



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS CORRENTE
CURSO TECNÓLOGO EM ANÁLISE E DESENVOLVIMENTO DE
SISTEMAS

JAMYLE DE MORAIS JACOBINA

REVISÃO BIBLIOGRÁFICA SOBRE A CAPACIDADE DE
HETEROIDENTIFICAÇÃO DOS ALGORITMOS DE BIOMETRIA FACIAL

CORRENTE

2023

JAMYLA DE MORAIS JACOBINA

REVISÃO SISTEMÁTICA SOBRE A CAPACIDADE DE HETEROIDENTIFICAÇÃO
DOS ALGORITMOS DE BIOMETRIA FACIAL

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Tecnólogo em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Corrente .

Orientador: Prof. Esp. Francisco Edson Rodrigues Cavalcante.

CORRENTE

2023

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

J16r Jacobina, Jamyla de Moraes
Revisão bibliográfica sobre a capacidade de heteroidentificação dos
algoritmos de biometria facial / Jamyla de Moraes Jacobina. - 2023.
16 p.: il. p&b.
Trabalho de Conclusão de Curso (Análise e Desenvolvimento de Sistemas) -
Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Corrente,
2023.
Orientador : Prof Esp. Francisco Edson Rodrigues Cavalcante.
1. Análise e Desenvolvimento de Sistemas - estudo e ensino. 2.
Reconhecimento facial. 3. Gerenciamento de riscos. 4. Banco de Dados.
I. Título.

CDD – 004.21

Elaborado por Tefischer Huanderson Soares e Sousa CRB 3/1251

AGRADECIMENTOS

Em primeiro lugar porque até aqui ele me sustentou, me deu perseverança e sabedoria para não desistir e vencer mais essa etapa na minha vida.

À minha família em especial minha mãe, meu pai, meus irmãos e minha madrinha que sempre me incentivaram para que eu pudesse concluir essa jornada.

Aos meus amigos e colegas que sempre estiveram ao meu lado apoiando, aos servidores e professores do IFPI Campus Corrente em especial ao meu orientador Francisco Edson pelo grande incentivo.

Você nunca chegará a 100% se
Se contentar com 99%.
(Chris Gardner).

RESUMO

Este trabalho tem como objetivo identificar falhas na capacidade de heteroidentificação nos algoritmos de reconhecimento facial, através da revisão sistemática de trabalhos que já relataram esses erros. Apontando a forma na coleta de dados para os repositórios utilizados nesta tecnologia e como o balanceamento de dados é importante para cessar os erros obtidos neste desenvolvimento. Irá ser utilizados artigos, livros, blogs, sites de pesquisa, documentários para identificar a importância do gerenciamento de riscos nesse processo, conceitos de reconhecimento facial, racismo. Analisando como as falhas nessa tecnologia podem afetar os indivíduos de cor negra, já que os além de serem os mais violentados de forma física os mesmos ainda sofrem de forma online através falhas nos algoritmos por conta de dados insuficientes, treinados pela inteligência artificial. Já que essas necessitam de dados concisos, coerentes e suficientes para que desempenhem com êxito o que lhes foi ensinado, assim podendo dar resultados de forma positiva e abrangendo o todo, não somente a maioria.

Palavras-chaves: Reconhecimento facial; Racismo; Tecnologia; Gerenciamento de Riscos; Banco de dados.

ABSTRACT

This work aims to identify flaws in the ability of heteroidentification in facial recognition algorithms, through systematic review of works that have already reported these errors. Pointing out how to collect data for the repositories used in this technology and how data balancing is important to stop the errors obtained in this development. It will be used articles, books, blogs, research sites, documentaries to identify the importance of risk management in this process, concepts of facial recognition, racism. Analyzing how failures in this technology can affect black individuals, since they are not only the most physically violated but also suffer online through flaws in the algorithms due to insufficient data trained by artificial intelligence. Since they need concise, coherent, and sufficient data to successfully perform what they have been taught, thus being able to give positive results and covering the whole, not just the majority.

