UNIVERSIDADE FEDERAL DE SANTA CATARINA – UFSC
CENTRO DE CIÊNCIAS DA EDUCAÇÃO – CED
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO – PGCIN

GABRIELA CHIRITTE GRANEMANN

DIGA "XIS": O RECONHECIMENTO FACIAL IDENTIFICADO NA LITERATURA CIENTÍFICA EM CIÊNCIA DA INFORMAÇÃO

FLORIANÓPOLIS
2023

GABRIELA CHIRITTE GRANEMANN

DIGA "XIS": O RECONHECIMENTO FACIAL IDENTIFICADO NA LITERATURA CIENTÍFICA EM CIÊNCIA DA INFORMAÇÃO

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Informação (PGCIN) da Universidade Federal de Santa Catarina (UFSC) como requisito para a obtenção do Grau de Mestre em Ciência da Informação em área de concentração: Gestão da Informação. Linha de pesquisa: Organização, Representação e Mediação da Informação e do Conhecimento. Eixo temático: Informação, Comunicação e Competências.

Orientador: Prof. Dr. Enrique Muriel-Torrado.
Coorientador: Prof. Dr. Edgar Bisset Alvarez.

.

FLORIANÓPOLIS
2023

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Chiritte Granemann, Gabriela
Diga "xis" : o reconhecimento facial identificado na literatura científica em ciência da informação / Gabriela Chiritte Granemann ; orientador, Enrique Muriel-Torrado, coorientador, Edgar Bisset Alvarez, 2023.
146 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação, Programa de Pós Graduação em Ciência da Informação, Florianópolis, 2023.

Inclui referências.

1. Ciência da Informação. 2. Reconhecimento Facial. 3. Algoritmos. 4. Racismo. 5. Biblioteca. I. Muriel-Torrado, Enrique. II. Bisset Alvarez, Edgar. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Informação. IV. Título.

Gabriela Chiritte Granemann

DIGA "XIS": O RECONHECIMENTO FACIAL IDENTIFICADO NA LITERATURA CIENTÍFICA EM CIÊNCIA DA INFORMAÇÃO

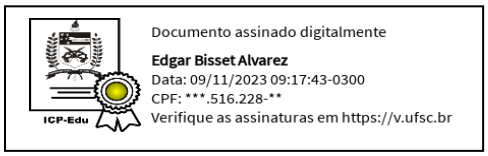
O presente trabalho em nível de mestrado foi avaliado e aprovado, em 09 de agosto de 2023, pela banca examinadora composta pelos seguintes membros:

Prof. Douglas Dyllon Jeronimo de Macedo, Dr.
Universidade Federal de Santa Catarina (PGCIN/UFSC)

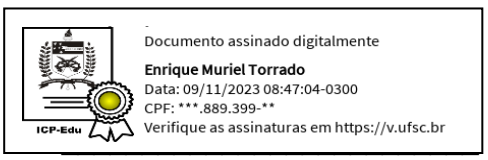
Prof.Marco Schneider, Dr.
Universidade Federal do Rio de Janeiro (PPGCI/IBICT-ECO/UFRJ)

Prof. Professor Medina Kern, Dr.
Universidade Federal de Santa Catarina (PGCIN/UFSC)

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestra em Ciência da Informação.



Prof. Edgar Bisset Alvarez, Dr.
Coordenação do Programa de Pós-Graduação



Prof. Enrique Muriel-Torrado, Dr.
Orientador

Florianópolis, 2023.

Dedico aos trabalhadores da informação do Brasil que incansávelmente lutam pelo acesso a informação democrática e (re)existência das bibliotecas públicas e escolares.

AGRADECIMENTOS

Em primeiro lugar, agradeço imensamente ao Artur, meu amigo, camarada e futuro esposo. Além de ter estado ao meu lado durante todo o processo de desenvolvimento, escrita e correções desta dissertação, me inspirou nas leituras dentro do pensamento marxista. Tenho certeza de que a cada nova conversa, a cada nova aventura, a cada nova cidade, a cada novo forró e chorinho serei mais grata e apaixonada pela sua companhia.

Meus pais, Ana Carla e Roney, pela vida e educação que hoje proporcionam para que este momento possa acontecer. Pelo apoio e suporte em todas as minhas escolhas profissionais, na torcida pela minha felicidade. À minha mãe, pelos afagos e comidinhas em dias difíceis, e ao meu pai, pelos conselhos e carinhos de incentivo.

Meu irmão Guilherme, um dos seres humanos mais inteligentes e determinados que conheço, obrigada pelo apoio e preocupação durante o período de pesquisa. Agradeço pela compreensão da minha ausência, que não foram poucas.

Ao Professor e meu orientador Enrique Muriel-Torrado, que em 2019 me aceitou em sua aula como ouvinte, sem estar na pós-graduação, e despertou o meu interesse pela pesquisa por meio de suas aulas maravilhosas. A sensibilidade e relevância que da aos temas pertinentes à sociedade constituíram elementos cruciais para o enriquecimento desta dissertação. Obrigada por me mostrar que posso ser pesquisadora, obrigada por todas as trocas, pelas orientações, as correções :) e pela amizade que construímos ao longo desta caminhada.

Ao Professor e meu coorientador Edgar Bisset Alvarez, obrigada por ter aceitado esta coorientação. Agradeço por suas orientações e conversas que abriram os caminhos desta pesquisa e que me levaram à qualificação e ao desenvolvimento seguinte.

Professor Douglas, por suas preciosas contribuições no exame de qualificação que ajustaram rumos da pesquisa e por aceitar o convite para compor a banca de defesa. Muito obrigada!

