FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

HENRIQUE BUENO DIB FIGUEIRA

RECONHECIMENTO FACIAL, INTELIGÊNCIA ARTIFICIAL E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

VOLTA REDONDA
2024

FUNDAÇÃO OSWALDO ARANHA
CENTRO UNIVERSITÁRIO DE VOLTA REDONDA
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

RECONHECIMENTO FACIAL, INTELIGÊNCIA ARTIFICIAL E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Monografia apresentada ao Curso de Direito do UniFOA como requisito à obtenção do título de bacharel em Direito.

Aluno: Henrique Bueno Dib Figueira

Orientador:
Professor Mestre Carlos José Pacheco

VOLTA REDONDA
2024

FOLHA DE APROVAÇÃO

Trabalho de Conclusão de Curso intitulado:

RECONHECIMENTO FACIAL, INTELIGÊNCIA ARTIFICIAL E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Elaborado por Henrique Bueno Dib Figueira, apresentado publicamente perante a Banca Avaliadora como parte dos requisitos para conclusão do Curso de Direito.

Aprovado em 25 de novembro de 2024

Banca Avaliadora:

.....

Carlos José Pacheco - UniFOA

.....

Izabelle Maria Patitucci de Azevedo - UniFOA

.....

Tania Cristina Prado - UniFOA

Dedico este trabalho a todos os que me ajudaram ao longo desta caminhada.

AGRADECIMENTOS

Agradeço a Deus por me dar forças para correr atrás dos meus sonhos.

À minha namorada, por todo o carinho, compreensão e motivação durante este período. Sua presença e incentivo foram fundamentais para que eu pudesse superar os desafios dessa caminhada.

Ao meu orientador por me inspirar em meu tema e por todo o suporte oferecido.

Aos meus pais e familiares, pela paciência, amor e apoio incondicional em cada passo da minha formação acadêmica.

RESUMO

Este trabalho aborda a utilização da inteligência artificial e o reconhecimento facial inseridos na sociedade, e investiga os aspectos jurídicos, direitos individuais e proteção de dados pessoais relacionados a essa tecnologia. O reconhecimento facial é uma tecnologia em ascensão que oferece uma ampla gama de aplicações em diferentes setores, como segurança, comércio e serviços. No entanto, seu uso levanta preocupações significativas em relação à privacidade dos indivíduos, bem como à coleta, armazenamento e compartilhamento de dados pessoais. O objetivo deste trabalho é analisar os aspectos jurídicos do uso do reconhecimento facial, com foco nos direitos individuais e na proteção de dados pessoais. Serão examinados os marcos legais existentes, como a legislação de privacidade e proteção de dados, bem como as questões éticas e sociais relacionadas ao reconhecimento facial. Além disso, serão apresentados estudos de casos para ilustrar os impactos reais do uso dessa tecnologia. Ao final, serão discutidas as medidas regulatórias e as recomendações para garantir a utilização responsável e ética do reconhecimento facial.

Palavras-chave: Reconhecimento facial; Inteligência artificial; Lei Geral de Proteção de Dados; Direitos fundamentais.

ABSTRACT

This work addresses the use of artificial intelligence and facial recognition in society, and investigates the legal aspects, individual rights and protection of personal data related to this technology. Facial recognition is a growing technology that offers a wide range of applications in different sectors such as security, commerce and services. However, its use raises significant concerns regarding the privacy of individuals, as well as the collection, storage and sharing of personal data. The objective of this work is to analyze the legal aspects of the use of facial recognition, focusing on individual rights and the protection of personal data. Existing legal frameworks will be examined, such as privacy and data protection legislation, as well as ethical and social issues related to facial recognition. In addition, case studies will be presented to illustrate the real impacts of using this technology. Finally, regulatory measures and recommendations to ensure the responsible and ethical use of facial recognition will be discussed.

Keywords: Facial recognition; Artificial intelligence; General Data Protection Law; Fundamental rights

SUMÁRIO

1. INTRODUÇÃO

Com o avanço da tecnologia de reconhecimento facial, surge a necessidade de uma análise aprofundada dos aspectos jurídicos, direitos individuais e proteção de dados pessoais relacionados a essa tecnologia.

O problema de estudo consiste em compreender os desafios e implicações legais decorrentes da utilização do reconhecimento facial em diferentes contextos presentes em nossa sociedade, como segurança pública, comércio, serviços públicos e etc.

Essa tecnologia permite a identificação e autenticação de indivíduos por meio de características faciais únicas. No entanto, seu uso generalizado pode levantar preocupações em relação à privacidade e violação dos direitos individuais. Por exemplo, o monitoramento em tempo real por câmeras de reconhecimento facial em espaços públicos pode ser visto como uma invasão da privacidade das pessoas, uma vez que suas imagens são coletadas e analisadas sem o consentimento explícito.

Além disso, a coleta e o armazenamento de dados biométricos, como imagens faciais, levantam questões sobre a proteção de dados pessoais. Como essas informações são altamente sensíveis e podem ser usadas para a identificação única de um indivíduo, é essencial garantir que existam salvaguardas adequadas para proteger esses dados contra acessos não autorizados ou usos indevidos.

A utilização do reconhecimento facial tem se expandido rapidamente em diferentes setores, como segurança pública, controle de acesso, comércio e serviços públicos. Embora essa tecnologia apresente benefícios em termos de eficiência, segurança e praticidade, também levanta preocupações significativas que devem ser devidamente abordadas.

Este trabalho será estruturado em quatro capítulos principais, cada um abordando aspectos essenciais para uma análise completa da tecnologia de reconhecimento facial e seus impactos legais, éticos e de proteção de dados.

Neste sentido, o capítulo segundo explora o conceito e a evolução histórica da Inteligência Artificial (IA), oferecendo uma introdução essencial para o entendimento das tecnologias modernas, incluindo o reconhecimento facial. Este

capítulo aborda o desenvolvimento da IA desde suas origens até os dias atuais, detalhando suas categorias principais, como o aprendizado de máquina, redes neurais artificiais e aprendizado profundo. Também discute o funcionamento desses sistemas e suas diversas aplicações, enfatizando como essas tecnologias se tornaram parte do cotidiano e fornecendo a base técnica necessária para contextualizar o reconhecimento facial dentro do escopo da IA.

Por consequência, no capítulo terceiro, o foco é voltado especificamente para a tecnologia de reconhecimento facial, uma aplicação particular da IA com um grande impacto em segurança, controle de acesso e autenticação de usuários. O capítulo define o conceito de reconhecimento facial, explica seu funcionamento técnico e examina suas principais aplicações, como em dispositivos móveis e sistemas de vigilância pública. Além disso, é apresentado um panorama do enquadramento legal e normativo da tecnologia, tanto em âmbito nacional quanto internacional, destacando leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e regulamentações internacionais que visam garantir a privacidade e a proteção dos direitos individuais.

O capítulo quarto trata das questões éticas e dos direitos fundamentais relacionados ao reconhecimento facial, com um enfoque na proteção de dados pessoais. Este capítulo discute como o uso dessa tecnologia pode afetar os direitos fundamentais, como o direito à privacidade e a liberdade individual, e explora a legislação de proteção de dados que regula o uso de informações biométricas sensíveis. Além disso, analisa as implicações éticas e o viés algorítmico que podem surgir no uso de sistemas de Inteligência Artificial, ressaltando a importância de uma abordagem ética para mitigar possíveis discriminações e abusos no emprego de tecnologias de reconhecimento facial.

No capítulo quinto, são apresentados os desafios e as controvérsias associados ao uso do reconhecimento facial, bem como as medidas regulatórias propostas para promover uma aplicação responsável e ética da tecnologia. Este capítulo discute as preocupações com a transparência dos algoritmos, a segurança dos dados e a precisão dos sistemas, especialmente no contexto de segurança pública e vigilância em massa. Propõe ainda princípios e diretrizes para o uso ético do reconhecimento facial, abordando a importância da responsabilidade e da supervisão na implementação dessa tecnologia, com o objetivo de minimizar os riscos à privacidade e aos direitos individuais.

2. CONCEITO E EVOLUÇÃO HISTÓRICA DA INTELIGÊNCIA ARTIFICIAL

Este capítulo apresenta uma abordagem sobre a Inteligência Artificial (IA), incluindo sua definição, histórico, categorias e aplicações. Além disso, discute-se o funcionamento da IA abordando os principais componentes e técnicas utilizadas. O objetivo é fornecer uma visão geral dos conceitos e fundamentos essenciais para compreender a inteligência artificial.

A Inteligência Artificial (IA) não é mais um conceito distante ou uma mera ficção, mas algo presente em nossas vidas diárias. Ela está integrada em várias atividades cotidianas que envolvem dispositivos e equipamentos modernos, bem como em sistemas de alta complexidade. Por exemplo, a Inteligência Artificial é fundamental ao realizar uma busca no Google, utilizar serviços de streaming, fazer compras online e até também para o funcionamento das redes sociais.

Atualmente, a Inteligência Artificial está tão entrelaçada em nossa rotina que muitas vezes nem se percebe sua presença. Ela possibilita a personalização de recomendações de conteúdo com base em nossos interesses e preferências, como sugestões de músicas, filmes ou produtos. Assistentes virtuais, como a Siri, Alexa e o Google Assistant, são exemplos de como a IA se tornou parte integrante de nossos dispositivos e nos ajuda a realizar tarefas simples.

2.1 Breve História da Inteligência Artificial

Há séculos a inteligência artificial já é utilizada, equipamentos eram usados para marcar o tempo e simular comportamento de animais. Com o tempo foram feitos relógios, técnicas para se calcular, como o ábaco, até chegar aos computadores. (BITTENCOURT, 2001).

Em 1943, Warren McCulloch e Walter Pitts realizaram o primeiro trabalho reconhecido como Inteligência Artificial. De acordo com Russell e Norvig (2004), Warren e Walter basearam-se em três fontes: “o conhecimento da fisiologia básica e da função dos neurônios no cérebro; uma análise formal da lógica proposicional criada por Russell e Whitehead; e a teoria da computação de Turing”. Os pesquisadores propuseram um modelo de neurônios artificiais em que cada neurônio pode estar

"ligado" ou "desligado", sendo ativado quando estimulado por um número suficiente de neurônios vizinhos. O estado do neurônio era “equivalente em termos concretos a uma proposição que definia seu estímulo adequado” (RUSSELL; NORVIG, 2004). Por exemplo, eles demonstraram que qualquer função computável pode ser calculada por uma determinada rede de neurônios interconectados e que todos os conectivos lógicos (como "e", "ou" e "não") podem ser implementados por estruturas de redes simples.

Ao longo dos anos, surgiram várias contribuições no campo da Inteligência Artificial (IA), mas um destaque importante é atribuído às obras de Alan Turing, conhecido como o "pai da computação". A partir de 1947, Turing começou a ministrar palestras sobre o tema na Sociedade Matemática de Londres. Em seu artigo de 1950, intitulado "Computing Machinery and Intelligence", Turing apresentou o famoso teste de Turing, além dos conceitos de aprendizagem de máquina, aprendizagem por reforço e algoritmos genéticos. Essa obra singular estabeleceu Turing como um pioneiro no campo da IA (RUSSEL; NORVIG, 2004).

A história da inteligência artificial remonta ao século XX, com marcos importantes como o teste de Turing e o desenvolvimento de algoritmos de aprendizado de máquina. Ao longo do tempo, a IA foi dividida em diferentes categorias, como IA fraca (ou estreita) e IA forte (ou geral).

A IA fraca refere-se aos sistemas construídos que podem ser considerados "inteligentes" em certa medida, mas não possuem a capacidade de raciocinar autonomamente. Por exemplo, um motor de inferência ou um chatbot consistem essencialmente em uma série de condicionais “if-then” (em português "se-então") encadeados. Eles não possuem capacidade de raciocínio ou vontades próprias, pois dependem do conhecimento fornecido por um humano como entrada, enquanto a IA forte busca criar máquinas inteligentes que possuam a capacidade de igualar ou superar a inteligência. Assim como uma criança em fase de aprendizado, a máquina de IA precisa adquirir conhecimento por meio de entradas e experiências, progredindo continuamente e aprimorando suas habilidades ao longo do tempo.

2.2 O Funcionamento da Inteligência Artificial

Inteligência Artificial é a parte da ciência da computação voltada para o desenvolvimento de sistemas de computadores inteligentes, ou seja, sistemas que exibem características, as quais se relacionam com a inteligência no comportamento do homem. (FERNANDES, 2003)

Trata-se de uma disciplina que almeja dotar máquinas e sistemas computacionais com a capacidade de simular processos cognitivos e comportamentos humanos, mediante a aplicação de algoritmos sofisticados e estruturas de aprendizado. Com habilidades multifacetadas, a inteligência artificial busca compreender, raciocinar, adaptar-se e tomar decisões de maneira autônoma, navegando em vastos oceanos de dados e aproveitando-se de padrões complexos para obter insights e soluções.