Keywords: Facial recognition; Racism; Technology; Risk management; Database.

Data de aprovação: 20/01/2023

¹ Graduanda em Análise e Desenvolvimento de Sistemas (IFPI). Email: janylademoraes@gmail.com.

² Professor Especialista (IFPI). Email: edsoncavalcante@ifpi.edu.br.

SUMÁRIO

1 INTRODUÇÃO	8
2 REFERENCIAL TEÓRICO	10
2.1 GERENCIAMENTO DE RISCOS.....	11
2.2 RECONHECIMENTO FACIAL.....	13
2.3 RACISMO ALGORÍTMICO	15
3 METODOLOGIA	6
4 CONCLUSÕES E CONSIDERAÇÕES FINAIS	18
REFERÊNCIAS.....	19

1 INTRODUÇÃO

A capacidade de raciocínio, o aprendizado e a busca do conhecimento nos levam sempre a um novo patamar, mas nunca a um nível de excelência para explorar nossa inteligência ao mais alto nível. Na contemporaneidade, por mais que não atinjam esse nível, o ser humano é capaz de criar máquinas que se baseiam em nosso raciocínio, nossos neurônios, nossa eficácia, ou melhor na nossa capacidade de pensar.

Com a evolução cada dia mais da Inteligência Artificial (IA), funcionalidades que antes eram atribuídas a seres humanos, passaram a se tornar aplicações desenvolvidas artificialmente.

As grandes empresas estão investindo em algoritmos autônomos, além de ser uma grande evolução no mundo da tecnologia, maior será sua vantagem no mercado, portanto aumentando sua chance de sucesso.

Um grande impasse é o gerenciamento de riscos neste meio, onde esse é responsável por administrar os riscos negativos ou positivos deste processo. Esta é uma das principais fases do desenvolvimento, pois pode afetar o todo. Algoritmos como os produzidos para reconhecimento facial estão contando com erros como a não identificação de pessoas da etnia preta, ou até mesmo falhas como indivíduos com características físicas parecidas terem acesso à privacidade uma da outra através do desbloqueio facial de seus dispositivos.

Com o crescimento das redes sociais, a coleta excessiva de informações tornou-se cada vez maior, porém os tratamentos destes dados ainda são insuficientes. Onde os mais afetados são pessoas negras, tornando até mesmo alvo de injustiça baseado em um sistema algorítmico com um tratamento de dados escasso.

Por meio do que foi mencionado acima o gerenciamento de riscos é um fator primordial para o desenvolvimento de software, assim como a identificação da capacidade de heteroidentificação dos algoritmos de biometria facial. Neste trabalho iremos pesquisar e investigar esse tipo de falhas nos algoritmos de reconhecimento facial.

Revisar trabalhos sobre algoritmos de reconhecimento facial, investigando nesses trabalhos como é tratado o repositório de dados e aprendizado para manter o balanceamento de análise do algoritmo facial, para assim identificar a presença de erros em reconhecer indivíduos de grupos raciais específicos.

O racismo tem várias faces, que vai além de discursos racistas. Quando se trata de tecnologia informática e da web, voltamos muitas vezes para palavras, discurso de ódio, mas há muito, além disso, por trás dos códigos esconde-se um mundo sociotécnico e de supremacia branca. A biometria facial vem atingindo falhas no reconhecimento de pessoas negras, ocorrendo até mesmo a prisão de forma equivocada de indivíduos negros. Iremos identificar trabalhos que discutem esses erros com o intuito de amenizar seus efeitos sociais e possíveis equívocos de cunho preconceituoso, o que pode caracterizar um racismo digital estruturado, possibilitando melhorias no meio social e empresarial.

2 REFERENCIAL TEÓRICO

Para que os sistemas de IA funcionem conforme esperado é necessário ter dados com um bom balanceamento onde o sistema possa usar para aprender e analisar padrões. O conjunto de dados para sistemas de IA deve considerar dados estruturados e não estruturados, seguindo uma estratégia robusta e eficiente de coleta de dados. Sem isto, e com dados insuficientes, os projetos de IA tendem a fracassar (FACUNDES, 1996-2021).

