputado Coronel Armando (PL/SC), que trata sobre ‘’Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais’’ (Brasil, 2022).

O texto possui pontos positivos ao buscar suprir um vácuo normativo da LGPD prevista no art. 4°, acerca do tratamento de dados no âmbito da segurança pública. Além disso, é destacado na justificação do projeto o intuito de disciplinar princípios e diretrizes em relação ao tratamento de dados, para que haja respeito aos direitos fundamentais de liberdade e à autodeterminação informativa (Brasil, 2022).

Todavia, é preciso analisar os pontos negativos que precisam de atenção. O PL 1515/2022 levanta preocupações quanto à privacidade dos indivíduos, tendo em vista que uma regulamentação excessivamente permissiva pode facilitar abusos por parte de autoridades no acesso aos dados. Além disso, sua implementação depende de regulamentações adicionais, o que pode gerar atrasos e dificuldades práticas. Há

também o risco de ampliação indevida dos poderes das autoridades, favorecendo práticas de vigilância excessiva.

De acordo com Melo (2024), na elaboração da LGPD penal, buscou-se uma comissão de juristas, de forma democrática, levando em consideração que no projeto o direito penal seria utilizado como último recurso (*ultima ratio*), diante da influência direta na privação de liberdade. Dessa forma, teve como objetivo a elaboração de normas que facilitassem o trabalho dos agentes públicos, porém, enfatizando que os direitos mínimos previstos na Constituição Federal não poderiam deixar de ser observados (Reis *et al.*, 2021).

Já o PL 3.069/2022, por sua vez, trata especificamente sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública, o que levanta preocupações sobre vigilância em massa e possíveis abusos por parte do Estado.

Em suma, o PL busca regulamentar o uso no âmbito da segurança pública, preenchendo um vácuo importante, tendo em vista que a LGPD não se aplica nesse caso. Dessa forma, o projeto é relevante para evitar usos arbitrários ou abusivos. Além disso, o projeto apresenta definições claras sobre ‘’reconhecimento facial’’, ‘’biometria’’ e ‘’identificação’’, de acordo com a justificação do projeto (Brasil, 2022), bem como a exigência de supervisão humana, obrigatoriedade de sinalização em locais com câmeras, busca por pessoas desaparecidas e cumprimento de mandados de prisão, e por fim, a adoção de outros métodos biométricos, a exemplo da papiloscopia.

Apesar dos pontos positivos, é importante analisar os pontos negativos e sua relevância na discussão da regulamentação. Mesmo com as medidas propostas, o uso da tecnologia em espaços públicos pode abrir margem para a vigilância em massa e coleta indiscriminada de dados, o que reflete diretamente na proteção de dados. Além disso, a tecnologia possui um histórico de taxas de erro mais altas para grupos sociais e étnicos, o que pode acarretar em injustiças e discriminações. A título de exemplo, em 2018 a Amazon utilizou um sistema de IA para revisão de currículos e seleção de candidatos, entretanto, candidatas mulheres foram discriminadas e receberam escores mais baixos, já que o algoritmo foi treinado com dados históricos representando uma quantidade superior de homens na área de tecnologia (Gonçalves, 2024).

Neste sentido, Dushi (2020) e Madiega e Mildebrath (2021) afirmam que as tecnologias de biometria podem ser influenciadas por vieses culturais e sociais por parte daqueles que criam e desenvolvem os sistemas. Esses vieses podem ser inconscientes ou conscientes, refletindo preconceitos ou desigualdades já presentes na sociedade.

Além dos desafios controversos citados anteriormente, o texto também não prevê penalidades claras diante do possível uso inadequado da tecnologia, o que pode diminuir a eficácia da proteção proposta. Por fim, há a ausência de controle social e transparência para assegurar o uso da tecnologia de forma legítima e proporcional, tendo em vista que não há mecanismos de auditoria ou supervisão clara sobre o uso da tecnologia, o que é de extrema importância fundamental para garantia de responsabilidade por parte das forças de segurança pública e prevenção de abusos

O projeto é relevante no contexto da regulamentação do reconhecimento facial, tendo em vista os pontos essenciais para disciplinar o uso pelas forças da segurança pública. Entretanto, a ausência de medidas contra os possíveis abusos e o risco de vigilância massiva destaca a necessidade de aprimoramentos no texto.

Por fim, é imprescindível falar do PL 2.338/2023 que tem como objetivo a regulamentação da Inteligência Artificial no Brasil. Esse projeto impacta diretamente no uso do reconhecimento facial, tendo em vista que a tecnologia é uma aplicação da IA. Além disso, como destacou Lacerda (2024), o Novo Marco Legal também menciona o uso de sistemas de reconhecimento facial em tempo real em espaços públicos, embora haja exceções, além da limitação do uso de vigilância em massa para proteção da privacidade.