> A Inteligência Artificial (I.A.) é “um ramo da Ciência da Computação cujo interesse é fazer com que os computadores pensem ou se comportem de forma inteligente” (GOMES, 2010, p. 239)

A inteligência artificial tem alcançado avanços impressionantes, impulsionados pelo crescimento exponencial da capacidade de processamento e pela disponibilidade de grandes volumes de dados. Essas melhorias têm se refletido em diversas áreas, desde o desenvolvimento de softwares que auxiliam na descoberta de novos medicamentos até algoritmos capazes de prever nossos interesses culturais.

O termo *Soft Computing* representa a combinação de tecnologias inteligentes, como a lógica fuzzy, raciocínio probabilístico, redes neurais artificiais (RNA) e algoritmos genéticos para a resolução de problemas. Cada uma dessas tecnologias proporciona raciocínio e buscam métodos complementares para resolver problemas complexos do mundo real (BONISSONE, 1997).

2.2.1 Aprendizado de Máquina (Machine Learning)

Existem diferentes abordagens para a criação de sistemas de IA, como o aprendizado de máquina (*Machine Learning*), sendo uma técnica que permite que as

máquinas aprendam a partir de dados e melhorem seu desempenho ao longo do tempo.

> Em 1959, Arthur Lee Samuel, pioneiro norte-americano no campo de jogos de computador e Inteligência Artificial, cunhou o termo “machine learning” (ML) (enquanto funcionário da IBM), inaugurando um subcampo da IA cuja finalidade é prover os computadores da capacidade de aprender sem serem programados. (KAUFMAN, 2018, p. 20)

O *Machine Learning* pode ser dividido em duas categorias principais: o aprendizado supervisionado, em que os algoritmos são treinados usando um conjunto de dados rotulados, o conjunto de dados consiste em exemplos de entrada, chamados de amostras, e as saídas desejadas correspondentes, chamadas de rótulos. O objetivo do modelo é aprender uma função que mapeie as entradas para as saídas corretas com base nos exemplos de treinamento. Já no aprendizado não supervisionado, os algoritmos são treinados em conjuntos de dados não rotulados. o objetivo principal é descobrir padrões, estruturas ou relações intrínsecas nos dados sem a necessidade de rótulos pré-existentes. O modelo é exposto aos dados e tenta encontrar características ou agrupamentos que possam explicar a estrutura subjacente dos dados.

> Evoluindo a partir do estudo do reconhecimento de padrões e da teoria de aprendizagem computacional na Inteligência Artificial, o *machine learning* explora o estudo e a construção de algoritmos que, seguindo instruções, fazem previsões ou tomam decisões baseadas em dados – modelos elaborados a partir de entradas de amostras. (KAUFMAN, 2018, p. 20)

2.2.2 Redes Neurais Artificiais (RNA)

Uma das principais técnicas usadas no aprendizado de máquina é a rede neural artificial (RNA). As redes neurais são um modelo computacional inspirado no funcionamento do cérebro humano. É composta por um conjunto de unidades de processamento interconectadas, chamadas de neurônios artificiais ou unidades de processamento, que trabalham em conjunto para realizar tarefas de processamento de informações. Elas podem ser definidas como um conjunto de unidades de processamento, caracterizadas por neurônios artificiais, que são interligados por um grande número de interconexões.

> As redes neurais artificiais são metodologias computacionais desenvolvidas com base no sistema nervoso humano. Possuem capacidade de adquirir conhecimento (baseado em experiências anteriores) e podem ser definidas como unidades de processamento, caracterizadas por neurônios artificiais, que são interligados por um grande número de interconexões (sinapses artificiais), sendo representadas aqui por vetores/matrizes de pesos sinápticos (DA SILVA, SPATTI, FLAUZINO, 2010, p.34).

As redes neurais artificiais (RNA) constituem uma forma de aproximação universal de funções, que apresenta um desempenho satisfatório durante a interpretação e classificação de padrões complexos. Estas são também bastante versáteis e podem aprender continuamente, além de apresentarem capacidade de generalização e alto desempenho computacional, devido ao seu forte paralelismo (BUTLER ET AL., 1997).

> As redes neurais são inspiradas nos processos e estruturas cerebrais, sendo compostas por nós que recebem informações e as transferem mediante conexões ponderadas entre camadas, em geral definidas como de entrada, ocultas e de saída. (CARDOSO JR, ROLIM & ZÜRN, 2004, p.7)

As redes neurais artificiais são organizadas em camadas, que consistem em grupos de neurônios artificiais conectados. A primeira camada é chamada de camada de entrada e recebe os dados de entrada. A última camada é chamada de camada de saída e produz as respostas ou previsões finais do modelo. As camadas intermediárias entre a camada de entrada e a camada de saída são chamadas de camadas ocultas. As conexões entre os neurônios são representadas por pesos sinápticos. Cada conexão possui um peso associado que determina a força e a direção da influência da entrada correspondente sobre o neurônio de destino. Durante o treinamento da rede neural, os pesos sinápticos são ajustados iterativamente para melhorar o desempenho do modelo.

O treinamento de uma rede neural envolve o processo de ajuste dos pesos sinápticos para que a rede seja capaz de aprender e realizar a tarefa desejada. O objetivo é encontrar uma configuração de pesos que minimize uma função de perda (ou função de custo), que mede o quão bem o modelo está realizando a tarefa.

O treinamento geralmente é realizado utilizando um algoritmo chamado de *backpropagation* (retropropagação). Esse algoritmo calcula o gradiente da função de

perda em relação aos pesos sinápticos e ajusta-os na direção oposta ao gradiente, utilizando um método de otimização, como o gradiente descendente.

As RNAs são capazes de aprender a partir de dados, reconhecer padrões complexos, generalizar informações e tomar decisões. Elas têm sido aplicadas em uma ampla variedade de áreas, incluindo reconhecimento de padrões, processamento de linguagem natural, visão computacional, previsão de séries temporais, jogos, entre outros. As redes neurais profundas (*Deep Learning*), são particularmente eficazes em tarefas complexas, como reconhecimento de imagem e processamento de linguagem natural.

2.2.3 Aprendizado Profundo (Deep Learning)

O *Deep Learning*, ou aprendizado profundo, é uma abordagem específica dentro do campo do aprendizado de máquina (*machine learning*) que se baseia no uso de redes neurais artificiais profundas. Ao contrário de modelos mais rasos, as redes neurais profundas possuem múltiplas camadas ocultas, permitindo uma representação hierárquica e complexa dos dados.

A camada de Entrada recebe os dados brutos de entrada, que podem ser imagens, texto, áudio, entre outros. Cada unidade nesta camada representa uma característica específica dos dados, como um pixel de uma imagem ou uma palavra em um texto.

As camadas ocultas são responsáveis por aprender características cada vez mais complexas dos dados. Cada neurônio em uma camada oculta recebe as saídas da camada anterior, realiza uma soma ponderada dessas entradas e aplica uma função de ativação. À medida que os dados fluem pelas camadas ocultas, características mais abstratas e de alto nível são extraídas. Por exemplo, em uma rede neural para reconhecimento de imagens, as primeiras camadas podem aprender a detectar bordas e texturas, enquanto as camadas mais profundas podem aprender a identificar objetos e rostos.

A camada de saída produz a resposta final do modelo. Ela recebe as saídas das camadas ocultas, realiza uma soma ponderada e aplica uma função de ativação adequada para a tarefa específica. Por exemplo, em um problema de classificação, a

função de ativação da camada de saída pode ser uma função *softmax,* que retorna a probabilidade de cada classe.

Durante o treinamento do modelo, os pesos sinápticos das conexões entre os neurônios são ajustados para que o modelo seja capaz de fazer previsões precisas. Isso é feito por meio de um processo iterativo chamado *backpropagation* (retropropagação). Durante o *backpropagation*, o erro entre as previsões do modelo e os rótulos verdadeiros é propagado de volta pela rede neural, e os pesos sinápticos são atualizados de acordo com o gradiente descendente.

Essa estrutura hierárquica permite que o modelo aprenda automaticamente as características relevantes para realizar a tarefa desejada, em vez de depender de características manualmente projetadas ou selecionadas. Essa capacidade de aprendizado automático de recursos é uma das principais vantagens do deep learning e depende da disponibilidade de um grande volume de dados de treinamento e recursos computacionais adequados para lidar com a complexidade dos modelos profundos.

O *deep learning* tem sido amplamente utilizado em diversas áreas, trazendo benefícios significativos para a sociedade. Uma das aplicações mais bem-sucedidas é a visão computacional, onde ele é utilizado para reconhecimento de imagem, detecção e segmentação de objetos, classificação de imagens e muito mais. Por exemplo, atividades de reconhecimento facial, o *deep learning* é capaz de identificar e autenticar indivíduos com alta precisão.

Outra área em que tem tido um impacto significativo é o processamento de linguagem natural. Ele revolucionou a forma como lidamos com texto e linguagem. Com o uso do *deep learning*, temos sistemas de tradução automática que melhoraram significativamente a comunicação entre idiomas. Além disso, também é aplicado na análise de sentimentos em texto, geração de texto automático e respostas automáticas em assistentes virtuais. Proporcionando uma interação mais natural e eficiente entre humanos e máquinas.

O reconhecimento de fala é outra aplicação de destaque do deep learning. Graças a essa tecnologia, temos assistentes virtuais, como Siri, Alexa e Google Assistant, que são capazes de entender e responder aos comandos de voz dos

usuários e também é empregado em tarefas de transcrição automática de áudio, permitindo converter facilmente áudio em texto, o que é útil em diversas situações.

Na área da medicina tem sido utilizado com sucesso. Ele é aplicado no diagnóstico médico, análise de imagens médicas, detecção de câncer, análise de genoma, entre outros. Essas aplicações ajudam a melhorar a precisão do diagnóstico, permitindo tratamentos mais eficazes e contribuindo para a medicina personalizada.

Na automatização industrial é utilizado para o controle de processos, otimização de produção e detecção de falhas em equipamentos. Tornando, os sistemas automatizados mais inteligentes e capazes de aprender com os dados coletados, resultando em maior eficiência e confiabilidade dos processos industriais.

Essas aplicações do *deep learning* representam apenas uma pequena amostra do seu potencial. À medida que essa área continua a se desenvolver, espera-se que novas aplicações surjam, trazendo ainda mais benefícios para diversos setores da sociedade.

2.2.4 Lógica Fuzzy

Outra abordagem importante na Inteligência Artificial é a lógica fuzzy, ao contrário da lógica booleana que trabalha com valores binários (verdadeiro ou falso), a lógica fuzzy permite que um valor possua um grau de pertinência em um intervalo contínuo entre 0 e 1. Esses valores são chamados de graus de pertinência ou graus de verdade e indicam o quão verdadeira ou falsa uma proposição é em relação a um determinado critério. Também conhecida como lógica difusa, é uma extensão da lógica booleana tradicional que lida com a incerteza e a imprecisão presentes em muitos problemas do mundo real. Ela foi proposta por Lotfi Zadeh em 1965 como uma forma de representar e raciocinar sobre informações vagas e subjetivas.

> A lógica clássica aristotélica é bivalente, isto é, reconhece somente dois valores: verdadeiro ou falso, enquanto a lógica fuzzy é multivalorada, isto é, reconhece diversos valores, assegurando que a verdade é uma questão de ponto de vista ou de graduação. A lógica fuzzy possibilita tratar de um modo mais adequado expressões verbais, imprecisas, qualitativas, inerentes da comunicação humana, que possuem vários graus de imprecisão e pode sistematicamente traduzir os termos difusos da comunicação humana em valores compreensíveis por computadores. (SILVEIRA, FURTADO, OLIVEIRA, E DA COSTA, 2004)

Esta lógica utiliza conjuntos fuzzy, que são conjuntos cujos elementos podem ter graus variados de pertinência. Por exemplo, em vez de dizer que uma pessoa é alta ou baixa, pode-se usar um conjunto fuzzy de altura que representa a altura de uma pessoa em termos de graus de pertinência, como "alta", "média" ou "baixa".

A lógica fuzzy encontra diversas aplicações práticas em diferentes tipos de sistemas. Por exemplo, em sistemas de reconhecimento de faces ou padrões, ela é utilizada para reconhecer e classificar objetos em imagens, como faces humanas em sistemas de segurança ou padrões em sistemas de visão computacional.

Além disso, a lógica fuzzy é aplicada em sistemas de apoio à decisão, onde lida com informações imprecisas e incertas para auxiliar na tomada de decisões. Isso pode ser visto em sistemas de avaliação de crédito, sistemas de recomendação de produtos e sistemas de gerenciamento de risco.