Os algoritmos replicam preconceitos históricos e, nessas circunstâncias, conforme Thieme (2018), a injustiça computacional pode codificar injustiças sociais. Essas dimensões devastadoras e propagadoras de injustiças das tecnologias de IA são, não ocasionalmente, denominadas weapons of math destruction (O'NEIL, 2016) ou “armas de destruição matemática” (AZEVEDO et. al, 2021).

Gradativamente mais essa tecnologia vem sendo usada para a segurança, tanto em ambientes públicos, como câmeras instaladas nas ruas como meio de monitoramento e reconhecimento de pessoas que fizeram alguma infração contra a Lei, quanto em locais privados onde o indivíduo adentra o ambiente de trabalho através da biometria facial. Essa tecnologia emprega para seu desenvolvimento, coleta de dados faciais de inúmeras pessoas, aplicando traços físicos como, o formato da boca, do nariz, assim fomentando o chamado padrão facial. Quando se trata da cor da pele na aprendizagem de máquina voltado para o reconhecimento facial este algoritmo é treinado com um banco de dados de maioria branca, assim ocorrendo inúmeros erros ao reconhecer pessoas da cor negra (COSTA et. al, 2022.).

A interface entre opacidade algorítmica em relação com o pacto narcísico da branquitude é uma das chaves para entender práticas que vão da visão computacional em artefatos lúdicos até tecnologias carcerárias algorítmicas, como o reconhecimento facial, que avançam em prol do encarceramento em massa e do genocídio negro (SILVA, 2022, p.5,6).

Imbricadas em bases de dados, interfaces e dinâmicas de recomendação de conteúdo, personalização e interação automatizada, as micro agressões manifestam hierarquias racistas que controlam representações, entre o sutil e o explícito, de forma extensiva. É significativo lembrar que este desenvolvimento pode causar discriminação e tirar o direito de uma pessoa de ir e vir em questão de instantes (SILVA, 2022).

Acompanhando essa problemática, os pesquisadores Woodrow Hartzog e Evan Sellinger (2020) indicam que o reconhecimento facial pode ser uma ferramenta “perfeita” para a opressão, visto que podem lesionar direitos à privacidade e outras garantias fundamentais, ocasionando a perseguição a pessoas negras e grupos étnicos específicos (COSTA et. al, 2022).

Alimentado muita das vezes por fotógrafos autônomos, os bancos de dados utilizam de um severo processo de rotulagem e seleção da associação da palavra-chave com as imagens proporcionadas pelo banco, assim também pela significância de um resultado em relação ao outro, portanto contribuem para construir uma “dupla opacidade” (SILVA, p.4, 2019) na sua materialidade tecnológica, uma vez que adicionam valores aos seus processos automatizados e não são suficientemente transparentes a respeito das suas dinâmicas de funcionamento.

Nesse sentido, embora compondo um universo tecnológico atualizado, estes bancos de imagem, ao invés de disponibilizarem representações mais acuradas da realidade social, podem estar reforçando processos de estereotipia e fortalecendo desigualdades e dinâmicas de opressão (CARRERA, 2020).

Esses algoritmos são utilizados na técnica de aprendizagem automática de machine learning, pois alimentam as máquinas, as quais internalizam dados históricos e fazem previsões, de modo que é possível que os algoritmos se auto desenvolvam a partir da análise de dados (AZEVEDO, 2022).

2.1 GERENCIAMENTO DE RISCOS

O gerenciamento de riscos tem sido considerado uma das principais atividades dos gerentes de projeto (OLIVEIRA et. al 2013). Consiste em prever os riscos que podem afetar o cronograma do projeto ou a qualidade do software que está sendo desenvolvido e tomar providências para evitar ou atenuar os impactos decorrentes desses riscos (HALL,1998). Assim pode-se entender um risco como um evento indesejado com consequências negativas (PFLEEGER al. et. 2009).