O projeto foi aprovado no dia 10 de dezembro de 2024 pelo Senado e busca garantir a proteção dos direitos em diversas esferas da sociedade, estabelecendo assim normas que tratam do desenvolvimento da IA (Lacerda, 2024). A proposta prevê a criação do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA) e estabelece diferentes níveis de risco para a classificação dos sistemas de IA (Brasil, 2023).

Analisando os pontos positivos, há um fortalecimento dos direitos fundamentais, ao promover a transparência e mitigação quanto à discriminação no uso da IA, além de impulsionar a competitividade no setor tecnológico através da

regulação (Brasil, 2023). O segundo ponto relevante do projeto é a classificação dos sistemas baseada em risco, permitindo assim que haja um monitoramento dos sistemas considerados de alto impacto, minimizando os prejuízos à sociedade (Brasil, 2023). O art. 23 assegura que as pessoas afetadas por decisões automatizadas, tenham o direito de direito à explicação e à revisão humanas de decisão por sistemas de IA, que será promovida pelo agente público competente nesse caso.

Por outro lado, o marco legal pode gerar complexidade e altos custos de conformidade, tendo em vista que empresas fornecedoras de sistemas de reconhecimento facial, podem sofrer um grande impacto com as normas diante de burocracia e custos, diante da regulamentação, avaliações de impacto, responsabilidades, o que demonstra o aumento nas exigências administrativas e financeiras por quem utilizar os sistemas de IA.

4.3. Lacunas e sugestões para a regulamentação

O reconhecimento facial tem sido utilizado de forma ampla, tanto pelo setor público, como pelo setor privado. Entretanto, ainda não há uma regulamentação específica. Assim como as primeiras pesquisas da tecnologia iniciaram com o objetivo de reconhecer pessoas ‘’suspeitas’’ de terem cometido algum ato ilícito, o seu uso atualmente é concentrado na segurança pública, com a finalidade de identificar foragidos da Justiça.

Nesse sentido, vale ressaltar que, de acordo com o art. 4°, inciso III da LGPD, a Lei não se aplica ao tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (Brasil, 2018). No entanto, o §1º do mesmo artigo prevê que, nesses casos, deve haver uma legislação específica que estabeleça medidas proporcionais e estritamente necessárias ao interesse público, observando o devido processo legal, os princípios gerais de proteção de dados e os direitos do titular (Brasil, 2018). Apesar dessa previsão, ainda não há normatização para o uso do reconhecimento facial, o que gera incerteza jurídica e risco de violação de direitos fundamentais.

Embora o uso dos sistemas de identificação facial no Brasil esteja centralizado na esfera da segurança, suas implicações vão além desse campo. A LGPD define, em seu art. 5º, inciso II, que os dados biométricos são dados pessoais

sensíveis, exigindo critérios rigorosos para seu tratamento. No entanto, o art. 11 da mesma lei dispensa a necessidade de consentimento em algumas situações, incluindo cumprimento de obrigação legal, segurança pública e proteção da vida do titular. Na prática, isso abre margem para interpretações diversas sobre quando e como o consentimento deve ser exigido, além da falta de clareza sobre consentimento e transparência.

Com isso, considerando que o Marco Legal da Proteção de Dados conceitua no art. 5°, inciso II, o dado biométrico como um dado pessoal sensível (Brasil, 2018), também determina requisitos para o tratamento, de acordo com o art. 11, incisos I e I, no qual enfatiza o consentimento do titular para esta operação. Entretanto, a Lei também dispensa o consentimento nas hipóteses previstas, como por exemplo:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;

Ou seja, apesar da LGPD ser a principal base jurídica que regulamenta os dados pessoais, garantindo que os tratamentos resguardem direitos fundamentais, a Lei não trata das especificidades da tecnologia.

Em geral, apenas a LGPD não é suficiente para tratar de todas as situações decorrentes do uso do reconhecimento facial (Oliveira, 2021). Neste sentido, é importante analisar quais são os pontos em comum entre os PL's que estão tramitando atualmente, principalmente do PL 2.338/2023 que trata sobre a Inteligência Artificial, para que se possa sugerir caminhos para regulamentação adequada.

Dessa forma, é essencial que a legislação brasileira acompanhe a evolução dessa tecnologia, pensando na proteção de direitos e no uso ético e responsável. O objetivo desse tópico é mostrar as lacunas encontradas na análise realizada dos

projetos de lei em tramitação, a fim de sugerir medidas que possam mitigar os riscos e preocupações oriundos do uso do reconhecimento facial.