Outra área de aplicação é em sistemas de cálculo e gerenciamento de risco. A lógica fuzzy é empregada em análises de risco financeiro, seguros e investimentos, permitindo considerar a incerteza e a imprecisão nas estimativas.

A lógica fuzzy também desempenha um papel importante nos sistemas de condução de veículos autônomos. Ela é utilizada no processo de tomada de decisões dos veículos, permitindo que eles lidem com informações imprecisas e incertas do ambiente, como a detecção de obstáculos e a escolha de trajetórias.

2.2.5 Processamento de Linguagem Natural (PLN)

O Processamento de Linguagem Natural (PLN) refere-se ao campo de estudo e aplicação da inteligência artificial que se concentra na interação entre computadores e a linguagem humana. O objetivo do PLN é capacitar as máquinas a compreender, interpretar e gerar linguagem humana de maneira similar aos seres humanos. É um campo desafiador e complexo que busca extrair significado e conhecimento de textos escritos ou falados.

O PLN tem diversas aplicações práticas, como chatbots, assistentes virtuais, sistemas de tradução automática, análise de sentimentos em mídias sociais, sistemas de recomendação personalizados, extração de informações de grandes volumes de

texto, entre outros. É uma área de pesquisa ativa e em constante evolução, com muitos desafios a serem enfrentados, como a ambiguidade da linguagem, o reconhecimento de ironia ou sarcasmo e a compreensão de contextos complexos.

2.2.6 Big Data

Big Data é um termo utilizado para descrever conjuntos de dados extremamente grandes e complexos, que são difíceis de serem gerenciados, processados e analisados pelos métodos tradicionais. Esses conjuntos de dados denominadas por Laney (2001), como "três Vs": Volume (grande quantidade de dados), Velocidade (alta taxa de geração e processamento dos dados) e Variedade (diversidade de formatos e tipos de dados).

O volume de dados em Big Data refere-se à enorme quantidade de informações que são geradas e armazenadas diariamente. Esses dados podem vir de várias fontes, como redes sociais, sensores, dispositivos móveis, transações comerciais, registros de saúde e muito mais. A escala do volume de dados em Big Data é geralmente medida em terabytes, petabytes, exabytes e além.

> Qualquer interação com tecnologias digitais deixa “rastros”, alguns voluntários como as publicações nas redes sociais – Facebook, Twitter e Instagram –, e outros involuntários, como as informações armazenadas nos bancos de dados digitais na compra com cartão de crédito, na movimentação bancária online, no acesso aos programas de fidelidade, no vale-transporte, nas comunicações por telefonia móvel, e inúmeras outras ações presentes em nossa rotina. (KAUFMAN, 2018, p. 25)

A velocidade está relacionada à taxa na qual os dados são gerados, transmitidos e processados. Com a proliferação de dispositivos conectados à Internet e a rápida troca de informações em tempo real, os dados em Big Data são gerados em uma velocidade impressionante. Isso requer soluções de armazenamento, processamento e análise capazes de lidar com altas taxas de ingestão e processamento de dados em tempo real.

A variedade refere-se à diversidade de tipos e formatos de dados presentes em Big Data. Os dados podem ser estruturados (como bancos de dados tradicionais), semiestruturados (como arquivos XML e JSON) e não estruturados (como e-mails,

imagens, vídeos, redes sociais). A variedade dos dados em Big Data apresenta desafios adicionais, pois diferentes técnicas e ferramentas precisam ser empregadas para lidar com cada tipo de dado.

O conceito de Big Data refere-se não apenas ao tamanho dos dados, mas também à capacidade de extrair informações e conhecimentos valiosos desses conjuntos de dados para tomar decisões e obter insights significativos. Com o crescimento exponencial da quantidade de dados gerados por empresas, dispositivos conectados e interações digitais, o Big Data tornou-se uma área de grande importância na era digital.

Para lidar com o Big Data, são utilizadas técnicas e tecnologias avançadas, como computação em nuvem, armazenamento distribuído, processamento paralelo e algoritmos de aprendizado de máquina. Essas ferramentas permitem a coleta, o armazenamento, o processamento e a análise eficiente desses grandes volumes de dados, possibilitando a descoberta de padrões, a identificação de tendências, a personalização de serviços e a tomada de decisões baseadas em dados.

> Big data requer formas inovadoras de processamento de grandes volumes de dados heterogêneos, amparando o processo de tomada de decisão guiado por dados (RAUTENBERG; CARMO, 2019, p. 57)

O objetivo do Big Data é extrair valor dos dados, gerando insights acionáveis que possam impulsionar a inovação, melhorar a eficiência operacional, aumentar a vantagem competitiva e aprimorar a experiência do usuário. É importante ressaltar que a gestão adequada do Big Data também envolve preocupações com privacidade, segurança e ética na coleta, armazenamento e análise dos dados, garantindo o uso responsável e proteção dos dados pessoais.

> Big data refere-se a coisas que se pode fazer em grande escala para extrair novos insights ou criar novas formas de valor, mudando os mercados, as organizações, a relação entre cidadãos e governos e muito mais. (KAUFMAN, 2018, p. 24)

Nesse contexto, a utilização do Big Data deve ser equilibrada com a observância de princípios legais e éticos, especialmente no que tange à proteção de dados pessoais e à privacidade dos indivíduos.

2.3 Aplicações da Inteligência Artificial

A inteligência artificial tem se tornado cada vez mais presente em nosso cotidiano, oferecendo uma variedade de aplicações que facilitam e melhoram nossas experiências. Uma delas é o reconhecimento facial, onde algoritmos de inteligência artificial são utilizados para identificar e autenticar pessoas com base em características faciais únicas. Essa tecnologia é amplamente aplicada em em sistemas de segurança para controle de acesso, smartphones para desbloqueio facial, e até mesmo em redes sociais para reconhecimento de amigos em fotos.

Outra aplicação comum é a presença de assistentes pessoais em nossos dispositivos. Além dos assistentes virtuais, como a Siri, Alexa e Google Assistant, temos assistentes pessoais em nossos smartphones, como o Google Now e o Microsoft Cortana. Esses assistentes utilizam a inteligência artificial para aprender sobre nossos hábitos, preferências e necessidades, oferecendo informações relevantes, como previsão do tempo, notícias atualizadas, sugestões de restaurantes e eventos, entre outros.

No setor financeiro, a inteligência artificial tem desempenhado um papel fundamental na detecção de fraudes e na gestão de riscos. Algoritmos de aprendizado de máquina são capazes de analisar grandes volumes de dados financeiros em tempo real, identificando padrões suspeitos que podem indicar atividades fraudulentas. Isso ajuda a proteger instituições financeiras e clientes, evitando prejuízos e garantindo a segurança das transações.

No campo do atendimento ao cliente, os chatbots têm se tornado cada vez mais comuns. Esses assistentes virtuais utilizam técnicas de processamento de linguagem natural e inteligência artificial para interagir com os clientes, responder perguntas e fornecer suporte. Eles podem agilizar o atendimento, melhorar a experiência do cliente e reduzir os custos operacionais das empresas.

A personalização de recomendações de compras é uma aplicação comum em plataformas de comércio eletrônico. Algoritmos de inteligência artificial analisam o histórico de compras, preferências do cliente e comportamento de navegação para oferecer recomendações personalizadas de produtos. Isso melhora a experiência de

compra, ajudando os usuários a descobrir produtos relevantes de acordo com seus interesses.

Os carros autônomos são uma aplicação revolucionária da inteligência artificial. Sensores e câmeras coletam dados do ambiente ao redor do veículo, enquanto algoritmos de aprendizado de máquina processam esses dados em tempo real para tomar decisões de direção seguras. Essa tecnologia promete transformar a indústria automobilística, tornando a condução mais segura e eficiente.

As aplicações da inteligência artificial são extremamente amplas e estão transformando o modo como vivemos, trabalhamos e interagimos com o mundo ao nosso redor, o que levanta questões controversas que precisam ser cuidadosamente consideradas.

Um dos principais pontos de debate é a privacidade e a proteção de dados. Com o uso da inteligência artificial, grandes quantidades de informações pessoais são coletadas, o que suscita preocupações sobre o acesso e o uso desses dados. A necessidade de regulamentações e leis de proteção de dados se torna crucial para garantir a privacidade dos indivíduos e evitar o mau uso dessas informações sensíveis.

Outra questão polêmica é o viés e a discriminação algorítmica. Os algoritmos de inteligência artificial são alimentados com dados de treinamento, que podem conter preconceitos ou tendências discriminatórias. Isso pode levar a decisões injustas ou discriminatórias quando aplicadas em contextos reais. É fundamental a transparência nos processos de treinamento e aplicação dos algoritmos, bem como a diversidade nos dados utilizados.

Entre as diversas aplicações da inteligência artificial, o reconhecimento facial destaca-se como uma das mais impactantes e controversas. Essa tecnologia levanta debates significativos sobre privacidade, proteção de dados e possíveis vieses discriminatórios em sua implementação. No próximo capítulo, será abordado o funcionamento do reconhecimento facial, suas principais utilizações e os desafios legais e éticos que surgem com sua adoção. Essa análise permitirá compreender como essa ferramenta se insere no contexto da inteligência artificial e quais são as implicações para a sociedade contemporânea.

3. TECNOLOGIA DE RECONHECIMENTO FACIAL

A tecnologia de reconhecimento facial representa uma das aplicações mais avançadas e controversas da inteligência artificial, sendo amplamente utilizada em diversos setores, como segurança pública, autenticação digital e marketing. Essa tecnologia baseia-se na identificação de características faciais únicas para verificar ou reconhecer a identidade de indivíduos, oferecendo praticidade e eficiência em suas aplicações. No entanto, seu uso crescente também levanta questões críticas relacionadas à privacidade, proteção de dados pessoais e possíveis discriminações algorítmicas. Neste capítulo, será explorado o funcionamento dessa tecnologia, suas principais aplicações e os desafios éticos e jurídicos que envolvem sua implementação, com foco nas implicações para a sociedade e no equilíbrio entre inovação tecnológica e direitos fundamentais.

3.1 Conceito de Reconhecimento Facial e Aplicações

O reconhecimento facial tem suas raízes em pesquisas e avanços tecnológicos ao longo das últimas décadas. Nos anos 1960 e 1970, os primeiros experimentos em reconhecimento facial automatizado começaram a surgir. Os pesquisadores exploraram técnicas baseadas em geometria facial, como a medição de distâncias e ângulos entre características faciais, para identificar indivíduos. Esses sistemas iniciais eram limitados em precisão e eficiência devido à tecnologia disponível na época.

À medida que a tecnologia avançava, o reconhecimento facial se beneficiou de progressos em áreas como processamento de imagens, inteligência artificial e aprendizado de máquina. Isso permitiu o desenvolvimento de algoritmos mais sofisticados e eficientes para a identificação e verificação de rostos.

Nos anos 1990 e 2000, surgiram abordagens baseadas em características faciais, como a identificação de pontos-chave ou características únicas do rosto, como olhos, nariz e boca. Esses sistemas usavam algoritmos para extrair e comparar essas características entre diferentes imagens faciais.

Mais recentemente, com o advento do aprendizado profundo (*deep learning*) e redes neurais artificiais, houve um avanço significativo no reconhecimento facial. Essas técnicas permitiram o desenvolvimento de modelos mais complexos e precisos, capazes de reconhecer padrões e características faciais com maior acurácia.

Com o avanço da tecnologia, a capacidade de processamento de imagens melhorou significativamente, permitindo o desenvolvimento de algoritmos mais eficientes e precisos. Além disso, o surgimento de grandes conjuntos de dados e técnicas de aprendizado de máquina impulsionaram ainda mais o progresso do reconhecimento facial.

O rosto, assim como as impressões digitais, constitui uma forma de biometria, ou seja, dados específicos e exclusivos que variam de indivíduo para indivíduo. Da mesma forma que as pessoas podem ser identificadas por meio de suas impressões digitais, elas também podem ser identificadas pelo registro preciso de seus rostos.

O primeiro passo no reconhecimento facial é detectar um rosto na imagem. Isso é feito usando algoritmos que identificam características faciais, como a posição dos olhos, nariz e boca. Uma vez que o rosto é detectado, o próximo passo é extrair características do rosto. Isso pode incluir detalhes como a distância entre os olhos, o formato do nariz, a largura da boca, etc. As características extraídas são então comparadas com as características de rostos conhecidos em um banco de dados. Isso é feito usando algoritmos de aprendizado de máquina que são capazes de identificar padrões e fazer correspondências.

Finalmente, o sistema identifica o rosto como pertencente a uma pessoa específica no banco de dados (identificação) ou verifica se o rosto corresponde a um rosto específico no banco de dados (verificação).