Professor, pesquisador e ser humano admirável, Marco Schneider, agradeço por ter sido sua aluna no período de isolamento social, nas disciplinas do IBICT/UFRJ que, junto ao Professor Arthur Bezerra Coelho, me trouxeram um pouco de leveza para este período duro, com leituras e debates que me ajudaram no amadurecimento do pensamento crítico. Agradeço por suas sugestões/aulas na banca de qualificação e de defesa.

À Professora e amiga Olinda Evangelista, por seus conselhos e pelas inúmeras vezes que se disponibilizou a me ajudar.

A Maristela e Samuel, pela preocupação, carinho e incentivo constante.

Às amigas Gabriela Bernardo, Gabriela Alvarez e Mariana Bernardo, agradeço a compreensão das minhas ausências em fases importantes. Celebraremos juntas, como tantas outras alegrias vividas.

À Danielle Borges, Mateus Rebouças e Jônatas Edison, amizade avassaladora do mestrado que me fez querer estar ao lado de vocês desde os primeiros dias. Jonatas, que além de amigos, somos colegas de orientação. Obrigada pelo apoio, pelas risadas, cafés, leituras conjuntas e toda a torcida.

À Pri Sena que de professora da graduação virou amiga, obrigada por todos os momentos de escuta, empatia e disponibilidade. Sua alegria é contagiante.

Às colegas e amigas da Coordenadoria Regional de Educação de Itajaí: Soraia por dividir seus dias e seus ensinamentos comigo, trazendo gargalhadas aos dias de trabalho intenso e tenso dentro da Educação Estadual de Santa Catarina. À André Torquato, pela amizade e por compartilhar suas experiências de pós-graduação. Me mostrou que tudo pode virar uma boa história. À Raquel, por sua genuína preocupação com minha saúde mental e física durante este processo. Agradeço ainda pelo seu carinho e torcida. D. Tânia por sua fé na educação pública e sua dedicação a ela.

A Luis Fernando Vanin e Janssen Vasconcelos de Souza, amigos da graduação/CAB, com quem tenho o prazer de dividir as alegrias e angústias da pós-graduação e a trajetória como bibliotecários na Educação Estadual de Santa Catarina.

Às fortes amizades que estão presentes em minha vida desde a escola e foram importantes em todas as fases: Guilherme de Sousa, Munique Boing, Cristina V. Virgílio, Thiago de Oliveira Aguiar, Vicente da Rosa, Talles Vinicius Pereira, Rafael Haviaras, Bruno Gayger e Patricia de Bairros.

Agradeço pelos anos de militância no Coletivo Feminista Classista Ana Montenegro, pela minha formação política e disciplinar de leituras densas, estudos e debates.

Agradeço à existência das bibliotecas públicas, universitárias, escolares e comunitárias que me serviram como verdadeiros portos todos esses anos de minha vida, em todas as cidades que passei.

A gratidão à generosidade e à atenção daqueles que contribuíram direta e indiretamente para a realização desta jornada ficam aqui expressadas.

A árvore quando é cortada
Chora e sofre de tal maneira
Pois vê que o machado que sangra o seu tronco
Também é feito de madeira
[...] Pra cada tronco um machado
Bem-vinda revolta cresce
Se quem bate mal se lembra
Quem apanha nunca esquece
Quem tombou pela cor?
Pela cor, quem tombou?
Quem sangrou pela cor?
Pela cor, quem sangrou?

Trovoada – El Efecto (2018)

RESUMO

Os algoritmos de reconhecimento facial (RF) são um dos segmentos em avanço contínuo da inteligência artificial e são aplicados em setores como segurança pública, marketing, saúde e bibliotecas. É crescente também a preocupação social sobre seu uso, e se colocam em questão a vigilância e a privacidade, além de denúncias de suspeitas de vieses racistas, machistas e transfóbicos. O objetivo geral desta pesquisa é verificar como a literatura acadêmica em ciência da informação (CI) compreende a existência de efeitos sociais decorrentes da aplicação de RF. Para nortear os caminhos deste estudo, foram definidos três objetivos específicos: a) Identificar as pesquisas sobre reconhecimento facial na CI no Brasil e no âmbito internacional. b) Caracterizar os efeitos sociais identificados na literatura científica derivados das aplicações de reconhecimento facial. c) Categorizar o reconhecimento facial identificado no levantamento, agrupado por especificidade ou correlação. Para atender aos objetivos deste estudo, a metodologia aplicada foi a pesquisa bibliográfica, exploratória e qualitativa. O trabalho foi composto por artigos científicos indexados nas bases: Web of Science, DOAJ, LENS e Dimensions. Os autores clássicos foram utilizados para conceituar e aprofundar o funcionamento dos elementos centrais da pesquisa, como explicar IA, machine learning e algoritmos de reconhecimento facial. A metodologia pensada para a categorização dos efeitos sociais identificados na literatura científica foi a categorização de Bardin, que indica cinco recomendações para categorias de qualidades: a) exclusão mútua; b) homogeneidade; c) pertinência; d) objetividade e fidelidade; e e) produtividade. Cada artigo faz parte de apenas uma categoria, pois a categoria representa o assunto do artigo analisado. Após a coleta e triagem, foram caracterizados e categorizados 37 artigos em cinco categorias. Categoria 1 – Vigilância e Privacidade: trata sobre a coleta e uso de informações pessoais por meio dos algoritmos de RF para monitoramento, vigilância, e a preocupação com a falta de privacidade ocasionada. Na Categoria 2 – Bibliotecas e Arquivos, os artigos trazem o uso do RF como segurança de acervos e usuários, monitoramento de acesso às bibliotecas e atrasos nos empréstimos. Existe uma possível substituição do profissional bibliotecário pela IA, porém a IFLA se posiciona contra o uso do RF, pois contraria os códigos e manuais de ética da profissão bibliotecária, que afirmam que o usuário tem o direito à proteção da privacidade. A Categoria 3 – Gênero e Raça expõe os problemas do RF referentes a gênero e raça, que incluem problemas prévios sociais fortalecendo racismo e misoginia. Na Categoria 4 – Saúde, os artigos desenvolvem boas aplicações do RF no diagnóstico de doenças e facilidades na vida de pessoas com deficiências. E a Categoria 5 – Software é composta por pesquisas em busca de melhorias nos algoritmos de RF para que os erros diminuam cada vez mais. Os resultados das análises e identificação dos efeitos e suas ligações com a CI demonstram que, embora seja promissor o uso nas áreas de saúde, nas demais categorias o uso é levantado como um "benefício limitado" e deve ser utilizado com responsabilidade e ética, buscando o desenvolvimento de políticas junto as bibliotecas, que não afetem os direitos humanos. Com isso, o estudo busca ser uma fonte de informação que possa fazer parte e expandir a comunicação científica do reconhecimento facial e suas ligações com a ciência da informação.