Diante dessas lacunas, diversos projetos de lei foram propostos para suprir a falta de regulamentação específica. Para regulamentar o uso do reconhecimento facial na segurança pública, foi proposto o PL 1.515/2022, que estabelece uma Lei de Proteção de Dados Pessoais voltada para a segurança do Estado, defesa nacional e repressão de infrações penais. O texto busca delimitar o uso da biometria por órgãos de segurança, mas ainda apresenta fragilidades em relação à fiscalização e à mitigação de riscos de discriminação. O art. 20 do PL 1.515/2022, por exemplo, prevê que agentes públicos devem justificar a coleta e o tratamento de dados biométricos, mas não determina regras rígidas para garantir que o cidadão tenha pleno conhecimento sobre quando e como suas informações estão sendo utilizadas.

O PL 3.069/2022, por sua vez, voltado especificamente para o uso do reconhecimento facial pelas forças de segurança pública, propõe regras para a implementação da tecnologia, mas não apresenta garantias concretas contra possíveis abusos e não prevê mecanismos de auditoria obrigatória para evitar erros e vieses discriminatórios. A inexistência de critérios rígidos pode abrir espaço para a vigilância em massa, um dos desafios do uso da tecnologia emergente, afetando direitos fundamentais como a privacidade e a liberdade de locomoção.

Por outro lado, o PL 2.338/2023, que propõe um marco regulatório para inteligência artificial no Brasil, pode impactar diretamente o reconhecimento facial, tendo em vista que abrange regras gerais sobre sistemas automatizados de decisão. Na seção III do art. 22, há medidas de governança que devem ser aplicadas pelo Poder Público, como por exemplo, que os cidadãos possam saber como e por quê suas informações estão sendo processadas e utilizadas. Além disso, o texto também estabelece no art. 29, que os desenvolvedores de IA de propósito geral e generativa, devem implementar medidas para mitigar a discriminação, bem como da exigência de avaliação de impacto algorítmico.

A análise dos projetos de lei atualmente em tramitação revela objetivos em comum: proteção de direitos, equilíbrio entre o uso da tecnologia com questões sociais e o anseio de preencher lacunas jurídicas. No entanto, também representam lacunas recorrentes. Apesar dos projetos propostos mostrarem que estamos avançando na discussão, ainda não há uma regulamentação completa que aborda os principais

desafios não resolvidos sobre o reconhecimento facial. Ou seja, ainda não temos critérios claros para o consentimento e transparência no tratamento de dados biométricos, não há menção sobre auditorias obrigatórias para mitigar vieses algorítmicos, incertezas sobre a responsabilização pelo uso da tecnologia, além disso, os projetos que tratam sobre a segurança pública não mencionam, nem estabelecem limites para evitar vigilância em massa e uso abusivo por parte da polícia.

Com base na análise feita do contexto brasileiro, dos projetos de lei em tramitação e também em consonância com o objetivo geral desse trabalho, para garantir uma regulamentação adequada que equilibre inovação e proteção de direitos, algumas medidas podem ser sugeridas.

1) *Exigência de consentimento informado e explícito:* a regulamentação deve detalhar como e quando o titular dos dados deve ser informado sobre a coleta e o uso de sua biometria;
2) *Estabelecimento de regras claras para o uso da tecnologia pelo setor público:* a legislação deve limitar o uso indiscriminado pela segurança pública, garantindo auditorias independentes e mecanismos de contestação para os cidadãos afetados; Vedação e sanções para o uso inadequado da tecnologia com finalidades não previstas em Lei.
3) *Fortalecer a fiscalização da ANPD:* A Autoridade Nacional de Proteção de Dados deve ter competência ampliada para monitorar o uso do reconhecimento facial e aplicar sanções efetivas em casos de abuso.
4) *Criar exigências de auditoria para reduzir vieses algorítmicos nos Órgãos Públicos:* Empresas e órgãos públicos que utilizam reconhecimento facial devem ser obrigados a realizar testes técnicos regulares para evitar discriminações e erros de identificação.
5) *Garantir transparência no armazenamento e compartilhamento de dados:* A regulamentação deve delimitar prazos de retenção e proibir o compartilhamento indiscriminado de bases de dados biométricos entre entidades públicas e privadas.

5. CONSIDERAÇÕES FINAIS

O presente trabalho analisou a regulamentação do reconhecimento facial no Brasil, abordando os desafios técnicos, jurídicos e sociais relacionados ao uso da tecnologia. Desde as primeiras pesquisas como ferramenta de identificação nos anos 90, o reconhecimento facial evoluiu consideravelmente, sendo utilizado de forma ampla por diversos setores, como segurança pública, setor privado e serviços governamentais. No entanto, o uso indiscriminado da tecnologia sem uma regulamentação específica levanta preocupações sobre privacidade, segurança dos dados biométricos e possíveis violações de direitos fundamentais.