Uma das aplicações mais comuns do reconhecimento facial é em sistemas de segurança e controle de acesso. Ele é usado para identificar e autenticar indivíduos em locais de alta segurança, como aeroportos, edifícios governamentais e empresas. O reconhecimento facial substitui métodos tradicionais de identificação, como cartões de acesso ou senhas, oferecendo uma forma mais segura e conveniente de autenticação.

Em locais de grande fluxo de pessoas, como estádios esportivos, estações de metrô e aeroportos, o reconhecimento facial é usado para monitorar multidões e

identificar pessoas suspeitas ou procuradas pelas autoridades. Ele pode ser integrado a sistemas de vigilância por câmeras para identificar e rastrear indivíduos em tempo real.

Outra aplicação do reconhecimento facial está relacionada à identificação criminal e investigação. Agências de segurança e aplicação da lei utilizam essa tecnologia para comparar rostos de suspeitos com registros criminais ou imagens de câmeras de vigilância. Essa abordagem auxilia na identificação e captura de indivíduos envolvidos em atividades criminosas.

Muitos dispositivos móveis, como smartphones e tablets, possuem recursos de desbloqueio facial. Esses sistemas utilizam o reconhecimento facial como uma medida de segurança biométrica para autenticar o usuário e desbloquear o dispositivo. Além disso, pode ser usado para autorizar pagamentos e transações bancárias em dispositivos móveis.

O reconhecimento facial tem uma ampla gama de aplicações, incluindo segurança e controle de acesso, autenticação em dispositivos móveis, monitoramento de multidões, análise de emoções, detecção de expressões faciais e muito mais. No entanto, sua implementação levanta preocupações éticas e legais, como privacidade, segurança de dados e viés algorítmico.

Embora tenha demonstrado ser uma tecnologia poderosa, é importante ressaltar que seu uso também levanta questões éticas, legais e de privacidade. É essencial garantir a proteção dos dados pessoais, o controle de acesso adequado e o uso responsável da tecnologia para mitigar qualquer risco potencial e garantir benefícios efetivos em todas as suas aplicações.

3.2 Enquadramento Legal e Normativo do Uso de Reconhecimento Facial

Atualmente, as autoridades estatais têm utilizado diversas ferramentas tecnológicas para auxiliar na segurança pública. Entre essas ferramentas, destacam-se as escutas telefônicas, o uso de câmeras de vigilância e o estudo estatístico para melhorar a eficiência das operações policiais em áreas e horários específicos.

As escutas telefônicas têm sido empregadas para monitorar comunicações suspeitas, permitindo que as autoridades obtenham informações relevantes para investigações criminais. As câmeras de vigilância são amplamente utilizadas para monitorar locais públicos, como ruas, praças e edifícios, com o objetivo de prevenir e detectar atividades criminosas.

Além disso, o estudo estatístico é uma prática adotada para identificar padrões e tendências de criminalidade, permitindo que as autoridades concentrem seus esforços em áreas e horários com maior incidência de crimes. Essas análises estatísticas auxiliam no planejamento e na tomada de decisões estratégicas para combater a criminalidade.

Em relação à tecnologia de reconhecimento facial (RF), seu uso como ferramenta complementar na atividade policial tem sido objeto de debate. O reconhecimento facial possibilita a identificação e verificação de pessoas com base em suas características faciais. Isso poderia ser útil para auxiliar na localização de suspeitos, investigações criminais e prevenção de crimes.

A implementação do reconhecimento facial como ferramenta de identificação e segurança tem suscitado debates intensos sobre os aspectos legais e éticos associados ao seu uso. No Brasil, a Lei Geral de Proteção de Dados (LGPD) representa o principal marco regulatório que incide sobre o tratamento de dados pessoais, incluindo aqueles coletados por meio de tecnologias biométricas. A LGPD destaca a importância do consentimento do titular dos dados, a necessidade de transparência na coleta e no uso dessas informações e a obrigação de proteger os dados contra acessos indevidos ou vazamentos.

A precisão do reconhecimento facial e os riscos de discriminação são questões críticas que desafiam a aplicação ética dessa tecnologia. A possibilidade de erros de identificação, que podem afetar desproporcionalmente grupos minoritários, exige uma reflexão profunda sobre como os algoritmos são treinados e a representatividade dos dados utilizados. A preocupação com o viés algorítmico e a discriminação sistêmica é um ponto central na discussão sobre a regulamentação do reconhecimento facial, levando à necessidade de diretrizes claras e padrões antidiscriminatórios no desenvolvimento e na implementação desses sistemas.

Embora a LGPD forneça uma base sólida para a proteção de dados pessoais, há uma lacuna na legislação específica para o uso de reconhecimento facial, especialmente em contextos de segurança pública e persecução penal. O Projeto de Lei 3069/22 surge como uma iniciativa para estabelecer um marco regulatório para o uso responsável e ético da tecnologia, assegurando que o reconhecimento facial seja empregado de forma a respeitar os direitos e liberdades fundamentais.

Quando abordamos a questão da proteção de dados pessoais na União Europeia, é essencial examinar dois instrumentos principais: a Convenção 108 para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais e o Regulamento Geral de Proteção de Dados (GDPR).

A Convenção 108, de aplicação obrigatória para os Estados-membros do Conselho Europeu, é o primeiro instrumento jurídico sobre proteção de dados pessoais. Seu artigo 6º proíbe o tratamento automático de dados que revelem origem racial, opiniões políticas, crenças religiosas, saúde ou vida sexual, a menos que a legislação nacional estabeleça salvaguardas adequadas. No entanto, o artigo 9º da mesma convenção permite exceções para proteger a segurança do Estado, segurança pública, interesses financeiros do Estado, repressão de infrações penais ou para proteger os direitos e liberdades de terceiros. Portanto, embora a convenção enfatize a dignidade humana, ela reconhece a relativização desse direito em prol da segurança em determinadas circunstâncias.

Em 2018, o Conselho da Europa iniciou um processo de modernização para adaptar a Convenção 108 aos desafios e oportunidades decorrentes do rápido avanço das tecnologias de informação e comunicação. Esta versão modernizada, conhecida como Convenção 108+, foi adotada em 2023 e tem previsão de entrar em vigor em junho de 2024. Além de abordar questões emergentes, como análise de grandes volumes de dados, inteligência artificial e tratamento de dados pessoais no contexto do ambiente de trabalho, a convenção fortalece os mecanismos de aplicação e incentiva a cooperação internacional em assuntos relacionados à proteção de dados.

Já o *General Data Protection Regulation* (GDPR), que entrou em vigor em 25 de maio de 2018, tem como objetivo fortalecer e unificar as regras de proteção de dados para todos os cidadãos da UE, estabelecendo diretrizes rigorosas sobre como os dados pessoais devem ser coletados, processados, armazenados e protegidos,

garantindo maior controle e privacidade aos indivíduos sobre suas informações pessoais.

No Brasil, apesar da promulgação da LGPD, não existe legislação que regule especificamente o uso de reconhecimento facial como medida de segurança pública. Entretanto, há projetos de lei em tramitação, tanto em nível federal quanto estadual, tanto favoráveis quanto desfavoráveis à utilização do instrumento pelo poder público.

O Projeto de Lei 3.069/22 busca regulamentar o uso do reconhecimento facial automatizado pelas forças de segurança pública em investigações criminais ou procedimentos administrativos, definindo-o como o procedimento biométrico automatizado para identificação humana a partir da captura de uma imagem facial. Este projeto pretende, entre outras finalidades, evitar que ações de restrição de liberdade sejam efetuadas apenas com base no reconhecimento facial.

Segundo o idealizador do projeto, deputado Gonzaga, "a utilização de resultados obtidos unicamente por meio de reconhecimento facial deve ser absolutamente evitada sob pena do cometimento de erros graves de identificação". Contudo, devido à grande utilidade da ferramenta no âmbito da segurança pública, embora não seja infalível, o sistema facial serviria como um primeiro filtro, devendo seu uso ser associado "com a etapa de revisão pericial humana, ou por meio de confirmação multibiométrica papiloscópica". (CONJUR, 2024)

O texto do projeto destaca que qualquer sinalização de identificação positiva a partir do uso de sistemas de reconhecimento facial deve ser confirmada por agente público responsável. O ex-deputado Subtenente Gonzaga, autor da proposta, esclarece que o texto foi elaborado pelo papiloscopista Petterson Vitorino de Morais, especialista em análise facial. (CONJUR, 2024)

O projeto determina ainda que nenhuma ação ou diligência policial de restrição da liberdade de ir e vir poderá ser efetuada simplesmente a partir do reconhecimento facial, sem a confirmação de um especialista. Nos locais onde houver captura de imagens para reconhecimento facial, devem ser fixadas placas visíveis informativas.

No âmbito estadual, observamos diversos projetos de lei ligados à iniciativa #SaiDaMinhaCara, que envolveu 50 parlamentares de diferentes partidos e apresentou propostas de lei proibindo o uso de reconhecimento facial em espaços

públicos. Destaco o Projeto de Lei nº 5240/2021, proposto por Dani Monteiro, Waldeck Carneiro, Luiz Paulo, Flavio Serafini, Mônica Francisco, Enfermeira Rejane, Carlos Minc, Renata Souza e Eliomar Coelho, apresentado no Estado do Rio de Janeiro, e o Projeto de Lei nº 385/2022, proposto por Leci Brandão (PCdoB), Isa Penna (PCdoB) e Érika Malunguinho (PSOL), apresentado no Estado de São Paulo. (CONJUR, 2024)

Ambos os projetos têm o mesmo teor e são contrários à adoção da tecnologia em qualquer circunstância. Eles proíbem que o Poder Público: adquira, retenha, venda, possua, receba, solicite, acesse, desenvolva, aprimore ou utilize tecnologias de reconhecimento facial ou informações derivadas delas; celebre contratos com terceiros com o objetivo de obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial, ou informações derivadas de uma tecnologia de reconhecimento facial, ou mantenha acesso a ela; celebre contratos com terceiros para auxiliar no desenvolvimento, melhoria ou expansão das capacidades da tecnologia de reconhecimento facial, ou fornecer acesso a informações que possam ajudar nisso; oriente pessoas jurídicas de direito público ou privado a adquirir ou usar tecnologias de reconhecimento facial em seu nome; permita que pessoas jurídicas de direito público ou privado usem tecnologias de reconhecimento facial em áreas urbanas, rurais ou mistas de sua jurisdição; implantem ou operacionalizem tecnologias de reconhecimento facial em espaços públicos e privados do Estado.

O uso do reconhecimento facial na segurança pública pode trazer benefícios significativos, como a eficiência na identificação de suspeitos e na prevenção de crimes. No entanto, é essencial que esse uso seja acompanhado de salvaguardas legais que garantam o respeito à privacidade e aos direitos individuais. A expansão dessa tecnologia deve ser monitorada cuidadosamente para evitar abusos e garantir a conformidade com os princípios constitucionais.

Durante o Carnaval do Rio de Janeiro em 2019, as 28 câmeras equipadas com tecnologia de reconhecimento de facial resultaram na recuperação de um veículo roubado. Além disso, no mesmo evento, o uso das câmeras com a tecnologia levou à prisão de quatro pessoas que tinham mandados de prisão em aberto. Essas câmeras foram capazes de identificar as pessoas procuradas, permitindo que as autoridades agissem prontamente. (G1, 2019)

Da mesma forma, em Salvador, também durante o Carnaval de 2019, um homem procurado pela polícia foi capturado graças ao sistema de reconhecimento facial utilizado pelas forças de segurança locais. O sistema foi capaz de identificar o indivíduo entre a multidão, possibilitando sua prisão imediata.(G1, 2019)

A adoção de um sistema de reconhecimento facial levantou preocupações por parte do Instituto Brasileiro de Defesa do Consumidor (IDEC), que expressou suas preocupações por meio de uma carta enviada à Polícia Militar, solicitando esclarecimentos sobre a segurança dos dados coletados. A preocupação levantada pelo IDEC reflete a importância de salvaguardar os dados pessoais coletados por meio do reconhecimento facial. O risco de vazamento ou utilização inadequada dessas informações pode comprometer a privacidade e os direitos individuais dos cidadãos.

Bárbara Simões, advogada e pesquisadora do programa de direitos digitais do IDEC, destacou a importância de garantir que as informações coletadas não estejam sujeitas a vazamentos ou uso indevido por parte do Estado ou de terceiros. Ela ressaltou que informações pessoais podem ser vendidas por empresas privadas, por exemplo, o que representa um risco para a privacidade e a segurança dos indivíduos. (IDEC, 2021)

A Receita Federal, em 2016, lançou também um sistema de reconhecimento facial para identificar os passageiros que chegassem de viagem nos aeroportos brasileiros. Ao analisar as características físicas dos indivíduos, é possível reconhecer criminosos procurados e controlar o fluxo de viajantes (RECEITA FEDERAL, 2016).