Palavras-Chaves: algoritmos; categorias; ciência da Informação; comunicação científica; reconhecimento facial.

ABSTRACT

Facial recognition algorithms (FR) are one of the continuously advancing segments of artificial intelligence and are applied in sectors such as public security, marketing, healthcare, and libraries. There is also growing social concern about their use, raising questions about surveillance and privacy, as well as allegations of racist, sexist, and transphobic biases. The overall objective of this research is to investigate how academic literature in information science (IS) understands the existence of social effects resulting from the application of FR. To guide the paths of this study, three specific objectives were defined: a) Identify research on facial recognition in IS in Brazil and internationally. b) Characterize the social effects identified in scientific literature derived from facial recognition applications. c) Categorize the facial recognition identified in the survey, grouped by specificity or correlation. To meet the objectives of this study, the applied methodology was bibliographic, exploratory, and qualitative research. The work consisted of scientific articles indexed in the following databases: Web of Science, DOAJ, LENS, and Dimensions. Classic authors were used to conceptualize and deepen the functioning of the central elements of the research, such as explaining AI, machine learning, and facial recognition algorithms. The methodology designed for categorizing the social effects identified in scientific literature was Bardin's categorization, which indicates five recommendations for quality categories: a) mutual exclusion; b) homogeneity; c) relevance; d) objectivity and fidelity; and e) productivity. Each article belongs to only one category because the category represents the subject of the analyzed article. After collection and screening, 37 articles were characterized and categorized into five categories. Category 1 - Surveillance and Privacy: addresses the collection and use of personal information through FR algorithms for monitoring, surveillance, and concerns about privacy infringements. In Category 2 - Libraries and Archives, the articles discuss the use of FR for the security of collections and users, monitoring access to libraries, and delays in loans. There is a potential replacement of library professionals by AI, but IFLA opposes the use of FR as it contradicts the codes and ethical manuals of the library profession, which affirm that users have the right to privacy protection. Category 3 - Gender and Race exposes the problems of FR regarding gender and race, including pre-existing social issues reinforcing racism and misogyny. In Category 4 - Health, the articles explore the positive applications of FR in disease diagnosis and improving the lives of people with disabilities. Category 5 - Software consists of research seeking improvements in FR algorithms to reduce errors. The results of the analyses and the identification of effects and their connections with IS demonstrate that while the use in healthcare shows promise, in other categories, the use is seen as a "limited benefit" and should be used responsibly and ethically, seeking the development of policies alongside libraries that do not infringe on human rights. Thus, the study aims to be an information source that can be part of and expand the scientific communication of facial recognition and its connections with information science.

Keywords: algorithms; categories; Information Science; scientific communication; facial recognition.

RESUMEN

Los algoritmos de reconocimiento facial (RF) son uno de los segmentos en constante avance de la inteligencia artificial y se aplican en sectores como seguridad pública, marketing, salud y bibliotecas. También existe una creciente preocupación social sobre su uso, cuestionando la vigilancia y la privacidad, así como denuncias de sospechas de sesgos racistas, sexistas y transfóbicos. El objetivo general de esta investigación es verificar cómo la literatura académica en ciencia de la información (CI) comprende la existencia de efectos sociales derivados de la aplicación de RF. Para guiar los caminos de este estudio, se definieron tres objetivos específicos: a) Identificar investigaciones sobre reconocimiento facial en CI en Brasil y a nivel internacional. b) Caracterizar los efectos sociales identificados en la literatura científica derivados de las aplicaciones de reconocimiento facial. c) Categorizar el reconocimiento facial identificado en el estudio, agrupado por especificidad o correlación. Para cumplir con los objetivos de este estudio, se aplicó una metodología de investigación bibliográfica, exploratoria y cualitativa. El trabajo consistió en artículos científicos indexados en las bases de datos: Web of Science, DOAJ, LENS y Dimensions. Se utilizaron autores clásicos para conceptualizar y profundizar en el funcionamiento de los elementos centrales de la investigación, como explicar IA, aprendizaje automático y algoritmos de reconocimiento facial. La metodología propuesta para la categorización de los efectos sociales identificados en la literatura científica fue la categorización de Bardin, que establece cinco recomendaciones para categorías de cualidades: a) exclusión mutua; b) homogeneidad; c) pertinencia; d) objetividad y fidelidad; y e) productividad. Cada artículo pertenece a una sola categoría, ya que la categoría representa el tema del artículo analizado. Después de la recopilación y selección, se caracterizaron y categorizaron 37 artículos en cinco categorías. Categoría 1: Vigilancia y Privacidad: aborda la recopilación y uso de información personal a través de algoritmos de RF para monitoreo, vigilancia y preocupaciones por la falta de privacidad. En la Categoría 2: Bibliotecas y Archivos, los artículos presentan el uso de RF para la seguridad de las colecciones y usuarios, el monitoreo del acceso a las bibliotecas y los retrasos en los préstamos. Existe una posible sustitución del profesional bibliotecario por IA, pero la IFLA se opone al uso de RF, ya que contradice los códigos y manuales éticos de la profesión bibliotecaria, que afirman que el usuario tiene derecho a la protección de la privacidad. La Categoría 3: Género y Raza expone los problemas de RF relacionados con el género y la raza, que incluyen problemas sociales previos que refuerzan el racismo y la misoginia. En la Categoría 4: Salud, los artículos desarrollan buenas aplicaciones de RF en el diagnóstico de enfermedades y en la mejora de la vida de las personas con discapacidades. Y la Categoría 5: Software está compuesta por investigaciones en busca de mejoras en los algoritmos de RF para reducir los errores cada vez más. Los resultados del análisis y la identificación de los efectos y sus conexiones con la CI demuestran que, aunque su uso en el ámbito de la salud es prometedor, en las demás categorías se plantea como un "beneficio limitado" y debe utilizarse de manera responsable y ética, buscando el desarrollo de políticas junto con las bibliotecas que no afecten los derechos humanos. Con esto, el estudio busca ser una fuente de información que pueda formar parte y ampliar la comunicación científica del reconocimiento facial y sus conexiones con la ciencia de la información.