Os passos para se evitar que tais riscos comprometam um projeto, inclui a tentativa de prevê-los, compreender seus impactos e tomar as providências cabíveis. Um gerenciamento de riscos é especialmente importante para projetos de software por causa das incertezas inerentes que a maior parte dos projetos enfrenta. Elas se originam de requisitos vagamente definidos, mudanças de requisitos devido a mudanças nas necessidades do cliente, dificuldades em estimar o tempo e os recursos necessários para o desenvolvimento do software e diferenças nas habilidades individuais. É preciso prever os riscos, compreender o impacto desses riscos sobre o projeto, o produto e o negócio e tomar medidas para evitar tais riscos (SOMMERVILLE, 2006).

Visando a melhorar a eficácia ou até mesmo a autonomia das ferramentas computacionais, diferentes técnicas da Inteligência Artificial (IA) vêm sendo empregadas nas mais diversas áreas. Os agentes inteligentes, uma das técnicas de IA, possuem características desejáveis para a construção de jogos de computador. Entre essas características, encontra-se o comportamento guiado por objetivos, reatividade, raciocínio, adaptabilidade, aprendizagem, comunicação e cooperação (OLIVEIRA et. al 2013).

2.2 RECONHECIMENTO FACIAL

O reconhecimento facial atua com um sistema que emprega algoritmos e softwares para mapear protótipos nos rostos das pessoas. O rosto humano, apesar das alterações de indivíduo para indivíduo, possui uma composição básica que não se altera, que é lida pelos aplicativos como pontos em comum, que variam de acordo com a complexidade do sistema (KLEINA, 2021).

Sistemas de IA utilizam métodos estatísticos, inteligência computacional e abordagem simbólica tradicional. Muitas ferramentas são usadas na IA, incluindo versões de pesquisa e otimização matemática, redes neurais artificiais e métodos baseados em estatística, probabilidade e economia. O campo da IA baseia-se em ciência da computação, engenharia da informação, matemática, psicologia, linguística, filosofia e muitos outros campos (FACUNDES,1996-2021).

Em Dubai, capital dos Emirados Árabes Unidos, um gigantesco “túnel-aquário” localizado no principal aeroporto da cidade conta com mais de 80 câmeras de segurança, que capturam e digitalizam, por meio de escâneres, o rosto das pessoas à medida que caminham por ele; por fim, realizada a análise das imagens obtidas, o sistema de segurança ou permite que a pessoa ingresse livremente no país ou emite um alerta, indicando a necessidade de uma análise mais aprofundada acerca da entrada do indivíduo. Nos Estados Unidos da América, no ano de 2016, ao menos 50% dos cidadãos adultos já constavam em bases de dados de reconhecimento facial do governo (COSTA al. el, 2020).

Nos algoritmos voltados para o reconhecimento facial os dados insuficientes ou o modelo com quais são treinados estão não identificando pessoas negras ou as reconhecendo de forma errônea, já que tais algoritmos são treinados na maior parte das vezes com indivíduos brancos (Bruna, 2021). O documentário “Coded Bias” produzido pela Netflix mostra falha nos algoritmos de reconhecimento facial, onde prova que estes não são precisos ao identificar pessoas negras, principalmente mulheres. Logo no início do documentário, Buolamwini demonstra o erro de um sistema de análise facial com uma simples ação. Ela posiciona o seu rosto em frente a um espelho com a IA. Quando ela coloca a máscara branca, o sistema detecta a face. Quando tira, nada acontece (CRUZ, 2021).

2.3 RACISMO ALGORÍTMICO

Segundo Francisco Porfírio, racismo é a designação da discriminação e do preconceito contra pessoas ou grupos por causa de sua cultura ou cor, seja ela de aspecto direto ou indireto. Diferente do preconceito a discriminação é ação de separar, excluir ou diferenciar indivíduos ou objetos. Essas micro agressões variam do verbal “fala”, como comportamentais, que apresentam desrespeito, ofensas, pejorativos ou negativos (PORFÍRIO, 2022):

Um exemplo disso é o chamado “racismo algorítmico”: distorções nas bases de dados de algoritmos que geram distorções nos resultados obtidos, sendo mais comuns os resultados de falso positivo em desfavor de pessoas negras que de pessoas brancas, criando situações de constrangimento e discriminação contra essa parcela da população que já é vítima de um racismo estrutural (AMPARO, 2020). Ademais, há, ainda, os dados que demonstram que 90,5% das pessoas presas através da utilização de monitoramento facial, no Brasil, são negros (NUNES, 2019), o que agrava tal panorama (BARROS al. el, 2020).