No âmbito regulatório, enquanto a União Europeia adota uma postura cautelosa e impõe restrições rigorosas ao reconhecimento facial em espaços públicos, conforme delineado pelo Regulamento Geral de Proteção de Dados (GDPR). Os Estados Unidos estão imersos em debates internos, evidenciados pelo projeto de lei *Facial Recognition Act*. No Brasil, o debate está em estágio inicial, com diversas propostas legislativas em análise, refletindo a urgente necessidade de uma legislação abrangente para orientar o uso ético e responsável da tecnologia.

A LGPD oferece um ponto de partida para a proteção de dados pessoais, mas é crucial que haja uma legislação específica que aborde os desafios únicos apresentados pela tecnologia de reconhecimento facial. Isso inclui garantir a precisão,

combater o viés algorítmico e proteger a privacidade e os direitos fundamentais dos cidadãos. O Projeto de Lei 3069/22 representa um avanço importante nessa direção, buscando estabelecer um equilíbrio entre os benefícios da tecnologia e a proteção dos direitos individuais e coletivos.

4. PROTEÇÃO DE DADOS PESSOAIS E ÉTICA

A proteção de dados pessoais é um tema de suma importância no contexto jurídico contemporâneo, especialmente diante da crescente digitalização da sociedade e da consequente proliferação de dados. No Brasil, a proteção de dados pessoais é assegurada por um robusto arcabouço legal, que inclui a Lei Geral de Proteção de Dados (LGPD) e a recente Emenda Constitucional 115/2022, que elevou a proteção de dados pessoais ao status de direito fundamental.

Fabiano Hartmann Peixoto e Roberta Zumblick Martins da Silva destacam que "ainda não existe uma definição comum e claramente estabelecida sobre o que seria uma 'ética da IA" (PEIXOTO; SILVA, 2019). Mesmo assim, eles explicam que "há muita reflexão teórica e filosófica sobre o tema, especialmente no que tange ao conceito de ética de máquina" (PEIXOTO; SILVA, 2019).

O reconhecimento facial é uma tecnologia que pode ser empregada tanto por cidadãos quanto por autoridades ou órgãos governamentais, frequentemente sem que os titulares dos dados sejam informados sobre os motivos do uso dessa tecnologia. Nesse contexto, o objetivo deste capítulo é examinar detalhadamente a prática do reconhecimento facial e sua relação com os dados pessoais, e, consequentemente, com a Lei Geral de Proteção de Dados (LGPD).

4.1 Direitos Fundamentais

A proteção de dados pessoais é um pilar fundamental na salvaguarda dos direitos fundamentais dos indivíduos, especialmente em uma era onde a tecnologia de reconhecimento facial avança rapidamente. A interseção entre a privacidade individual e a inovação tecnológica coloca em destaque a necessidade de um equilíbrio entre o progresso e a proteção dos direitos humanos.

A privacidade, como direito fundamental, é intrínseca à dignidade da pessoa humana e está intimamente ligada à liberdade de cada indivíduo. A autonomia sobre os próprios dados pessoais, ou a autodeterminação informativa, é uma extensão desse direito, permitindo que cada pessoa controle como suas informações são

coletadas, processadas e compartilhadas. Este controle é essencial para a manutenção da privacidade e para a proteção contra usos indevidos que possam afetar a honra e a imagem do indivíduo.

No contexto do reconhecimento facial, os dados biométricos são considerados sensíveis e, portanto, merecem um nível elevado de proteção. A coleta e o processamento desses dados devem ser realizados com o máximo cuidado, respeitando-se os princípios de finalidade, adequação, necessidade e transparência. O consentimento informado do titular dos dados é um requisito legal e ético, sem o qual o tratamento dos dados não deve ocorrer.

A segurança dos dados pessoais é outro aspecto crítico. As entidades responsáveis pelo tratamento dos dados devem implementar medidas técnicas e administrativas capazes de proteger as informações contra acessos não autorizados, vazamentos e outras formas de violação. A governança de dados, por sua vez, deve assegurar que as práticas estejam alinhadas com a legislação vigente, como a Lei Geral de Proteção de Dados no Brasil.

Na China, o reconhecimento facial foi empregado pelo governo para monitorar a conformidade da população com a rigorosa política de lockdown adotada durante a pandemia de Covid-19. Com milhares de câmeras de monitoramento biométrico espalhadas pelo país, as autoridades governamentais exerceram um controle rigoroso sobre a população, permitindo identificar focos de disseminação do vírus, determinar o isolamento social das pessoas infectadas e penalizar os infratores do regime de quarentena. (O GLOBO, 2022)

Outro país asiático que se destacou no uso do reconhecimento facial foi o Japão. As Olimpíadas de 2020, originalmente planejadas para ocorrer em Tóquio, foram adiadas para 2021 devido à pandemia de Covid-19. Com a realização dos Jogos, foram implementadas medidas de segurança avançadas, incluindo o uso de reconhecimento facial. Esta tecnologia foi empregada em diversos aspectos dos Jogos Olímpicos, desde a recepção no aeroporto internacional e controle de acesso aos locais de competição até a segurança em áreas públicas, facilitando a identificação e rastreamento de pessoas, contribuindo para a segurança do evento. (EXAME, 2021)

Desde 2017, o Reino Unido também tem intensificado o uso de reconhecimento facial na segurança pública. A aplicação dessa tecnologia tem sido cada vez mais frequente, especialmente para fiscalizar e prevenir ocorrências em grandes eventos. Exemplos do uso dessa ferramenta pela polícia britânica incluem o show da Beyoncé, a coroação do Rei Charles e o Grande Prêmio da Grã-Bretanha de Fórmula 1. Nesses eventos, milhares de rostos foram escaneados ao vivo e comparados, por meio de inteligência artificial, com imagens de indivíduos procurados pela polícia que compunham uma lista de observação, visando identificar e deter suspeitos. (CONJUR, 2024)

No Brasil, o Instituto Brasileiro de Defesa do Consumidor (IDEC) ajuizou uma ação civil pública contra a empresa ViaQuatro, concessionária da Linha 4 (Amarela) do metrô da capital paulista, alegando que nas estações da linha amarela estaria ocorrendo uso de reconhecimento facial dos usuários sem o devido consentimento. Conforme a denúncia, a ViaQuatro teria instalado um sistema de câmeras capaz de detectar a presença humana e identificar emoções, gênero e faixa etária das pessoas que passavam em frente a anúncios publicitários. De acordo com o IDEC, o objetivo do mecanismo não seria a melhoria dos serviços de transporte público. (CONJUR, 2021)

A utilização de reconhecimento facial para fins comerciais, a partir de imagens captadas dos usuários do metrô de São Paulo sem autorização prévia, configura uma conduta altamente reprovável, capaz de impactar a moral coletiva, considerando o vasto número de passageiros que circulam diariamente pelas plataformas. Com base nesse entendimento, a 8ª Câmara de Direito Público do Tribunal de Justiça de São Paulo condenou a ViaQuatro ao pagamento de uma indenização de R$ 500 mil por dano moral coletivo, em razão do uso de câmeras de segurança para captar imagens dos usuários sem consentimento, com finalidades comerciais e publicitárias, conforme julgado a seguir:

> EMBARGOS DE DECLARAÇÃO. Apelações. Ação civil pública. Concessionária da Linha 4 do Metrô de São Paulo S.A. (Via Quatro) que opera, por meio das "Portas Interativas Digitais" dos trens da linha de metrô coletando diversos dados e informações dos consumidores usuários. Captação das imagens que eram utilizadas para fins publicitários e comerciais, tendo-se em vista que se buscava detectar as principais características dos indivíduos que circulavam em determinados locais e horários. Omissões, contradições, obscuridades ou erros materiais. Não caracterização. Ausentes qualquer das hipóteses do artigo 1.022, incisos I e

> II, do Código de Processo Civil. Recurso com escopo infringente. Inadmissibilidade. EMBARGOS REJEITADOS.
>
> (TJ-SP - Embargos de Declaração Cível: XXXXX-42.2018.8.26.0100 São Paulo, Relator: Antonio Celso Faria, Data de Julgamento: 29/11/2023, Data de Publicação: 20/12/2023)

O uso do reconhecimento facial é um tema atual, mas sua regulamentação ainda é incipiente e fragmentada. Embora a proteção de dados pessoais tenha se tornado uma preocupação significativa nos últimos anos, impulsionando a criação de diretrizes legais em vários países, o tratamento de dados biométricos obtidos por meio de reconhecimento facial ainda necessita de uma normatização mais detalhada e restritiva. Tal regulamentação é essencial para impedir abusos, discriminação e invasão de privacidade do controlador dos dados obtidos.

Além disso, a proteção de dados pessoais não deve ser vista como um obstáculo ao desenvolvimento tecnológico. Pelo contrário, deve-se buscar uma harmonização que permita a inovação e o progresso, sem comprometer os direitos individuais. A livre iniciativa e a defesa do consumidor são princípios que coexistem com a proteção de dados, exigindo que as empresas atuem de forma responsável e transparente.

4.2 Legislação de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados (LGPD), sancionada no Brasil, representa um marco regulatório fundamental para a proteção de dados pessoais e a privacidade dos cidadãos. A legislação reflete uma crescente conscientização global sobre a importância da segurança da informação e o respeito aos direitos individuais no contexto digital.

A LGPD, Lei nº 13.709/2018, estabelece um conjunto de princípios e regras para o tratamento de dados pessoais, tanto por entidades públicas quanto privadas. A lei visa garantir a privacidade e a liberdade dos indivíduos, impondo limites e condições para a coleta, uso, processamento e armazenamento de dados pessoais. Entre os princípios fundamentais estabelecidos pela LGPD estão a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Um dos pilares da LGPD é o consentimento do titular dos dados, que deve ser livre, informado e inequívoco, especialmente para dados considerados sensíveis, como aqueles coletados por tecnologias de reconhecimento facial. A legislação também prevê a possibilidade de revogação do consentimento, reforçando o poder do indivíduo sobre o uso de suas informações.

Em caso de violação de dados pessoais, a LGPD exige que as organizações notifiquem tanto a Autoridade Nacional de Proteção de Dados (ANPD) quanto o titular dos dados sobre o incidente, de maneira clara e adequada. Isso demonstra a preocupação com a pronta resposta e mitigação de possíveis danos aos titulares dos dados.

A Emenda Constitucional 115/2022 fortaleceu ainda mais a proteção de dados pessoais, inserindo-a expressamente no rol dos direitos fundamentais previstos na Constituição Federal. Com isso, a proteção de dados pessoais passa a ser um direito inalienável, que deve ser respeitado e promovido pelo Estado e pela sociedade, garantindo-se, assim, a dignidade e o livre desenvolvimento da personalidade dos cidadãos.

Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) foi instituída como órgão responsável pela fiscalização e aplicação da LGPD, com poderes para editar normas e procedimentos sobre a proteção de dados pessoais. A ANPD atua como um ente regulador e orientador, promovendo a cultura de proteção de dados no país e zelando pelo cumprimento da legislação.

No entanto, apesar dos avanços legislativos, a implementação efetiva da proteção de dados pessoais enfrenta desafios, especialmente no que tange à adequação das organizações às novas normas e à conscientização da população sobre seus direitos. A complexidade tecnológica e a dinâmica da inovação exigem uma constante atualização das normativas e das práticas de segurança da informação, bem como uma vigilância atenta contra abusos e violações.

Em face desses desafios, é imperativo que o Brasil continue a desenvolver sua legislação e infraestrutura de proteção de dados pessoais, alinhando-se às melhores práticas internacionais e aos padrões estabelecidos por organismos como a União Europeia, que possui o Regulamento Geral sobre a Proteção de Dados (GDPR). A harmonização das leis de proteção de dados e a cooperação internacional

são essenciais para enfrentar os desafios transnacionais, como o fluxo de dados entre países e a atuação de empresas multinacionais.

A proteção de dados pessoais no Brasil representa um campo jurídico em constante evolução, que requer um compromisso contínuo com a promoção e defesa dos direitos dos cidadãos na era digital. A LGPD e a Emenda Constitucional 115/2022 são marcos importantes nesse processo, mas é necessário um esforço conjunto de todos os setores da sociedade para garantir que a proteção de dados pessoais seja efetiva e abrangente, assegurando a privacidade e a liberdade dos indivíduos em um mundo cada vez mais conectado.

No contexto brasileiro, a LGPD tem sido o centro das discussões jurídicas, estabelecendo um novo paradigma na proteção de dados pessoais. As decisões judiciais recentes demonstram a preocupação dos tribunais em garantir a efetividade dos direitos previstos na LGPD, especialmente no que tange ao consentimento informado, à segurança dos dados e ao direito de reparação em caso de danos.

As jurisprudências têm abordado diversos aspectos práticos da aplicação da LGPD, desde a responsabilidade das organizações pelo vazamento de dados até a legalidade do uso de tecnologias de reconhecimento facial por entidades públicas e privadas. Os tribunais têm sido enfáticos ao afirmar que a proteção de dados pessoais não é apenas uma questão de conformidade regulatória, mas um direito fundamental que deve ser respeitado e garantido.