A pesquisa demonstrou que, apesar da Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece diretrizes gerais para o tratamento de dados pessoais no Brasil, essa legislação não é suficiente para tratarmos da regulamentação, tendo em vista as especificidades do reconhecimento facial. Neste sentido, é válido reforçar que o tratamento de dados biométricos é considerado sensível e requer salvaguardas adicionais para evitar abusos. No entanto, as lacunas normativas ainda persistem, como a ausência de regras claras para a obtenção de consentimento, transparência no uso da tecnologia e limites para sua aplicação em âmbitos como a segurança pública, no qual o principal uso da tecnologia está concentrado atualmente.

No capítulo dedicado ao panorama da regulamentação no Brasil, analisou-se a legislação atual e os projetos de lei em tramitação. Foi observado que há uma preocupação crescente com os impactos sociais e jurídicos do reconhecimento facial, especialmente no que se refere à segurança pública. Projetos como o PL 12/2015, PL 1515/2022 (considerada ‘’LGPD Penal’’), PL 3.069/2022 e PL 2.338/2023 propõem restrições e diretrizes para o uso da tecnologia, mas ainda carecem de precisão quanto à fiscalização e à proteção dos direitos dos cidadãos.

Outro ponto de destaque na pesquisa foi a análise dos desafios enfrentados pelo reconhecimento facial, especialmente no que diz respeito ao viés discriminatório e à vigilância em massa. Na segurança pública, por exemplo, o uso tem como objetivo a promessa de aumentar a eficiência na identificação de foragidos e na prevenção de crimes. Entretanto, embora a tecnologia seja efetiva, ela também aponta falhas. Pesquisas, notícias e documentários demonstram que sistemas de reconhecimento

facial apresentam taxas de erro mais altas na identificação de pessoas negras nos bancos de dados utilizados para treinar os algoritmos. Casos de erros na identificação de indivíduos pode resultar em abordagens policiais desproporcionais e prisões indevidas, reforçando desigualdades estruturais, o que justifica a necessidade de uma regulamentação mais rigorosa.

Ademais, a vigilância em massa é um dos riscos mais alarmantes do uso irrestrito dessa tecnologia. A possibilidade de monitoramento constante de indivíduos sem seu consentimento levanta preocupações sobre liberdade de expressão e direito à privacidade. Como discutido no trabalho, a implantação de sistemas de reconhecimento facial sem mecanismos de transparência e controle social pode levar à criação de um estado de vigilância, no qual indivíduos são monitorados de forma indiscriminada e sem justificativa adequada.

No estudo também foi abordado um panorama da regulamentação internacional, destacando experiências como a da União Europeia e a legislação de San Francisco, nos Estados Unidos, que estabeleceram restrições ao uso da tecnologia em função dos riscos associados à vigilância em massa e à discriminação algorítmica. Na prática, essas experiências podem servir de referência para o Brasil na formulação de normativas mais adequadas para o uso da tecnologia de reconhecimento facial, tendo em vista que o Marco Legal da Proteção de Dados possui bastante similaridade com a GDPR, por exemplo.

Diante dos desafios quanto ao uso da tecnologia e de tudo que foi abordado até aqui, o estudo aponta algumas recomendações para aprimorar a regulamentação do reconhecimento facial no Brasil. É de extrema importância a discussão acerca do consentimento do indivíduo quanto ao uso da tecnologia por parte do Poder Público, e, consequentemente, que a legislação estabeleça diretrizes claras para sua obtenção, garantindo que os cidadãos tenham pleno conhecimento sobre como seus dados biométricos estão sendo utilizados e, inclusive, a oportunidade de não consentir com a coleta e armazenamento. Além disso, é necessário um reforço na fiscalização por parte da Autoridade Nacional de Proteção de Dados (ANPD), garantindo que o uso da tecnologia, independente da esfera (setor privado ou público), esteja em conformidade com princípios de proteção de dados e direitos fundamentais.

Outra medida essencial é a implementação de auditorias independentes para avaliar a precisão e os impactos dos sistemas de reconhecimento facial, iniciativa

prevista, inclusive, no PL 2.338/2023 (Marco Legal da Inteligência Artificial). Essas auditorias podem contribuir para a redução de vieses algorítmicos e para a criação de padrões mais justos para a utilização da tecnologia. Além disso, a participação de especialistas em direito digital, proteção de dados, direitos humanos, desenvolvedores de software e a sociedade civil, é fundamental para garantir que as regulamentações sejam eficazes e alinhadas com os princípios democráticos, garantindo que diferentes setores possam contribuir para um marco regulatório equilibrado.

Por fim, este estudo reforça a importância de um debate amplo e qualificado sobre o tema. Somente assim será possível desenvolver uma legislação que assegure tanto a inovação tecnológica quanto a proteção dos direitos dos cidadãos.