Com a internet crescendo cada dia mais, essas micro agressões passaram a ser não apenas verbais ou comportamentais mais também online, com discursos de ódio na internet, comentários ofensivos, uma discriminação racial online:

Segundo um estudo da NIST (National Institute of Standards and Technology), de 2018, os algoritmos de inteligência artificial se tornaram 25 vezes mais eficazes, com taxa de erro em cerca de 0,2%. Esse número, no entanto, não é o mesmo para pessoas negras (OLHAR DIGITAL, 2020).

É extensa a lista dos desafios de gerenciamento de projetos de IA, entretanto, podemos destacar os pontos que fazem fracassar os projetos de IA nas organizações: treinamento da equipe, desalinhamento de expectativas e dados insuficientes (FACUNDES,1996-2021).

Joy Buolamwini uma estudante de pós-graduação do MIT (Massachusetts Institute of Technology), por uma das mais consideradas instituições dos EUA, formada em várias áreas da tecnologia. Onde parte de sua jornada é pesquisar a ligação entre a tecnologia de impacto social e inclusão, desenvolveu um projeto onde utilizou um software genérico de reconhecimento facial, porém descobriu que para testá-lo com seu rosto teria que utilizar uma máscara branca, revelando que o software não estava pronto para identificar indivíduos da cor negra, apenas indivíduos brancos.

Segundo Joy, isso é bem problemático: “o preconceito algorítmico, como o preconceito humano, resulta da injustiça. Porém, os algoritmos, tal como os vírus, podem espalhar preconceitos numa grande escala num ritmo rápido. O preconceito em algoritmos também pode levar a experiências de exclusão e a práticas discriminatórias.” (PAES,2017).

Embora a inteligência artificial utilize um sistema que permite o processamento de dados pelas próprias máquinas, ainda há vieses algorítmicos, pois os dados fornecidos inicialmente às máquinas são disponibilizados por humanos, imputando seus posicionamentos aos sistemas. Destarte, a alimentação das máquinas por humanos traz, por conseguinte, discriminações e vieses algorítmicos(AZEVEDO,2022).

Os mesmos algoritmos que facilitam a vida de todos, como ao abrir seu smartphone não ser necessário inserir uma senha manual, apenas “mostrar” seu rosto para a câmera e seu dispositivo será desbloqueado com tal facilidade ao identificar seus traços. Podem também ter comportamentos racistas.

3 METODOLOGIA

Esta abordagem do Gerenciamento de Riscos é baseada no modelo de leitura, os métodos utilizados foram observações dos riscos de projetos utilizando algoritmos autônomos. Como em qualquer processo de tomada de decisão, precisamos de dados confiáveis e concisos para tomarmos decisões corretas, o mesmo aplicando-se em sistemas de IA (SOMMERVILLE, 2006).

Este estudo foi inspirado em tecnologias de reconhecimento facial que foram testadas com pessoas negras e obtiveram fracasso, pois as mesmas não identificaram os indivíduos por causa da sua cor. Pretendemos demonstrar os procedimentos metodológicos utilizados, como a coleta de dados e forma como o tratamento de dados é limitada e insuficiente.

Foram feitas revisões em trabalhos voltados para a Engenharia de Software onde obtivemos conceitos sobre os riscos em um desenvolvimento de uma tecnologia, riscos esses positivos e negativos onde pode afetar o todo de modo significativo. Foi observado que apesar de estarmos sempre desenvolvendo novas tecnologias gradualmente ainda existem muitas falhas.