Essas jurisprudências demonstram a importância crescente da proteção de dados pessoais e os desafios enfrentados no contexto do reconhecimento facial. É fundamental que as instituições financeiras e outras organizações adotem medidas rigorosas para garantir a segurança e a privacidade dos dados dos usuários.

4.3 Implicações Éticas e Viéses Algorítimicos

A discriminação algorítmica é um fenômeno que ocorre quando um algoritmo perpetua ou amplifica preconceitos existentes na sociedade, trazendo resultados que são injustamente tendenciosos ou prejudiciais para certos grupos ou indivíduos. Este

fenômeno pode ser observado em diversos contextos, desde sistemas de recomendação online até decisões de concessão de crédito bancário.

Em sua obra, Fabiano Hartmann Peixoto e Roberta Zumblick Martins da Silva destacam que o viés na seleção dos dados é um fator crucial para a reprodução da discriminação pelos algoritmos:

> [...] os algoritmos podem ter sido treinados em dados nos quais uma parcela demográfica não esteja bem representada, o que levaria a não ser reconhecida. Um algoritmo treinado em um *dataset* majoritariamente caucasiano não vai desempenhar bem com pessoas com traços de outras etnias. Um algoritmo que não foi submetido à diversidade no treinamento não tem como reconhecê-la na aplicação. (PEIXOTO; SILVA, 2019)

Este é um problema complexo que exige uma abordagem multifacetada para sua resolução. Isso inclui a diversificação dos conjuntos de dados de treinamento, a implementação de práticas de uso mais transparentes e responsáveis, e a regulamentação do uso de algoritmos em áreas sensíveis, como contratação, crédito e aplicação da lei.

Os algoritmos de reconhecimento facial estão se tornando cada vez mais sofisticados, sendo capazes de lidar melhor com desafios como o envelhecimento, condições de iluminação inadequadas e rostos cobertos. Paralelamente, os bancos de dados faciais têm se expandido em decorrência da proliferação de câmeras de segurança e da coleta de imagens provenientes de diversas fontes. Deve-se destacar que essa expansão também é impulsionada pela crescente submissão a escaneamentos faciais, pela extração de imagens das redes sociais e pela coleta de dados realizada por aplicativos e autoridades.

No entanto, esses algoritmos podem levar a resultados discriminatórios, por exemplo, se os dados usados para treinar o algoritmo de reconhecimento facial não forem representativos de todas as populações, o algoritmo pode ter um desempenho pior para os grupos sub-representados. Por exemplo, se o conjunto de dados contém principalmente rostos de pessoas caucasianas, o algoritmo pode ser menos preciso ao identificar rostos de pessoas de outras etnias.

A ausência de exatidão e precisão no emprego do Reconhecimento Facial acarreta implicações de extrema gravidade. Por exemplo, em virtude de uma suposta necessidade de aprimorar a segurança por meio da tecnologia, verifica-se a

propensão para discriminar minorias, o que pode resultar em condutas abusivas por parte das forças policiais. Além disso, há o risco associado ao viés de confirmação do algoritmo. Esse viés se manifesta quando as autoridades policiais recorrem à Inteligência Artificial para determinar as áreas que demandam maior patrulhamento. Consequentemente, aumenta-se a vigilância nos locais identificados pelos dados como necessitados, promovendo assim o envio de mais efetivos policiais para tais regiões, o que por sua vez gera novos conjuntos de dados retroalimentando o referido viés.

Os algoritmos são programados por humanos e podem inadvertidamente herdar seus preconceitos. Por exemplo, se um programador inconscientemente dá mais peso a certas características faciais sobre outras, isso pode levar a um viés no algoritmo.

Um dos exemplos mais evidentes da discriminação algorítmica está nos sistemas automatizados de recrutamento e seleção. Esses algoritmos podem acabar favorecendo candidatos brancos em detrimento de candidatos negros, mesmo que ambos possuam habilidades e qualificações equivalentes. Tal situação ocorre porque os algoritmos são treinados com dados históricos que refletem as desigualdades presentes no mercado de trabalho.

Em 2018, a Amazon implementou um sistema de seleção de candidatos utilizando inteligência artificial. Esse sistema foi projetado para analisar currículos, sendo treinado com dados de funcionários anteriores da empresa. Embora a Amazon tenha afirmado que o algoritmo foi treinado para evitar preconceitos, a base de dados utilizada era antiquada e predominantemente composta por perfis masculinos, o que resultou na seleção preferencial de candidatos do sexo masculino. Como consequência, mulheres e candidatos formados em instituições frequentadas por mulheres foram excluídos do processo de seleção. (GARCIA, 2020)

Conforme exposto, algoritmos que se baseiam em dados históricos têm o potencial de perpetuar preconceitos e discriminação em seus resultados, levando a consequências injustas para grupos marginalizados. É crucial que os desenvolvedores de inteligência artificial incorporem considerações de diversidade e inclusão em todo o processo de desenvolvimento e adotem metodologias que reduzam a discriminação algorítmica. Para enfrentar esses desafios éticos, é indispensável um compromisso sólido por parte dos desenvolvedores, das empresas

e dos governos, garantindo que a inteligência artificial seja desenvolvida e empregada de forma responsável.

Mesmo que um algoritmo seja preciso e livre de viés, ele ainda pode ser usado de maneira discriminatória. Por exemplo, se a tecnologia de reconhecimento facial for usada de maneira desproporcional em certas comunidades (por exemplo, comunidades de minorias), isso pode levar a uma maior vigilância e discriminação dessas comunidades.

Recentemente, o programa Fantástico relatou casos de falhas no sistema de reconhecimento facial em Sergipe. Pessoas foram detidas erroneamente devido a erros no sistema. Especialistas alertam para os riscos e vieses dessas tecnologias. Nos EUA, algoritmos de reconhecimento facial erraram mais no caso de mulheres negras. A falta de legislação adequada no Brasil também é um problema. O governo de Sergipe suspendeu o uso do sistema após as polêmicas. (G1, 2024)

Em Sergipe, o personal trainer João Antônio Trindade Bastos, de 23 anos, foi preso por engano em um estádio de Sergipe após uma falha no sistema de reconhecimento facial. Outro caso em Sergipe envolveu a auxiliar administrativa Taislaine Santos, de 31 anos, que foi identificada pelo reconhecimento facial como foragida da Justiça durante uma prévia carnavalesca. Ela passou duas horas na delegacia e precisou provar que não era a mulher que os policiais procuravam. (G1, 2024)

Houve um caso na Bahia, em que um homem negro foi preso injustamente durante a festa junina de 2022, em Salvador, após ser identificado erroneamente pelo sistema de reconhecimento facial. Ele foi detido e ficou preso por 26 dias por um crime que não cometeu. O verdadeiro criminoso havia usado o nome e as digitais do homem inocente para se identificar. (G1, 2023)

Em 2019, nos Estados Unidos Robert William foi preso após ser identificado erroneamente pela tecnologia de reconhecimento facial como o autor de um furto a uma joalheria. O verdadeiro criminoso era outra pessoa que estava acima do peso e era negra, assim como William. (CONJUR, 2021)

Esses casos ilustram como o uso incorreto do reconhecimento facial pode levar a consequências graves, incluindo a prisão injusta de indivíduos inocentes. Eles

destacam a necessidade de melhorar a precisão desses sistemas e implementar salvaguardas adequadas para proteger os direitos dos indivíduos.

5. DESAFIOS E MEDIDAS REGULATÓRIAS

O reconhecimento facial é uma tecnologia que tem ganhado destaque nas últimas décadas, sendo utilizada em diversas áreas como segurança pública, autenticação de usuários, marketing, entre outras. No entanto, essa tecnologia também traz consigo uma série de desafios e controvérsias que precisam ser abordados para garantir uma utilização responsável e ética. Este capítulo explora esses desafios, discute as controvérsias associadas ao reconhecimento facial e apresenta medidas regulatórias que podem ser adotadas para mitigar os riscos e assegurar a proteção dos direitos individuais.

Um dos desafios éticos da inteligência artificial é a falta de transparência na construção dos algoritmos e na forma como tomam decisões. Algoritmos opacos podem levar a decisões enviesadas, resultando em discriminação e exclusão social. É imperativo que os desenvolvedores de inteligência artificial adotem práticas transparentes e auditáveis para garantir que as decisões tomadas pelos sistemas baseados em inteligência artificial sejam justas e imparciais.

A transparência é particularmente desafiadora em sistemas que utilizam *machine learning* e *deep learning*. Os modelos de aprendizado profundo são constituídos por camadas complexas de processamento de dados, o que dificulta a interpretação do funcionamento interno do modelo, especialmente quando os dados são obtidos e processados de forma autônoma, sem supervisão humana.

Outro desafio do reconhecimento facial é a precisão dos algoritmos, que pode variar significativamente entre diferentes populações. Estudos têm demonstrado que muitos sistemas de reconhecimento facial apresentam taxas de erro mais altas para pessoas de pele mais escura e para mulheres em comparação com homens de pele mais clara. Esse viés algorítmico ocorre devido a conjuntos de dados de treinamento desequilibrados, onde as amostras não representam adequadamente a diversidade da população.

Além disso, o desafio ético relevante é a atribuição de responsabilidade pelas decisões tomadas por sistemas de inteligência artificial. Visto que a inteligência artificial se baseia em algoritmos e não em decisões humanas, a determinação da responsabilidade pode ser complexa. Por isso, é crucial que a legislação defina claramente a extensão da responsabilidade dos desenvolvedores pelas decisões

tomadas pelos sistemas e estabeleça medidas de reparação quando houver consequências negativas.

A coleta e o armazenamento de dados biométricos levantam sérias preocupações de privacidade. Dados faciais são informações altamente sensíveis e, se não forem protegidos adequadamente, podem ser alvo de vazamentos e usos indevidos. A utilização indiscriminada de reconhecimento facial em espaços públicos também levanta questões sobre vigilância em massa e a invasão da privacidade dos cidadãos.

A identificação errônea de indivíduos por sistemas de reconhecimento facial pode ter consequências graves, especialmente quando usada por forças de segurança. Casos de prisões injustas e detenção de pessoas inocentes devido a falhas nos sistemas destacam a necessidade de uma supervisão rigorosa e de mecanismos de recurso para aqueles que são erroneamente identificados.

5.1 Controvérsias e Impactos do uso do Reconhecimento Facial

O reconhecimento facial é uma tecnologia avançada que possibilita a identificação ou verificação da identidade de indivíduos por meio de imagens ou vídeos, comparando características faciais com bases de dados preexistentes. Embora essa tecnologia ofereça benefícios evidentes em áreas como segurança e conveniência, ela também suscita uma série de controvérsias e desafios significativos. Este capítulo visa analisar os principais desafios e controvérsias relacionados ao uso do reconhecimento facial, bem como seus impactos sociais e legais.

Os algoritmos de reconhecimento facial frequentemente são treinados com conjuntos de dados que não refletem adequadamente a diversidade racial e de gênero da população. Esse desequilíbrio resulta em sistemas que apresentam precisão significativamente menor para determinados grupos, como pessoas de pele mais escura e mulheres. Tal viés algorítmico pode acarretar consequências graves, como a identificação errônea de indivíduos, exacerbando a desconfiança na tecnologia e ressaltando a necessidade de conjuntos de dados mais representativos e de auditorias regulares.

A precisão dos sistemas de reconhecimento facial pode ser comprometida por fatores ambientais, como iluminação e ângulos das câmeras. Erros de identificação podem ter impactos profundos, especialmente em contextos de segurança e aplicação da lei, onde uma identificação equivocada pode resultar em detenções injustas e danos à reputação dos indivíduos.

A coleta e o armazenamento de dados faciais suscitam preocupações significativas em relação à privacidade. Dados biométricos são únicos e permanentes, ao contrário de senhas que podem ser alteradas. Vazamentos ou uso indevido desses dados podem causar danos irreversíveis aos indivíduos afetados. Além disso, existe o risco de que esses dados sejam utilizados para fins não autorizados, como vigilância excessiva e monitoramento de atividades cotidianas sem o conhecimento ou consentimento dos indivíduos.

O emprego de reconhecimento facial em espaços públicos pode ser interpretado como uma forma de vigilância em massa, potencialmente infringindo liberdades civis fundamentais. A possibilidade de monitoramento constante pode criar uma sociedade na qual os indivíduos se sentem continuamente observados, o que pode ter um efeito inibidor sobre a liberdade de expressão e de reunião.

Frequentemente, a coleta de dados faciais é realizada sem o consentimento explícito dos indivíduos. Em muitos casos, as pessoas não estão cientes de que estão sendo monitoradas ou de como seus dados estão sendo utilizados.