REFERÊNCIAS

BATISTA, Vera M. **A questão criminal no Brasil contemporâneo**. 2° Fórum Nacional de Alternativas Penais: "Audiências de Custódia e a Desconstrução da Cultura do Encarceramento em Massa". Salvador, 2016. Disponível em: https://issuu.com/amilcarpacker/docs/caderno_oip_vera_malaguti. Acesso em: 02 fev. 2025.

BARBOSA SOBRINHO, Marcionílio; CORRÊA, Fábio; SOARES, Aleida. N.; RIBEIRO, Jurema. S. de. A. N.; DIAS, Roberto. C. Uso da biometria facial para o controle de benefícios e gratuidades no Transporte Público Coletivo: um estudo de caso na cidade de Ilhéus, Bahia, Brasil. **Revista Transporte y Territorio**, n. 30, p. 149-157, 2024. Disponível em: http://revistascientificas.filo.uba.ar/index.php/rtt/article/view/11947. Acesso em: 15 de out. 2024.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida.** Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

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, 1997. Disponível em: <fisherface-pami97.pdf (idiap.ch)>. Acesso em: 22 jun. 2024.

BENTO, G. **Reconhecimento Facial da Bahia localiza 689 foragidos em 2024**. Disponível em: https://www.cnnbrasil.com.br/nacional/reconhecimento-facial-da-bahia-localiza-689-foragidos-em-2024/#goog_rewarded. Acesso em: 15 dez. 2024.

BISSI, Thelry David. **Reconhecimento Facial com os Algoritmos Eigenfaces e Fisherfaces**. 2018. 41 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Federal de Uberlândia, Uberlândia, 2018. Disponível em: https://repositorio.ufu.br/handle/123456789/22158. Acesso em: 05 jun. 2024.

BLEDSOE, Woodrow W. The model method in facial recognition. **Panoramic Research Inc., Palo Alto, CA, Rep. PR1**, v. 15, n. 47, p. 2, 1966. Disponível em: A Facial Recognition Project Report: Woodrow Wilson Bledsoe : Free Download, Borrow, and Streaming : Internet Archive. Acesso em: 23 mai. 2024

BRASIL. Lei 13.709/2018, de 14 de agosto de 2018. Regulamenta a proteção de dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. **Diário Oficial da União.** Brasília, DF, 14 out. de 2018. Acesso em: 13 jun. 2024

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 3 de maio de 2023**. Brasilia, DF, 03 mai. 2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233?city=1832. Acesso em: 27 jan. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei N° 3.069/2022, de 22 de dezembro de 2022**. Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências. Brasília, DF, 22 dez. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2228103&filename=PL%203069/2022. Acesso em: 30 jan. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei N.º 12/2015, de 02 de fevereiro de 2015**. Dispõe sobre a utilização de sistemas de verificação biométrica e dá outras providências. Brasília, DF, 02 fev. 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1296692&filenam. Acesso em: 28 jan. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1515/2022 de 12 de agosto de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF, 12. ago. 2022. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300&fichaAmigavel=nao. Acesso em: 09 jan. 2025.

BRUNELLI, R.; POGGIO, T. Face Recognition: Features versus Templates. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 15, n. 10, p. 1042-1052, 1993.

BUGHIN, J.; HAZAN, E.; Ramaswamy, S.; CHUI, M.; MANYIKA, J.; BROWN, B.; BYRNE, R.; DOBBS, R. Artificial Intelligence: The Next Digital Frontier? **McKinsey Global Institute**, 2017. Disponível em: https://www.mckinsey.com/de/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.pdf. Acesso em: 18 jan. 2025.

BUOLAMWINI, Joy.; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: **Conference on fairness, accountability and transparency**. PMLR, 2018. p. 77-91. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a.html?mod=article_inline&ref=akusion-ci-shi-dai-bizinesumedeia. Acesso em: 19 jan. 2025.

CARTACAPITAL. **Prefeito de São Paulo assina contrato para programa de reconhecimento facial**. 2022. Disponível em: https://www.cartacapital.com.br/politica/prefeito-de-sao-paulo-assina-contrato-para-programa-de-reconhecimento-facial/. Acesso em: 15 dez. 2024.

CEPEJ. Comissão Europeia para a eficácia da justiça. **Carta Europeia de ética sobre o uso da inteligência artificial em sistemas judiciais e seu ambiente, de 3 de dezembro de 2018.** Estrasburgo, 2018. Disponível em: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment. Acesso em: 04 jan. 2025.

CITY AND COUNTY OF SAN FRANCISCO. **Board of Supervisors.** Administrative Code - Acquisition of Surveillance Technology. Ordinance n. 107-19, 2019. Disponível em: https://sfbos.org/sites/default/files/o0107-19.pdf?utm_source=chatgpt.com. Acesso em: 04 jan. 2025.