Palabras clave: algoritmos; categorías; ciencia de la Información; comunicación científica; reconocimiento facial.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ALA	American Library Association
BRAPCI	Base de dados de Periódico sem Ciência da Informação
RF	Reconhecimento Facial
CI	Ciência da Informação
DUDH	Declaração Universal dos Direitos Humanos
IA	Inteligência artificial
IFLA	International Federation of Library Associations and Institutions
IoT	*Internet of Things*
LGBTQIAP+	Lésbicas, gays, bissexuais, transsexuais, Queer, Interssexo, Assexuais e Pansexuais +
LIS	Library and Information Science
ONU	Nações Unidas
WoS	*Web of Science*

SUMÁRIO

1 INTRODUÇÃO

> Os meios de comunicação e informação de massas – controlados e manipulados eletronicamente – têm como objetivo construir e apresentar midiaticamente o mundo capitalista como o único possível, sem o qual não são, se quer, concebíveis outras formas de vida, de trabalho e de existência humana. Trata-se de convencer as pessoas de que os princípios da concorrência entre os seres humanos, a 'destruição criativa' de empresas, homens e natureza, o individualismo, o egoísmo, o racismo e o instinto de sobrevivência, constituem os eixos motores de toda ação humana, que são perfeitamente compatíveis com a ordem estabelecida pelo sistema capitalista (VALENCIA, 2019, p. 209-210).

Em 2023, a Declaração Universal dos Direitos Humanos (DUDH) (ONU, 1948) completa 75 anos, surgiu como uma resposta imediata das Nações Unidas (ONU) após duas grandes guerras mundiais. Seu texto expõe a garantia para qualquer ser humano, em qualquer país e sob quaisquer circunstâncias, de condições mínimas de sobrevivência e crescimento em ambiente de respeito e paz, igualdade e liberdade. No entanto, a DUDH nasceu em tempos diferentes da tecnologia de inteligência artificial (IA) existentes em nosso cotidiano.

A IA teve suas primeiras pesquisas e uso em meados dos anos de 1950, após a Segunda Guerra Mundial, momento em que surge a primeira rede de computadores, a internet, e atualmente abrange uma variedade de subcampos, está presente no mercado de ações, dirige carros, atua nas contratações de RH, diagnóstico de doenças, automatiza atendimentos, desenvolvimento de textos e vídeos e reconhecimentos de imagens, dentre outras funções.

Em uma iniciativa da *UN Global Pulse*[1] , Joseph Bullock e Miguel Luengo-Oroz (2019)[2] utilizaram apenas os dados de código-fonte aberto e colocaram em funcionamento um falso gerador de discursos de líderes políticos em assembleias da ONU. Treinaram este modelo em discursos proferidos em Assembleias Gerais da ONU de 1970 a 2015, e em 13 horas de trabalho os pesquisadores conseguiram novos discursos "realistas" com temas variados e sensíveis ao mundo (BARBOSA, 2019). Assim como vemos o ChatGPT com respostas e textos produzidos baseado no conteúdo que o alimenta.

---

[1] "A Global Pulse das Nações Unidas é o laboratório de inovações da Secretaria Geral, um hub de experimentação para fundamentar e avançar a carta das Nações Unidas" (UN GLOBAL PULSE, 2023, tradução nossa). No original estava "UN Global Pulse *is the Secretary-General's Innovation Lab — a hub for experimentation to support and advance the UN Charter"* (UN GLOBAL PULSE, 2023).

[2] BARBOSA (2019, p. 50), não informa o nome dos pesquisadores em seu livro.

Com a IA e a Internet das Coisas (IoT - do inglês *Internet of Things*)[3], formou-se um “meio informacional”, decorrente da conexão propiciada entre o mundo físico e o digital (ROZSA *et al*., 2017). Isso impulsionou a chegada das mídias sociais e a gama de informações que a população é estimulada a inserir nelas rotineiramente sobre suas vidas, sob uma ideia de sensação de liberdade.