Os artigos, documentários estudados foram identificados relatos de pessoas negras que foram "constrangidas" por desenvolvimentos de biometria facial, onde por exemplo ao tentar adentrar ao seu ambiente de trabalho teve seu rosto recusado pelo algoritmo. Isso porque as bases de dados utilizado na maioria desses desenvolvimentos são de uma supremacia branca, assim não identificando indivíduos de cor negra.

Foi revisado também sites, blogs, livros, revistas onde abrange conceito do racismo online e histórico, como este, afeta na vida das pessoas de cor negra abrangendo assim micro agressões. Apontando a significância de como a coleta de dados é primordial para evitar tais erros no desenvolvimento de tecnologias de biometria facial.

Quadro 1 - Artigos acadêmicos selecionados

TIPO	ANO	AUTOR	OBJETIVO DE ESTUDO	TÍTULO
Artigo	2019	Tarcízio Roberto da Silva	Padrões de branquitude na aprendizagem de máquina.	Visão computacional e vieses racializados: branquitude como padrão de aprendizado de máquina.
Artigo	2020	Fernanda Carrera	Como os algoritmos de reconhecimento facial se "alimentam".	A raça e o gênero da estética e dos afetos: Algoritmização do racismo e do sexismo em bancos contemporâneos de imagens digitais.
Artigo	2020	Isabela Maria Pereira Paes de Barros, Isabela Inês Bernardino de Souza Silva	Analisar a utilização do reconhecimento facial e em empresas públicas e privadas, identificando erros e falsos positivos.	Utilização do reconhecimento facial eletrônico por empresas para identificação de suspeitos: segurança ou violação do estado democrático de direito?
Artigo	2021	Alice Azevedo Magalhães, Tício Spínola Gomes	Como os algoritmos replicam preconceitos históricos.	Regulação de sistemas de reconhecimento facial para fins de segurança pública no Brasil: riscos e desafios.
Artigo	2022	Ramon Costa, Bianca Kremer	Desafios e perspectivas nos grupos vulneráveis no reconhecimento facial.	Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial.
Artigo	2022	Tarcízio Silva	Como as tecnologias impactam na minoria negra.	Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código.
Monografia	2022	Ingrid Borges de Azevedo	Direito e falhas no reconhecimento facial.	Reconhecimento facial e direito: propostas para uma IA antidiscriminatória.

Fonte: Elaborado pelo autor (2022).

4 CONCLUSÕES E CONSIDERAÇÕES FINAIS

Neste trabalho revisamos trabalhos que identificaram erros no reconhecimento facial com pessoas da cor negra, apontando riscos não apenas por conta das falhas descobertas nesse desenvolvimento, mas também para os indivíduos atingidos, onde estes podem ser ofendidos de forma online por esta tecnologia. Surgindo assim o chamado racismo algorítmico bem como as micro agressões.

Segundo Azevedo (2022) a inteligência artificial é alimentada por dados tendenciosos que possuem discriminações, uma vez que são inseridos por humanos. Sendo assim, a IA correlaciona os conceitos e cumpre seu objetivo de encontrar uma solução para um problema por meio de atividades, no entanto, não os compreende e replica padrões discriminatórios.

Identificamos desde os conceitos, as ações executadas pelos algoritmos de inteligência artificiais voltados para a capacidade de heteroidentificação de algoritmos de biometria facial. Revisando artigos, livros, blogs, documentários onde todos propuseram que os bancos de dados ainda são insuficientes e de supremacia branca.

Este trabalho foi de grande importância para o nosso conhecimento, como pessoa e programador. O aprofundamento deste tema fez com que refletimos não somente em inovar ou desenvolver algo novo, mas como o processo de desenvolvimento deve ser feito, o que irá atingir, quais são as consequências de que poderão vir a surgir, caso aquele projeto não seja feito de forma concisa, com dados significativamente balanceados. Devem-se cessar as falhas obtidas no desenvolvimento de tecnologias de biometria facial já que esta mostra em inúmeros relatos o mesmo erro.