CODED Bias. Direção: Shalini Kantayya. Produção: Sabine Hoffman. Intérprete: Joy Buolamwini. Roteiro: Shalini Kantayya. Fotografia: Steve Acevedo. Estados Unidos: Netflix, 2020. Online streaming. Disponível em: https://www.netflix.com/br/title/81328723. Acesso em: 04 mar. 2025.

COMISSÃO EUROPEIA. **Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões:** Inteligência Artificial para a Europa. Bruxelas, 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018DC0237>. Acesso em: 04 jan. 2025.

COMISSÃO EUROPEIA. **Proposta de regulamento do parlamento Europeu e do conselho.** Que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da União. Bruxelas, 2021. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206. Acesso em: 01 fev. 2025.

CNN BRASIL. **Reconhecimento facial será obrigatório nos estádios a partir de 2025**. CNN Brasil, 2024. Disponível em: https://www.cnnbrasil.com.br/esportes/futebol/reconhecimento-facial-sera-obrigatorio-nos-estadios-a-partir-de-2025/#goog_rewarded. Acesso em: 18 jan. 2025.

DUSHI, Desara. **The use of facial recognition technology in EU law enforcement:** Fundamental rights implications, 2020. Disponível em: https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content. Acesso em: 01 fev. 2025.

EBC. **O que é o racismo algorítmico**. Revista Rio. 2020. Disponível em: https://radios.ebc.com.br/revista-rio/2020/11/o-que-e-o-racismo-algoritmico. Acesso em: 15 dez. 2020.

EBDS. **Biometria nas empresas:** Principais usos. Inovação, Tecnologia da Informação, 2023. Disponível em: https://ebds.com.br/biometria-nas-empresas/. Acesso em: 02 out. 2024.

EMBRATEL. As quatro eras do reconhecimento facial e seu efeito na privacidade. **Próximo Nível.** 2021. Disponível em https://proximonivel.embratel.com.br/as-quatro-eras-do-reconhecimento-facial-e-seu-efeito-na-privacidade/. Acesso em: 12 mai. 2024.

MADIEGA, Tambiama; MILDEBRATH, Hendrik. **Regulating facial recognition in the EU**. Research Service, EPRS, 2021a. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)698021. Acesso em: 01 jan. 2025.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 3/2019 on processing of personal data through video devices.** 2020. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. Acesso em: 01 fev. 2025.

G1 BAHIA. **Carnaval de Salvador terá mais de 100 câmeras de reconhecimento facial e tecnologia para contagem de público**. 2024. Disponível em: https://g1.globo.com/ba/bahia/carnavalnabahia/noticia/2024/02/07/carnaval-de-salvador-tera-mais-de-100-cameras-de-reconhecimento-facial-e-tecnologia-para-contagem-de-publico.ghtml. Acesso em: 21 de dez. 2024.

G1 PERNAMBUCO. **Escolas municipais de Jaboatão adotam reconhecimento facial para controlar a frequência de alunos**. 2024. Disponível em: https://g1.globo.com/pernambuco/noticia/escolas-municipais-de-jaboatao-adotam-reconhecimento-facial-para-controlar-frequencia-de-alunos.ghtml. Acesso em: 26 jun. 2024.

GOMES, Helton Simões. **Por que uma das maiores cidades dos EUA baniu o reconhecimento facial**. UOL, 2019. São Paulo, 16 maio 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/05/16/por-que-uma-das-maiores-cidades-dos-eua-baniu-o-reconhecimento-facial.htm. Acesso em: 08 dez. 2024.

GONÇALVES, Mariana S. Viés algorítmico e discriminação: Como os algoritmos de IA podem perpetuar e amplificar vieses sociais. Migalhas, 2024. Disponível em: https://www.migalhas.com.br/depeso/415125/vies-algoritmico-e-discriminacao-ia-pode-amplificar-vieses-sociais> Acesso em: 01 fev. 2025.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. **Deep learning**. p. 216-261, 2016. Disponível em: https://www.deeplearningbook.org/contents/regularization.html. Acesso em: 09 fev. 2025.

GUPTA, R.; GUPTA, S.; SINGHAL, A. Big Data: Overview. **International Journal of Computer Trends and Technology (IJCTT)**. v. 9, n. 5, 2014. Disponível em: https://arxiv.org/abs/1404.4136. Acesso em: 09 fev. 2025.

HAN, Byung-Chul. **No enxame:** perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018.

HARTZOG, Woodrow. Facial recognition is the perfect tool for oppression. **Medium**, 2018. Disponível em:https://medium.com/@hartzog/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66. Acesso em: 04 jan. 2025.

Haykin, S. **Neural Networks:** A Comprehensive Foundation. Prentice Hall PTR. 1994. Disponível em: <https://dl.acm.org/doi/abs/10.5555/541500>. Acesso em: 09 fev. 2025.