A ideia de liberdade, para Bauman (2001), foi fortalecida nas discussões acerca da vida contemporânea. A esse respeito, o autor asserta que a liberdade individual pode ser considerada como uma pseudoliberdade. A liberdade individual muito propalada pelo neoliberalismo, por poder expor suas opiniões, às vezes como verdades únicas (BAUMAN, 2001). Em outras palavras, embora as pessoas acreditem que são livres para tomar suas próprias decisões, essa sensação de liberdade não reflete a verdadeira liberdade em si. Essa ilusão de liberdade é o resultado de fatores externos, tais como a influência da mídia, pressão social, restrições econômicas que limitam as opções disponíveis para as pessoas. Para superar essa pseudoliberdade, é necessário que as pessoas questionem a origem de suas escolhas e reflitam sobre o conceito de liberdade individual, a fim de tomar decisões mais conscientes e autônomas. Além disso, é crucial que sejam criadas condições para que as pessoas tenham acesso a um conjunto mais amplo de opções, permitindo-lhes desfrutar de uma verdadeira liberdade de escolha.

Nas mídias sociais, a liberdade é muitas vezes ilusória, uma vez que plataformas de recomendação usam algoritmos para monitorar, analisar e filtrar grandes quantidades de dados, conhecidos como big data. Essa abordagem, conhecida como “cultura algorítmica”, é projetada para oferecer uma experiência personalizada aos usuários, mas pode acabar limitando suas opções e reforçando sua posição dentro de um ecossistema fechado.

Ao navegar pelas redes socias, os usuários são apresentados a uma série de recomendações que são selecionadas com base em seus interesses, comportamentos e histórico de navegação. Isso pode criar a ilusão de que estão livres para escolher o que desejam, mas, na verdade, as escolhas já estão limitadas pelas recomendações apresentadas a ele. A possibilidade de que um usuário seja exposto apenas a informações e opinioes preexistentes, sem ter contato com perspectivas alternativas, tende a levar a um empobrecimento do debate público e a polarização ainda maior das

[3] Foi estimado, por Evans (2011), que em 2008, a internet das pessoas foi superada pela internet das coisas. Desde então, a diferença entre o número de coisas e o número de pessoas conectados à internet cresceu tanto que, atualmente, o número de coisas conectadas pela internet é mais de dez vezes o número de pessoas.

opiniões.

É importante destacar que as midias sociais são frequentemente condicionadas pelo objetivo das plataformas de maximizar o engajamento do usuário, mantendo-o conectado para consumir conteúdo o maior tempo possível. Essa lógica pode levar a um aumento da dependência das mídias sociais e a um comprometimento da privacidade e segurança dos seus usuários (HAN, 2017).

Embora o *big data* esteja associado e exemplificado constantemente como "um grande volume de dados", sua definição é dada por um conjunto de três (3) a cinco (5) dados produzidos com volume, velocidade e variedade (Vs). O volume diz respeito à quantidade de dados gerados, a variedade está relacionada aos diferentes formatos dos dados, que incluem imagens, sons e vídeos – muitos compartilhados por aplicativos de redes sociais –, e às diferentes fontes de onde os dados são gerados, como sensores cada vez mais específicos e sofisticados, como os usados para monitorar o corpo quando uma pessoa realiza atividades físicas. Para dois "Vs" a mais, aparece veracidade e valor (SONG; ZHU, 2016).

AMARAL (2016) explica que big data é o fenômeno em que os dados são produzidos em formatos diversificados e armazenados por uma grande quantidade de dispositivos e equipamentos. Nossos dados são coletados por meio de algoritmos que, intrínsecos da IA[4] são frequentemente ilustrados como atividades cotidianas. Os algoritmos não são necessariamente programas de computador, mas sim os passos que devem seguir para realizar tarefas. E no caso das redes, as tarefas podem variar de coleta e disseminação:

> Os algoritmos se empanturram de dados sobre você a cada segundo. Em que tipos de link você clica? Quais são os vídeos que vê até o fim? Com que rapidez pula de uma coisa a outra? Onde você está quando faz essas coisas? Com quem está se conectando pessoalmente on-line? Quais são as suas expressões faciais? Como o tom da sua pele muda em diferentes situações? O que você estava fazendo pouco antes de decidir comprar ou não alguma coisa? Você vota ou se abstém? […] Os algoritmos correlacionam o que você faz com o que quase todas as outras pessoas têm feito (LARNIER, 2018).

A internet, no início da disseminação de seu uso como fonte de informação e notícias, oferecia a perspectiva de ser livre acesso à informação e sem intermediação, o que "libertava" as pessoas da curadoria tradicional e vieses da mídia. Com a exploração e acumulação dos dados, o modo de disseminação das informações deixou de ser um livre acesso para uma entrega automatizada de informação filtrada, conteúdo

[4] Os algoritmos fazem parte de subcampos da Inteligência Artificial.

recomendado e personalizado[5].

Para a pesquisadora Shoshana Zuboff, *big data* não é uma tecnologia ou efeito tecnológico inevitável. Não é um processo autônomo, sua origem é plenamente social. A autora intitula essa nova lógica de acumulação, que troca dados pessoais por dinheiro, de Capitalismo de Vigilância, do qual o *big data* é tanto uma condição como uma expressão (ZUBOFF, 2015, p. 77).

> O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como *superávit* comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em *produtos de predição* que antecipam o que um determinado individuo faria agora, daqui a pouco e mais tarde. [...] Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro (ZUBOFF, 2020, p.19).

O monitoramento de dados não é algo neutro ou utilizado para uma única finalidade, ele é promovido por corporações e pelo próprio Estado. A vigilância digital é compreendida com base na sua operação, e conforme os últimos acontecimentos no Brasil e no mundo envolvendo mídias sociais, percebemos que não é apenas para fins de publicidade, mas também para fins políticos (BEZERRA, 2017).