REFERÊNCIAS

AZEVEDO, I. B. : **RECONHECIMENTO FACIAL E DIREITO: propostas para uma ia antidiscriminatória.** (2022)

BARROS, I. M. P. P. , SILVA I. I. B. S. S. : **UTILIZAÇÃO DO RECONHECIMENTO FACIAL ELETRÔNICO POR EMPRESAS PARA IDENTIFICAÇÃO DE SUSPEITOS: SEGURANÇA OU VIOLAÇÃO DO ESTADO DEMOCRÁTICO DE DIREITO?**

COSTA R., KREMER B. : **INTELIGÊNCIA ARTIFICIAL E DISCRIMINAÇÃO: DESAFIOS E PERSPECTIVAS PARA A PROTEÇÃO DE GRUPOS VULNERÁVEIS DIANTE DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL.** Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1316/1065>(2022).

CRUZ, B.S.. : **INTELIGÊNCIA ARTIFICIAL Com didatismo, "Coded Bias" é um "O Dilema das Redes" sobre falhas das IAs.** Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/04/10/coded-bias-da-netflix-prova-como-a-tecnologia-e-racista-e-viola-direitos.htm>(2021)

FACUNDES,E.: **Projetos de Inteligência Artificial.** Disponível em: <https://efagundes.com/projetos-de-inteligencia-artificial/>,1996-2021.

HALL, E.: **Managing Risk: Methods for Software Systems Development.** Addison-Wesley Reading (1998).

KLEINA N. : **Como funciona o reconhecimento facial.** Disponível em: <https://www.tecmundo.com.br/camera-digital/10347-como-funcionam-os-sistemas-de-reconhecimento-facial.htm>(2021).

MAGALHÃES, A. A., GOMES T. S. : **REGULAÇÃO DE SISTEMAS DE RECONHECIMENTO FACIAL PARA FINS DE SEGURANÇA PÚBLICA NO BRASIL: RISCOS E DESAFIOS.** (2021).

OLHAR DIGITAL, **De novo: reconhecimento facial incrimina erroneamente pessoas negras.** Disponível em : <https://olhardigital.com.br/2020/09/05/noticias/de-novo-reconhecimento-facial-incrimina-erroneamente-pessoas-negras/>, (2020).

OLIVEIRA C. D. C., CINTRA M. E., NETO F. M. M.: **Jogo sério para o ensino da Gestão de Riscos em Projetos de Softwares usando Inteligência Artificial,**(2013).

PASQUALE, F. : **The black box society.** Harvard University Press. Disponível em: <https://olhardigital.com.br/2020/09/05/noticias/de-novo-reconhecimento-facial-incrimina-erroneamente-pessoas-negras/>(2015).

PAES, B. : **JOY BUOLAMWINI E O PRECONCEITO ALGORÍTMICO.** Disponível em: <http://ovelhamag.com/joy-buolamwini-e-o-preconceito-algoritmico/>(2017).

PORFÍRIO, F.; **Racismo**. Disponível em: brasilecola.uou.com.br/sociologia/racismo.html(2022).

PFLEEGER, S. L., ATLEE, J. M.: **Student Study Guide for Software Engineering: Theory and Practice**(4th ed.). Prentice Hall Press, (2009).

SILVA,T. : **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais**. Publisher: Sesc Edições SP,. Disponível em: researchgate.net/publication/358278108_Racismo_algoritmico_inteligencia_artificial_e_discriminacao_nas_redes_digitais (2022).

SILVA, T. : **Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código**, (2019)

SILVA, T. R. : **VISÃO COMPUTACIONAL E VIESES RACIALIZADOS:BRANQUITU DE COMO PADRÃO NO APRENDIZADO DE MÁQUINA**. Disponível em:https://www.copenenordeste2019.abpn.org.br/resources/anais/13/copenenordese2019/1562639906_ARQUIVO_e9a44399eb59657e3a09d60cac35b5a8.pdf, (2019)

SOMMERVILLE, I.. **Software Engineering**. 8th edition. International Computer Science. Addison- Wesley Longman Publishing Co., Inc. (2006).