INSTITUTO IGARAPÉ. Reconhecimento Facial no Brasil. Instituto Igarapé. Disponível: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 15 nov. 2024.

KANADE, Takeo. Picture processing system by computer complex and recognition of human faces. 1974. Disponível em: https://repository.kulib.kyoto-u.ac.jp/dspace/bitstream/2433/162079/2/D_Kanade_Takeo.pdf. Acesso em: 24 mai. 2024.

KRIZHEVSKY, Alex; SUTSKEVER, Ilya; HINTON, Geoffrey E. Imagenet classification with deep convolutional neural networks. **Advances in neural information processing systems**, v. 25, 2012. Disponível em: https://proceedings.neurips.cc/paper_files/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf. Acesso em: 25 jun. 2024.

LACERDA, Nara. **Senado aprova PL da inteligência artificial. Brasil de fato. 2024**. Disponível em: https://www.brasildefato.com.br/2024/12/10/senado-aprova-pl-da-inteligencia-artificial?utm_source=chatgpt.com. Acesso em: 30 jan. 2025

LECUN, Yann; BENGIO, Yoshua; HINTON, Geoffrey. Deep learning. **Nature**, v. 521, n. 7553, p. 436-444, 2015. Disponível em: https://www.nature.com/articles/nature14539. Acesso em: 18 jan. 2025.

LI, S. Z.; JAIN, A. K. **Handbook of Face Recognition**. New York: Springer, 2005.

LYON, D. **Surveillance After September 11**. Cambridge, UK: Polity Press. 2003.

MAURO, Maria F. **Big Data, inteligência artificial e o pensamento crítico**. Portal da mente. 2022. Disponível em: https://mariafranciscamauro.com.br/blog/big-data-inteligencia-artificial-e-o-pensamento-critico/?utm_source=chatgpt.com. Acesso em: 18 jan. 2025.

MELO, Stephanny Resende de. **E quando o suspeito for você?:** Reconhecimento Facial na segurança pública. São Paulo: Editora Dialética, 2024.

MONTEIRO, Thaís. Joy Buolamwini alerta sobre IA e viés algorítmico no SXSW 2024. **Meio e Mensagem**, 2024. Disponível em: https://www.meioemensagem.com.br/sxsw/joy-buolamwini-ia. Acesso em: 02 fev. 2025.

NEOWAY. **Reconhecimento Facial:** Entenda como funciona e suas aplicações. Neoway, 2021. Disponível em: https://blog.neoway.com.br/reconhecimento-facial/. Acesso em: 02 fev. 2025.

NKONDE, Mutale, Automated Anti-Blackness: Facial Recognition in Brooklyn. **Harvard Kennedy School Journal of African American Policy**. v. 20, 2019. Disponível em: https://pacscenter.stanford.edu/wp-content/uploads/2020/12/mutalenkonde.pdf?utm_source=chatgpt.com. Acesso em: 04 fev. 2025.

NOÉ, Ítalo T. **Redes neurais convolucionais aplicadas ao reconhecimento facial em indivíduos com máscara**. 2021. 47 f. Monografia (Graduação em Engenharia de Computação) - Instituto de Ciências Exatas e Aplicadas, Universidade Federal de Ouro Preto, João Monlevade, 2021. Disponível em: https://www.monografias.ufop.br/bitstream/35400000/3487/6/MONOGRAFIA_RedesNeuraisConvolucionais.pdf. Acesso em: 17 jun. 2024.

NUNES, Pablo; SOUZA, Raquel. **A adoção da tecnologia de reconhecimento facial em estádios**. Nexo, 2024. Disponível em: https://www.nexojornal.com.br/externo/2024/09/23/reconhecimento-facial-estadios-futebol-tecnologia. Acesso em 15 dez. 2024.

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

ORWELL, George. **1984**. Editora Companhia das Letras, 2009.

PHILLIPS, P. Jonathon *et al.* The FERET evaluation methodology for face-recognition algorithms. IEEE **Transactions on pattern analysis and machine intelligence**, v. 22, n. 10, p. 1090-1104, 2000. Disponível em: https://www.nist.gov/publications/feret-evaluation-methodology-face-recognition-algorithms. Acesso em: 09 mai.2024

PREFEITURA MUNICIPAL DE SÃO PAULO. ***Programa Smart Sampa.*** São Paulo, 2025. Disponível em: https://capital.sp.gov.br/web/seguranca_urbana/w/smart-sampa-2. Acesso em: 18 jan. 2025.

RAJI, Inioluwa Deborah; FRIED, Genevieve. About face: A survey of facial recognition evaluation. **AAAI 2020 Workshop on AI Evaluation**. 2021. Disponível em: arXiv preprint arXiv:2102.00813. Acesso em: 09 mai. de 2024.