Se o discurso utilizado por candidatos a eleições era considerado uma das ferramentas para manipular a opinião pública, hoje, ele se aliou às tecnologias, passando a utilizar dados pessoais adquiridos nas mídias sociais por meio dos algoritmos.

Além de interferir na legitimidade em eleições, a IA, de forma contínua pode trazer consequências sociais afetando a condução de temas de interesse da sociedade. A sociedade atual é desregulamentada, pois o mercado é quem dita as regras e as regras do mercado são marcadas pelo modelo econômico capitalista, o qual tem adotado o serviço de empresas que coletam informações pessoais dos consumidores e as revendem ou compartilham com outras, denominadas como *data brokers (*BAUMAN, 2001).

A conexão digital tem sido um meio para fins comerciais de terceiros. Em sua essência, o capitalismo de vigilância é parasítico e autorreferente. Que nos traz a imagem conceitual de Karl Marx sobre o capitalismo ser como um vampiro que se

[5] Personalização não é o mesmo que individualização, o que ocorre é uma "desindividualização".

alimenta da força de trabalho[6], e agora o capitalismo de vigilância se alimenta de todos os aspectos e de toda a experiência humana (ZUBOFF, 2020, p. 20).

Estamos diante do próprio capitalismo e sua tendência é transformar tudo em mercadoria. Os dados pessoais são os principais insumos para os lucros das corporações que fazem uso de *big data*, que tomam decisões cruciais sobre como classificar e hierarquizar os indivíduos analisando nossas atividades de compras, o que assistimos e até nossa característica física, por meio de algoritmos fechados cuja observação não permite saber o que fazem.

Nosso comportamento nas plataformas é observado e estimulado com pequenas "doses de dopaminas", conforme apelidado por Sean Parker, primeiro Presidente do Facebook (LARNIER, 2018). Seriam as técnicas de modificação de comportamento que resultam em um vício, e quanto mais alimentamos as redes mais o algoritmo aprende sobre nós. De acordo com Assange (2015, p. 15) "[...] a influência do Google sobre as escolhas e o comportamento de todos os seres humanos se traduz em um poder concreto de influenciar o rumo da história".

O sistema inteligente das plataformas não visa, prioritariamente, oferecer o conteúdo considerado de melhor qualidade aos usuários, mas maximizar sua permanência na rede social, promovendo e ampliando as interações. Quanto mais tempo e intensidade de interação, mais dados são gerados, o que favorece o aprendizado de máquina e os modelos de negócios baseados em dados.

Os algoritmos estão em todo lugar, fazem parte de nossas rotinas e permitem avanços tecnológicos expressivos para a sociedade: nas áreas da educação, mobilidade urbana, desenvolvimento de casas e carros inteligentes, no consumo de produtos, auxiliam setores de marketing a atingir seu público-alvo de forma mais certeira. Na saúde, colaboram na prevenção e diagnósticos de doenças com análise de imagens ou indicadores de sintomas, trazendo mais conforto à população, muitas vezes com o intuito de chegar atendimento a comunidades distantes. Um dos segmentos que acompanham essa evolução é o sistema de reconhecimento facial (RF), também chamado de "biometria facial".

O reconhecimento facial permite a identificação de pessoas em meio à multidão, sendo bem aplicado na área de segurança pública e privada, no desbloqueio dos aparelhos digitais, nos bancos digitais como forma comprobatória do documento de

[6] O vampiro que se alimenta do sangue e suor da força de trabalho e não fica saciado nunca. Para Marx não é o trabalho mas o trabalhador. "[...] o tempo em que está livre para vender sua força de trabalho é o tempo em que é forçado a vende-la e que seu vampiro não o solta 'enquanto houver um músculo, um nervo, uma gota de sangue a explorar'" (MARX, 2011, p. 346).

identificação e no transporte público. Recentemente a Hering, uma indústria especializada em vestuário, colocou sistemas semelhantes em uma loja da capital paulista com o intuito de examinar os comportamentos dos consumidores, seus interesses e práticas para considerar uma estratégia de marketing (AGENCIABRASIL, 2019). Além da biometria facial, outras formas utilizadas de reconhecimento do ser humano são a íris, a retina, as digitais dos dedos das mãos, as veias da mão, a voz, o rosto, entre outros (KOCH, 2012).

Contudo, esse "regime de informação", termo utilizado por González de Gomez (2002) para definir o modo de produção de informação dominante em uma formação social, têm apresentado resultados que ferem as leis de direitos humanos, que não produzem verdades comprobatórias, chegam a realizar condenações penais de pessoas inocentes, demissões de pessoas e até a não contratação para uma vaga de emprego (BARBOSA, 2019).

Castells (2012) alertava que este novo sistema poderia gerar ou teria uma tendência a aumentar a desigualdade social.

> Os sistemas de coleta e análise de informações que apoiam decisões de guerra e investigações policiais são conhecidos pelo simpático nome de "inteligência". Eles trazem promessa de intervenções mais justas, cirúrgicas, pouco sangue derramado, sequelas mínimas (ENTLER, 2021, p. 1).

Em 2013, um homem foi condenado nos Estados Unidos após o juiz responsável utilizar um sistema de IA conhecido como COMPASS. Conforme a avaliação de risco e previsão do *software* o cidadão teria grande probabilidade de reincidência. Também em Chicago/EUA, em 2015, foi criada a Lista de Assuntos Estratégicos (*Strategic Subject List*), que tem por objetivo classificar quais cidadãos têm mais probabilidade de envolvimento em atividades criminosas (CASSINO; AVELINO; SILVEIRA, 2019). Neste caso apesar da lista não apresentar nome, cor e etnia para o público, visto que foi publicada online, nos questionamos até onde este regime não fere a transparência dos julgamentos e o direito de presunção de inocência.