A ausência de transparência em relação ao funcionamento dos sistemas de reconhecimento facial, incluindo os algoritmos utilizados e as políticas de privacidade, aumenta a desconfiança pública. As organizações que utilizam essa tecnologia devem ser transparentes sobre como os dados são coletados, armazenados, utilizados e protegidos.

A utilização de sistemas de reconhecimento facial com viés pode exacerbar desigualdades existentes e perpetuar discriminações sistêmicas. Identificações incorretas ou tendenciosas podem resultar em consequências negativas para grupos minoritários, incluindo assédio, vigilância excessiva e injustiças legais.

A vigilância constante pode ter efeitos psicológicos negativos sobre os indivíduos, incluindo aumento do estresse, ansiedade e uma sensação de perda de autonomia. A percepção de estar continuamente monitorado pode alterar o

comportamento das pessoas, limitando a expressão livre e a participação em atividades sociais e políticas.

5.2 Princípios para utilização ética e responsável

O advento do reconhecimento facial representa uma promissora inovação tecnológica, contudo, sua implementação traz consigo uma série de questões éticas e morais. Em virtude disso, é premente a adoção de um conjunto de princípios norteadores que visem assegurar que esta tecnologia seja empregada de maneira ética e socialmente responsável.

A implementação do reconhecimento facial deve estar em conformidade com leis de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil. Essas leis exigem que a coleta e o processamento de dados pessoais sejam realizados de maneira justa, transparente e para finalidades específicas e legítimas.

É imperativo que as entidades que implementam sistemas de reconhecimento facial adotem uma postura transparente, fornecendo informações claras e abertas ao público acerca dos processos, finalidades e consequências associadas à utilização desta tecnologia. A divulgação transparente dos mecanismos de coleta, armazenamento e processamento de dados é essencial para a construção de confiança e a salvaguarda dos direitos dos indivíduos.

A transparência deve ser acompanhada por práticas de auditoria regulares e pela publicação de relatórios detalhados que avaliem o desempenho, a precisão e os possíveis impactos dos sistemas de reconhecimento facial. Tais relatórios devem ser submetidos à revisão independente, garantindo a integridade e a responsabilidade das entidades responsáveis pela implementação e operação desses sistemas.

O princípio do consentimento demanda que a coleta e o uso de dados faciais sejam precedidos pela obtenção do consentimento explícito e deliberado dos indivíduos. Este consentimento deve ser obtido de forma clara, acessível e completa, assegurando que os indivíduos estejam plenamente cientes das finalidades para as quais seus dados serão utilizados.

Os indivíduos devem ser assegurados do direito inalienável de recusar-se a participar de sistemas de reconhecimento facial sem que isso resulte em qualquer forma de discriminação ou prejuízo. Mecanismos eficazes devem ser implementados para garantir que os indivíduos possam retirar seu consentimento a qualquer momento, resguardando assim sua autonomia e privacidade.

A coleta de dados deve ser estritamente limitada ao mínimo necessário para atingir os objetivos legítimos e específicos do sistema de reconhecimento facial. Este princípio preconiza a exclusão de quaisquer informações não essenciais e o armazenamento dos dados apenas pelo tempo necessário para cumprir suas finalidades.

Medidas abrangentes de segurança devem ser implementadas para proteger os dados faciais contra acesso não autorizado, vazamentos e outros incidentes de segurança. Isso envolve a adoção de técnicas de criptografia, a implementação de controles rigorosos de acesso e a vigilância constante das infraestruturas de dados.

Os desenvolvedores e operadores de sistemas de reconhecimento facial devem buscar ativamente identificar e mitigar quaisquer vieses algorítmicos que possam estar presentes nos sistemas. Isso requer o uso de conjuntos de dados diversificados e representativos durante o treinamento dos modelos, bem como a realização de testes periódicos para garantir que os sistemas operem de forma equitativa para todas as populações.

É essencial garantir que os sistemas de reconhecimento facial tratem todos os indivíduos de forma justa e equitativa, independentemente de sua raça, gênero, idade ou outras características protegidas. Quaisquer disparidades de desempenho devem ser identificadas e abordadas de imediato, promovendo assim a igualdade de tratamento e o respeito à diversidade.

As organizações responsáveis pela implementação e operação de sistemas de reconhecimento facial devem ser responsabilizadas por qualquer uso indevido ou falhas em proteger os direitos dos indivíduos. É crucial estabelecer políticas claras de responsabilização e mecanismos eficazes para investigar e remediar quaisquer violações éticas ou legais que possam ocorrer.

A supervisão independente desempenha um papel fundamental na garantia da conformidade e da integridade dos sistemas de reconhecimento facial. Órgãos de

supervisão independentes devem ser estabelecidos para monitorar a implementação e operação desses sistemas, assegurando que eles atendam aos mais altos padrões éticos e legais.

A utilização do reconhecimento facial deve ser restrita a finalidades legítimas, claramente definidas e proporcionais aos objetivos almejados. É imprescindível que os sistemas de reconhecimento facial sejam empregados de maneira que respeite os direitos individuais e coletivos, evitando seu uso excessivo ou desproporcional. A definição das finalidades de uso deve ser baseada em critérios objetivos e transparentes, comunicados de forma clara ao público, e sujeitos à avaliação constante de sua pertinência e adequação.

Antes da implementação de sistemas de reconhecimento facial, deve ser conduzida uma avaliação de impacto abrangente, que contemple os potenciais riscos, benefícios e implicações éticas associadas à tecnologia. Esta avaliação deve considerar os possíveis efeitos sobre a privacidade, os direitos individuais e a sociedade como um todo, orientando a tomada de decisão e as práticas de uso do reconhecimento facial. É fundamental que as conclusões dessa avaliação sejam utilizadas para informar políticas e práticas que promovam o uso responsável e ético dessa tecnologia.

6. CONCLUSÃO

O avanço da tecnologia, particularmente a inteligência artificial e o reconhecimento facial, tem provocado mudanças significativas na sociedade moderna. Este trabalho buscou analisar os aspectos jurídicos do uso do reconhecimento facial, com ênfase nos direitos individuais e na proteção de dados pessoais. Através desta investigação, foi possível identificar os principais desafios e oportunidades associados a esta tecnologia emergente.

Em primeiro lugar, o reconhecimento facial oferece inegáveis benefícios, como a melhoria da segurança pública, a eficiência em sistemas de autenticação e a conveniência em diversas aplicações comerciais. No entanto, esses avanços tecnológicos também trazem preocupações substanciais em relação à privacidade e à proteção dos dados pessoais.

No contexto jurídico, a utilização do reconhecimento facial está submetida a um conjunto complexo de normas que visam proteger os direitos individuais. A Lei Geral de Proteção de Dados (LGPD) no Brasil, por exemplo, estabelece diretrizes claras sobre o tratamento de dados pessoais, incluindo dados biométricos, que são essenciais para o reconhecimento facial. A LGPD exige o consentimento explícito dos indivíduos para a coleta e uso de seus dados pessoais, assegurando, assim, um controle maior sobre suas informações.

Entretanto, a aplicação prática dessas normas ainda enfrenta desafios significativos. Um dos principais problemas é a falta de regulamentação específica e detalhada sobre o uso do reconhecimento facial, o que pode levar a abusos e ao uso indevido de dados. Além disso, a transparência nas operações de coleta e processamento de dados é crucial para garantir que os direitos dos indivíduos sejam respeitados.

Outro aspecto crucial abordado foi a questão dos direitos individuais. O reconhecimento facial pode, em algumas situações, implicar na violação da privacidade e na discriminação, especialmente quando utilizado sem o devido controle e supervisão. As tecnologias de reconhecimento facial podem apresentar vieses, levando a erros de identificação que afetam desproporcionalmente certos grupos sociais, o que é uma preocupação de direitos humanos.

Portanto, é essencial que haja uma fiscalização rigorosa e a implementação de políticas claras que assegurem a equidade e a justiça no uso do reconhecimento facial. As empresas e órgãos governamentais que utilizam essa tecnologia devem adotar práticas de transparência e prestação de contas, garantindo que os dados coletados sejam utilizados de forma ética e responsável.

Dado o exposto, a utilização do reconhecimento facial representa uma fronteira tecnológica que necessita de um equilíbrio cuidadoso entre inovação e proteção dos direitos individuais. É imperativo que a legislação continue a evoluir para acompanhar o ritmo da tecnologia, protegendo os dados pessoais dos cidadãos sem impedir os benefícios que o reconhecimento facial pode trazer para a sociedade. Somente através de uma abordagem regulatória robusta e de práticas responsáveis é que poderemos usufruir dos avanços tecnológicos de maneira segura e justa.

7. REFERÊNCIAS

AGRELA, Lucas. **AS TECNOLOGIAS POR TRÁS DA OLIMPÍADA 2021**. Exame, 2021. Disponível em: https://exame.com/tecnologia/as-tecnologias-por-tras-da-olimpiada-2021/. Acesso em 20 de junho de 2024.

ALENCAR, I. **COM MAIS DE MIL PRISÕES NA BA, SISTEMA DE RECONHECIMENTO FACIAL É CRITICADO POR 'RACISMO ALGORÍTMICO'; INOCENTE FICOU PRESO POR 26 DIAS.** G1 Globo. 01 de setembro de 2023. Disponível em: https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml. Acesso em 10 de abril de 2024.

ANDERSON, E. **CONTROVERSIAL DETROIT FACIAL RECOGNITION GOT HIM ARRESTED FOR A CRIME HE DIDN'T COMMIT.** Detroit Free Press. 10 de julho de 2020. Disponível em: https://olhardigital.com.br/2020/09/05/noticias/de-novo-reconhecimento-facial-incrimina-erroneamente-pessoas-negras/. Acesso em 05 de maio de 2024.

ARBIX, G. **A TRANSPARÊNCIA NO CENTRO DA CONSTRUÇÃO DE UMA IA ÉTICA.** Scielo Brasil. 12 de outubro de 2020. Disponível em: https://www.scielo.br/j/nec/a/pD9k5gtHpXwsgFcsMC5gbJg/#. Acesso em 10 de maio de 2024.

BITTENCOURT, G. **INTELIGÊNCIA ARTIFICIAL: FERRAMENTAS E TEORIAS**. 2. ed. Florianópolis: Editora da UFSC, 2001.

BONISSONE, P. P. (1999). **SOFT COMPUTING SYSTEMS: COMMERCIAL AND INDUSTRIAL APPLICATIONS.** IEEE International Fuzzy Systems Conference Proceedings. Seoul.

BRASIL. Constituição (1988). **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 04 de março de 2024.

BRASIL. Lei Nº 12.965, de 23 de abril de 2014. **ESTABELECE PRINCÍPIOS, GARANTIAS, DIREITOS E DEVERES PARA O USO DA INTERNET NO BRASIL.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 de março de 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 de abril de 2024.

BRASIL. Projeto de Lei nº 5240 de 2021. **DISPÕE SOBRE RESTRIÇÕES DO USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL PELO PODER PÚBLICO NO ESTADO DO RIO DE JANEIRO.** Disponível em: http://www3.alerj.rj.gov.br. Acesso em: 8 de Junho de 2024.

BUOLAMWINI, J. **RESPONSE: RACIAL AND GENDER BIAS IN AMAZON REKOGNITION — COMMERCIAL AI SYSTEM FOR ANALYZING FACES.** 25 de janeiro de 2019. Disponível em: https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced. Acesso em 05 de maio de 2024.

BUTLER, K. L.; MOMOH, J. A.; SOBAJIC, D. J.; 1997. **FIELD STUDIES USING A NEURAL-NET-BASED APPROACH FOR FAULT DIAGNOSIS IN DISTRIBUTION NETWORKS.** IEE Proc.-Gener. Transm. Distrib, Vol. 144, Nº 5.

CÂMERAS COM RECONHECIMENTO FACIAL SÃO INSTALADAS EM COPACABANA DURANTE O CARNAVAL. G1 Globo. 01 de março de 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/03/01/cameras-com-reconhecimento-facial-sao-instaladas-em-copacabana-durante-o-carnaval.ghtml. Acesso em: 10 de julho de 2024.

CAMIMURA, L. **DIREITO PRECISA DAR DIRETRIZES PARA A PRODUÇÃO E USO DE RECONHECIMENTO FACIAL SEM DISTORÇÕES RACIAIS.** Conselho Nacional de Justiça. 16 de agosto de 2023. Disponível em: https://www.cnj.jus.br/direito-precisa-dar-diretrizes-para-a-producao-e-uso-de-reconhecimento-facial-sem-distorcoes-raciais/. Acesso em 30 de março de 2024.