REIS, C.; ALMEIDA, R.; SILVA, R.; DOURADO, T. **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil:** versão resumida. Laboratório de Políticas Públicas e Internet (LAPIN), 2021. Disponível em: https://lapin.org.br/download/4141/. Acesso em: 09 jan. 2025.

RIBAS JUNIOR, Douglas. **Metrô de SP é condenado por captar expressões faciais sem consentimento**. Canaltech, 2023. Disponível em: https://canaltech.com.br/colunas/metro-de-sp-e-condenado-por-captar-expressoes-faciais-sem-consentimento/. Acesso em: 18 jan. 2025.

RODOTÀ, Stefano. Democracia y protección de datos. **Cuadernos de derecho público**, n. 19 – 20. 2003. Disponível em: https://revistasonline.inap.es/index.php/CDP/article/view/690/745. Acesso em: 12 jan. de 2025.

RUSSELL, Stuart J.; NORVIG, Peter. **Artificial intelligence:** a modern approach. Pearson, 2016.

SAINI, Yashwant. Face recognition using Fisherfaces. Opengenus IQ. Disponível em: https://iq.opengenus.org/face-recognition-using-fisherfaces/#google_vignette. Acesso em: 22 jun. 2024.

SANTOS, Camila Ferreira dos. **O novo estado de vigilância baseado em tecnologias de Reconhecimento Facial:** Ensinamentos do passado, explicações do presente e reservas do futuro. Dissertação (Mestrado em Ciências Jurídico-Políticas) – Faculdade de Direito, Universidade de Coimbra, Coimbra, 2023. Disponível em: https://estudogeral.uc.pt/handle/10316/111035. Acesso em: 13 jan. de 2025.

SCHROFF, Florian; KALENICHENKO, Dmitry; PHILBIN, James. Facenet: A unified embedding for face recognition and clustering. **Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)**. p. 815-823, 2015. Disponível em: https://www.cv-foundation.org/openaccess/content_cvpr_2015/papers/Schroff_FaceNet_A_Unified_2015_CVPR_paper.pdf. Acesso em: 25 jun. 2024.

SERPRO – SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **LGPD entra em vigor — LGPD - Lei Geral de Proteção de Dados Pessoais.** 2020. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-entra-em-vigor>. Acesso em: 17 nov. 2024.

SERPRO – SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. O que são dados pessoais, segundo a LGPD. 2025. https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd?utm_source=chatgpt.com. Acesso em: 10 fev. 2025.

SHIMABUKURO, I.; LIMA, L. **O que é algoritmo? Entenda como funciona o conjunto de instruções de um programa.** Tecnoblog, 2024. Disponível em: https://tecnoblog.net/responde/o-que-e-algoritmo/. Acesso em: 21 dez. 2024.

SIROVICH, Lawrence; KIRBY, Michael. Low-dimensional procedure for the characterization of human faces. **Journal of the Optical Society of America A**, v. 4, n. 3, p. 519-524, 1987. Disponível em: https://opg.optica.org/josaa/abstract.cfm?uri=josaa-4-3-519. Acesso em: 20 jun. 2024.

SMANIO, Gianluca M. **A vigilância policial em meio digital:** entre o garantismo e a eficiência. 2021. Dissertação (Mestrado em Direito Processual) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. Acesso em: 2025-02-10. Disponível em: https://bdtd.ibict.br/vufind/Record/USP_7bc03f5df4aca4f2757027967f905f1c. Acesso em: 13 jan. 2025.

TAJRA, Alex. Vigiar e Punir: Ainda sem regulação, estados prendem centenas de pessoas utilizando reconhecimento facial. **Consultor Jurídico (Conjur)**. 2024. Disponível em:

https://www.conjur.com.br/2024-mai-17/sem-regulacao-estados-prendem-centenas-utilizando-reconhecimento-facial/. Acesso em: 18 jan. 2025.

TURING, Alan M. Computing machinery and intelligence. **Springer Netherlands**, 2009. Disponível em: https://link.springer.com/chapter/10.1007/978-1-4020-6710-5_3. Acesso em: 04 fev. 2025.

TURK, Matthew; PENTLAND, Alex. Eigenfaces for recognition. **Journal of cognitive neuroscience**, v. 3, n. 1, p. 71-86, 1991. Disponível em: https://direct.mit.edu/jocn/article/3/1/71/3025/Eigenfaces-for-Recognition. Acesso em: 24 mai. 2024.

UNIÃO EUROPEIA. Tecnologia de reconhecimento facial: considerações de direitos fundamentais no contexto da aplicação da lei. **Agência dos Direitos Fundamentais da União Europeia (FRA)**, 2019. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology_pt.pdf. Acesso em: 01 fev. 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrínseca, 2020.