Tecnologias de imagem não são úteis apenas a esse campo, conforme Virilio (1991), antes de encontrarem seu lugar na vida do cotidiano, esses sistemas nasceram e alcançaram seus desempenhos como tecnologias de guerra (VIRILIO, 1991). Se analisássemos dessa forma, poderíamos tentar fazer alguns paralelos: Numa guerra, teoricamente, nós combatemos um inimigo, e hoje será que temos algum inimigo a ser combatido?

Em 2021, um cientista de dados foi preso por engano, no Brasil, por meio de RF

feito por foto. A única semelhança entre ele e o suspeito é a cor da pele: ambos são negros. Só no Rio de Janeiro, foram 73 pessoas presas injustamente por reconhecimento facial, e 81% destas pessoas apontadas como suspeitas nesses inquéritos são negras (GELEDES, 2021). Além de denúncias de racismo, o algoritmo de reconhecimento facial tem se mostrado com pouca eficácia em reconhecer pessoas transgêneros e mulheres cis em comparação a homens brancos.

Preconceito contra mulheres, negros, lésbicas, gays, bissexuais, transsexuais, Queer, Interssexo, Assexuais e Pansexuais (LGBTQIAP+) ou qualquer outro grupo é uma violação do Artigo 7° da Declaração Universal dos Direitos Humanos: “Todos são iguais perante a lei e, sem distinção, têm direito a igual proteção da lei. Todos têm direito a proteção igual contra qualquer discriminação que viole a presente Declaração e contra qualquer incitamento a tal discriminação” (ONU, 1948), mas podem os algoritmos por si serem preconceituosos?

Nas últimas décadas, pesquisadores da área da Ciência da Informação (CI) (BEZERRA, 2017; GONZÁLEZ DE GÓMEZ, 2002; ROZSA *et al.,* 2017) têm direcionado suas pesquisas para regime de informação, IA, IoT, Algoritmos, destacando por vezes os aspectos sociais intrínsecos da área. Por essa razão, este estudo pretende abordar as pesquisas realizadas sobre o RF por meio dos olhares da CI, e por ser uma área habilitada a atuar nas etapas do ciclo da informação, além de sua função social.

Esta pesquisa é motivada pelo aumento de denúncias e suspeitas de algoritmos que podem conter viés racial, de gênero e transfobia, como mencionado anteriormente. Com o desenvolvimento da IA, da aprendizagem de máquina surgiu o questionamento de como os algoritmos de reconhecimento facial têm interferido e quais os seus efeitos na sociedade, a partir dos dados que os alimentam? Para responder à pergunta central desta pesquisa, se propõe como objetivo principal: verificar como a literatura acadêmica em ciência da informação apreende a existência de efeitos sociais consequentes da aplicação de reconhecimento facial.

Para nortear o estudo e êxito do objetivo central, foram adicionados três objetivos específicos:

a) Identificar as pesquisas sobre reconhecimento facial na CI no Brasil e no âmbito internacional.
b) Caracterizar os efeitos sociais identificados na literatura científica derivados das aplicações de reconhecimento facial.

c) Categorizar o reconhecimento facial identificado no levantamento, agrupado por especificidade ou correlação.

1.1 DELIMITAÇÃO DA PESQUISA

A presente pesquisa visou analisar estudos que abordassem os efeitos sociais dos algoritmos de reconhecimento facial. Para tanto, foram examinados temas intimamente relacionados, como a internet, o desenvolvimento da inteligência artificial, a ciência da informação e a sociedade, esta última sendo um ator indispensável na existência e nos efeitos desses elementos. A pesquisa foi delimitada na coleta por meio da área de estudo em biblioteconomia e ciência da informação (*Library and Information Science*, em inglês, LIS).

2.1 ORGANIZAÇÃO DO TEXTO

A dissertação que constitui este texto está estruturada em cinco seções. Inicia-se com a introdução que explicita o assunto desta pesquisa, breves conceitos, os objetivos, pergunta central deste estudo e a delimitação da pesquisa. A segunda seção apresenta a fundamentação teórica, com subseções sobre a Inteligência Artificial onde se apresenta o histórico e desenvolvimentos tecnológicos, com fatos ocorridos no Brasil e no mundo. Na subseção Algoritmos e Sociedade explora-se as formas com as quais o algoritmo tem se mostrado presente na sociedade. Na seção de reconhecimento facial é trabalhado o surgimento, o objetivo do RF e como tem sido sua repercussão nas diferentes áreas de uso e pesquisas em andamento.

Na terceira seção, sobre Escolhas Metodológicas, são apresentados os procedimentos de pesquisa para atingir os objetivos selecionados, o que inclui as metodologias aplicadas para a caracterização da pesquisa e a metodologia de categorização.

Na seção quatro expõe-se a análise dos artigos, a apresentação dos resultados, desde a caracterização dos artigos, exposição de gráficos e tabelas para melhor visualização da amostra, seguindo a ordem dos objetivos específicos. Na última subseção encontra-se os comentários da pesquisadora sobre os artigos de cada categoria. Na seção cinco constam as considerações finais do trabalho e as sínteses que foram elaboradas.

2 REFERENCIAL TEÓRICO

Esta seção de revisão de literatura sobre os temas centrais do estudo, se dá pela necessidade de elaborar o aprofundamento sobre a inteligência artificial, o reconhecimento facial, e relação dos algoritmos e a sociedade. Cada tema está divido em capítulos e subcapítulos quando necessário, para assim ter melhor compreensão das categorias estabelecidas

2.1 ALGORITMO E SOCIEDADE

¿Quién quiere que yo quiera lo que creo que quiero?
Dime qué debo cantar
Oh, algoritmo
Sé que lo sabes mejor
Incluso que yo mismo
Por ejemplo, esta canción
¿Qué algoritmo la parió?
Me pregunto si fui yo
¿La elegiste o te eligió?
[…] Are you the fish or the bait?