CARDOSO JR G, ROLIM JG, ZÜRN HH. **DIAGNÓSTICO DE FALTAS EM SISTEMAS DE POTÊNCIA: DEFINIÇÃO DO PROBLEMA E ABORDAGENS VIA INTELIGÊNCIA ARTIFICIAL.** Sba Controle & Automação [Internet]. 15 de Abril de 2004. Disponível em: https://doi.org/10.1590/S0103-17592004000200010. Acesso em 15 de maio de 2024.

CHINA USA TELEFONES E RECONHECIMENTO FACIAL PARA RASTREAR MANIFESTANTES. O Globo. 03 de dezembro de 2022. Disponível em: https://oglobo.globo.com/mundo/noticia/2022/12/china-usa-telefones-e-reconhecimento-facial-para-rastrear-manifestantes.ghtml. Acesso em: 15 de julho de 2024.

CONSELHO DA EUROPA. **CONVENÇÃO PARA A PROTEÇÃO DAS PESSOAS RELATIVAMENTE AO TRATAMENTO AUTOMATIZADO DE DADOS DE CARÁTER PESSOAL (CONVENÇÃO 108).** Estrasburgo, 1981. Disponível em: https://www.coe.int. Acesso em: 8 de Maio de 2024.

DE MELO, J. **AÇÃO PEDE BANIMENTO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NOS EUA.** Consultor Jurídico. 26 de abril de 2021. Disponível em: https://www.conjur.com.br/2021-abr-26/acao-banimento-tecnologia-reconhecimento-facial-eua/. Acesso em 18 de agosto de 2024.

EMENDA CONSTITUCIONAL. Nº 115, de 10 de fevereiro de 2022. **ALTERA A CONSTITUIÇÃO FEDERAL PARA INCLUIR A PROTEÇÃO DE DADOS PESSOAIS ENTRE OS DIREITOS E GARANTIAS FUNDAMENTAIS E PARA FIXAR A COMPETÊNCIA PRIVATIVA DA UNIÃO PARA LEGISLAR SOBRE PROTEÇÃO E TRATAMENTO DE DADOS PESSOAIS.** Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em 04 de maio de 2024.

ESPECIALISTA DO IDEC FALA SOBRE CUIDADOS NAS COMPRAS PELA INTERNET. Instituto de Defesa de Consumidores. 27 de janeiro de 2021. Disponível em: https://idec.org.br/release/parlamentares-de-todas-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do. Acesso em 20 de junho de 2024.

FERNANDES, C. **RECONHECIMENTO FACIAL NAVEGANDO PELOS DESAFIOS JURÍDICOS E ÉTICOS NA ERA DIGITAL.** Guimarães Fernandes Advogados

Associados. 07 de agosto de 2023. Disponível em: https://gfadvogados.com/reconhecimento-facial-navegando-pelos-desafios-juridicos-e-eticos-na-era-digital/. Acesso em 30 de março de 2024.

FILHO, P. **RECONHECIMENTO FACIAL: COMPREENDENDO OS LIMITES DE USO.** Consultor Jurídico. 26 de junho de 2021. Disponível em: https://www.conjur.com.br/2021-jun-26/opiniao-reconhecimento-facial-compreendendo-limites-uso/. Acesso em 18 de fevereiro de 2024.

GARCIA, A. **ÉTICA E INTELIGÊNCIA ARTIFICIAL.** Revista da Sociedade Brasileira de Computação. 16 de novembro de 2020. Disponível em: https://sol.sbc.org.br/journals/index.php/comp-br/article/view/1791. Acesso em 10 de maio de 2024.

GOODFELLOW, I., BENGIO, Y., & COURVILLE, A. (2016). **DEEP LEARNING.** MIT PRESS.

GOMES, D. DOS S (2010). **INTELIGÊNCIA ARTIFICIAL: CONCEITOS E APLICAÇÕES. REVISTA OLHAR CIENTÍFICO**. v. 1, n. 2.

HIGÍDIO, JOSÉ. **VIAQUATRO DEVE INDENIZAR POR IMPLANTAR SISTEMA DE DETECÇÃO FACIAL NAS ESTAÇÕES.** Consultor Jurídico. 10 de maio de 2021. Disponível em: https://www.conjur.com.br/2021-mai-10/viaquatro-indenizar-implantar-sistema-deteccao-facial/. Acesso em 18 de julho de 2024.

INTELIGÊNCIA ARTIFICIAL – IBM. Discovery Brasil, 2018. Documentário. Disponível em: https://www.youtube.com/watch?v=W95YlM5-iPk. Acesso em 18 de maio 2024.

INTELIGÊNCIA ARTIFICIAL: MULHERES NEGRAS SOFREM MAIS ERROS EM ABORDAGENS DE RECONHECIMENTO FACIAL DO QUE BRANCOS. G1 Globo. 15 de fevereiro de 2024. Disponível em: https://g1.globo.com/podcast/o-assunto/noticia/2024/02/15/inteligencia-artificial-mulheres-negras-sofrem-mais-erros-em-abordagens-de-reconhecimento-facial-do-que-brancos.ghtml. Acesso em 30 de março de 2024.

KAUFMAN, DORA. **DOSSIÊ: DEEP LEARNING: A INTELIGÊNCIA ARTIFICIAL QUE DOMINA A VIDA DO SÉCULO XXI.** Teccogs: Revista Digital de Tecnologias Cognitivas, TIDD | PUCSP, São Paulo, n. 17. 2018. Disponível em: https://www.pucsp.br/pos/tidd/teccogs/edicao_completa/teccogs_cognicao_informacao-edicao_17-2018-completa.pdf. Acesso em 15 de maio de 2024.

LANEY, DOUG. **3D DATA MANAGEMENT: CONTROLLING DATA VOLUME, VELOCITY AND VARIETY. IN: BLOG GARTNER, 2001.** Disponível em: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Acesso em: 20 Junho de 2024.

LUGER, G. F., & STUBBLEFIELD, W. A. (2004). **ARTIFICIAL INTELLIGENCE: STRUCTURES AND STRATEGIES FOR COMPLEX PROBLEM SOLVING.**

MITCHELL, T. M. **MACHINE LEARNING.** New York: McGraw-Hill, 1997.

METRÔ DE SP INICIA OPERAÇÃO DE SISTEMA DE RECONHECIMENTO FACIAL; TJ CHEGOU A IMPEDIR INSTALAÇÃO. G1 Globo. 21 de novembro de 2022. Disponível em: https://g1.c.com/sp/sao-paulo/noticia/2022/11/21/metro-de-sp-inicia-operacao-de-novo-sistema-de-monitoramento-eletronico-por-meio-de-

reconhecimento-facial-tj-chegou-a-impedir-instalacao.ghtml. Acesso em: 09 de maio de 2024.

NABESHIMA, Y. **USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA.** Consultor Jurídico. 07 de janeiro de 2024. Disponível em: https://www.conjur.com.br/2024-jan-06/uso-do-reconhecimento-facial-na-seguranca-publica/. Acesso em 15 de março de 2024.

PARLAMENTARES DE TODAS AS REGIÕES DO BRASIL APRESENTAM PROJETOS DE LEI PELO BANIMENTO DO RECONHECIMENTO FACIAL EM ESPAÇOS PÚBLICOS. Instituto de Defesa de Consumidores. 20 de junho de 2022. Disponível em: https://idec.org.br/release/parlamentares-de-todas-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do. Acesso em 20 de abril de 2024.

PEIXOTO, Fabiano Hartmann; SILVA, Roberta Zumblick Martins da. **INTELIGÊNCIA ARTIFICIAL E DIREITO.** Curitiba: Alteridade, 2019. Disponível em: https://www.alteridade.com.br/wp-content/uploads/2019/05/suma%CC%81rio-Intelige%CC%82ncia-Artificial-e-Direito.pdf. Acesso em 15 de maio de 2024.

PROJETO DE LEI. PL 3069/22, de 21 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.** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2345261&fichaAmigavel=nao. Acesso em 04 de maio de 2024.

PROCURADO POR HOMICÍDIO VAI PARA O CARNAVAL DE SALVADOR VESTIDO DE MULHER E É PRESO APÓS SER FLAGRADO POR CÂMERA. G1 Globo. 05 de março de 2019. Disponível em: https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/05/procurado-por-homicidio-vai-para-o-carnaval-de-salvador-vestido-de-mulher-e-e-preso-apos-ser-flagrado-por-camera.ghtml. Acesso em 10 de julho de 2024.

QUEIROZ, G. **A INTELIGÊNCIA ARTIFICIAL E O RECONHECIMENTO FACIAL: IMPACTOS À POPULAÇÃO NEGRA NO BRASIL.** Repositório Institucional. 2023. Disponível em: https://repositorio.idp.edu.br/bitstream/123456789/4800/1/DISSERTA%c3%87%c3%83O_GUILHERME%20MATHEUS%20QUEIROZ_MESTRADO%20PROFISSIONAL%20E%20INTERDISCIPLINAR%20EM%20DIREITO_2023.pdf. Acesso em 08 de maio de 2024.

RAUTENBERG, SANDRO; CARMO, PAULO RICARDO VIVIURKA DO (2018). **BIG DATA E CIÊNCIA DE DADOS: COMPLEMENTARIEDADE CONCEITUAL NO PROCESSO DE TOMADA DE DECISÃO.** Brazilian Journal of Information Science. 2019. Disponível em: https://researchgate.net/publication/336307200_BIG_DATA_E_CIENCIA_DE_DADOS. Acesso em 04 de Junho de 2024.

RUSSELL, S., NORVIG, P., & DAVIS, E. (2010). **ARTIFICIAL INTELLIGENCE: A MODERN APPROACH.** PRENTICE HALL.

RUSSELL, S.J.; NORVIG, P. **INTELIGÊNCIA ARTIFICIAL.** Rio de Janeiro: Elsevier, 2013.

SILVA, I. N.; SPATTI, D. H.; FLAUZINO, R. A. **REDES NEURAIS ARTIFICIAIS: PARA ENGENHARIA E CIÊNCIAS APLICADAS.** São Paulo: Artliber, 2010.

SILVEIRA, A. M.; FURTADO, A. B.; OLIVEIRA, R. C. L.; DA COSTA JR., C. T. **IDENTIFICAÇÃO DE ABORDAGENS ADMINISTRATIVAS: UM ENSAIO COM LÓGICA FUZZY.** INFOCOMP Journal of Computer Science. 01 de março de 2004. Disponível em: https://infocomp.dcc.ufla.br/index.php/infocomp/article/view/80. Acesso em 15 de fevereiro de 2024.

SISTEMAS DE RECONHECIMENTO FACIAL SÃO CONFIÁVEIS? COMO FALHAS RECENTES REACENDEM O DEBATE SOBRE RISCOS. G1 Globo. 22 de abril de 2024. Disponível em: https://g1.globo.com/fantastico/noticia/2024/04/22/sistemas-de-reconhecimento-facial-como-falhas-recentes-reascendem-o-debate-sobre-riscos.ghtml. Acesso em: 10 de maio de 2024.

SOUZA, M. **PROJETO REGULAMENTA O USO DE RECONHECIMENTO FACIAL POR FORÇAS DE SEGURANÇA PÚBLICA.** Intranet Câmara dos Deputados. 23 de março de 2023. Disponível em: https://www.camara.leg.br/noticias/946010-projeto-regulamenta-o-uso-de-reconhecimento-facial-por-forcas-de-seguranca-publica/. Acesso em: 10 de fevereiro de 2024.

STJ TRAZ NOVOS AVANÇOS NO ENTENDIMENTO SOBRE O RECONHECIMENTO DE PESSOAS. Superior Tribunal de Justiça. 17 de março de 2022. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/17032022-STJ-traz-novos-avancos-no-entendimento-sobre-o-reconhecimento-de-pessoas.aspx. Acesso em 08 de maio de 2024.

TAUTE, F. **RECONHECIMENTO FACIAL E SUAS CONTROVÉRSIAS.** Fundação Heinrich Böll Brasil. 07 de fevereiro de 2020. Disponível em: https://br.boell.org/pt-br/2020/02/05/reconhecimento-facial-e-suas-controversias/. Acesso em 30 de março de 2024.

TJ-SP - EMBARGOS DE DECLARAÇÃO CÍVEL: XXXXX-42.2018.8.26.0100 São Paulo, Relator: Antonio Celso Faria, Data de Julgamento: 29/11/2023, Data de Publicação: 20/12/2023. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2110910767

TURING, A. **COMPUTING MACHINERY AND INTELLIGENCE.** Mind, v. 59.1950.

WALKER, Ben. **EVERY DAY BIG DATA STATISTICS – 2.5 QUINTILLION BYTES OF DATA CREATED DAILY.** 2015. Disponível em: http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/. Acesso em 04 de março de 2024.

UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 27 DE ABRIL DE 2016. **REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (GENERAL DATA PROTECTION REGULATION – GDPR).** Disponível em: https://eur-lex.europa.eu. Acesso em: 8 Julho de 2024.