Jorge Drexler (2022)

Os algoritmos estão no mercado de ações, corrigem e escrevem artigos, podem prever epidemias, compor músicas, nas avaliações de crédito e inúmeras atividades sociais, econômicas e políticas como mencionado na seção anterior.

Cathy O'neil (2017) relata em seu livro *Armas de la destrucción matemática, cómo el Big Data aumenta la desigualdade y amenaza la democracia* que os algoritmos têm um grande potencial para incrementar a desigualdade social, estão desde nossas atividades mais comuns do dia-a-dia como seguir uma receita na cozinha, como nas propagandas designadas a nós de acordo com nossa classe social.

A sociedade da informação para González de Gómez (1999), "poderia ser entendida como aquela em que o regime de informação caracteriza e condiciona todos os outros regimes sociais, econômicos, culturais, das comunidades e do estado". Três anos depois a autora utiliza da expressão "regime de informação" como argumento para questionar quais as "estruturas de informação poderiam sustentar os processos de formação, circulação e institucionalização do poder, em um horizonte democrático".

> Um "regime de informação" constituiria, logo, um conjunto mais ou menos estável de redes socio comunicacionais formais e informais nas quais informações podem ser geradas, organizadas e transferidas de diferentes produtores, através de muitos e diversos meios, canais e organizações, a

> diferentes destinatários ou receptores, sejam estes usuários específicos ou públicos amplos (GONZÁLEZ DE GÓMEZ, 2002, p. 34).

O conceito de “regime de informação”, sintetiza uma situação em que passamos a ser consumidores e produtores de conteúdo que chega até nós em todas as redes como Netflix, Google, Facebook e outras redes de tecnologia, partindo do uso de algoritmos, ou seja, protocolos de informática que monitoram e categorizam a navegação do usuário e filtram o conteúdo que será a ele disponibilizado em suas plataformas digitais (BEZERRA, 2017).

A manipulação dos dados ofertados por nós e sobre nós todos os dias nas redes *“Bummer”*[7] como Lanier (2017) descreve as redes sociais, como algo que nos traz frustrações tem levado a uma mudança de comportamento imperceptível aos olhos dos demais usuários.

Os algoritmos em certa medida, podem facilitar a nossa vida, por nos poupar tempo de busca, pois aprendem a nos enviar o que nos interessa e concordamos, mas não devemos deixar de refletir no quanto somos vigiados por quem nem conhecemos. Podem interferir em nossas tomadas de decisões, principalmente quando trabalham em conjunto com a disseminação de desinformação (BAUMAN, 2014).

> O uso massivo de bots sociais pode influenciar o primeiro tipo de mecanismo de visibilidade por interação com qualquer publicação acessível. Ao interagir de forma automatizada e massificada, os robôs conseguem enganar os sistemas de redes sociais, fazendo-os compreender que pessoas reais estão engajando com o conteúdo em grande volume, o que, consequentemente, aumenta seu alcance (RUEDIGER, 2018, p. 8).

A tecnologia não é algo ruim, contudo, Álvaro Vieira Pinto (2003) dizia: “quanto mais se desenvolve a tecnologia tanto mais frágil a tecnocracia” e “recusou-se a ver na disseminação do uso da máquina e do computador um elemento comprovador da ‘qualidade’ presente na opção vulgarmente defendida pelas elites de então: entrar na ‘era tecnológica’ para superar a desigualdade” (FREITAS, 2006, p. 93).

Algo similar é relatado por Giuliano da Empoli sobre a tecnologia dos algoritmos em *engenheiros do caos*:

> Para conquistar uma maioria, ele não vai convergir para o centro, e sim unir-se aos extremos [...]. Cultivando a cólera de cada um sem se preocupar com a coerência do coletivo, o algoritmo dos engenheiros do caos dilui as antigas barreiras ideológicas e rearticula o conflito político tendo como base uma simples oposição entre “o povo” a “as elites.” (EMPOLI, 2020, p. 21).

---

[7] Outros autores tratam o termo como Boomer, porém Lanier traz como Bummer.

Vivemos nesta enxurrada de informações em qualquer canto do mundo, e censores trabalham para o modo de produção capitalista disseminando informações falsas e nos distraindo.

O progresso tecnológico avança em ritmo acelerado, devido principalmente às pesquisas mundiais diante das necessidades humanas. Um dos maiores avanços tecnológicos nos últimos anos foi a expansão dos algoritmos (FIGLIUZZI, 2018). Os algoritmos pertencem a IA, uma área da ciência e da engenharia com objetivo de: analisar e de interpretar os dados complexos, simular ou reproduzir a inteligência humana em máquina e traz como resultados o diagnóstico, o tratamento e a previsão de resultados (WELCHEN, 2019). Existe uma preocupação com o uso dos dados pelas empresas, principalmente ao uso indevido e da combinação da IA com *big data*, pois nesse caso, pode haver uma quebra da privacidade desses dados coletados sem o consentimento prévio.

Ainda quando se adiciona o conceito de “sociedade positiva” de Han (2019), de que só deve-se ver o que nos agrada e por esse motivo, provavelmente, o facebook negue a introdução de um *emotion* de *dislike*. O valor passa a ser medido apenas pela quantidade e velocidade da troca de informações, sendo que a massa de comunicação também eleva o seu valor econômico, com *like* a comunicação de compartilhamento é muito mais rápida do que com *dislike.*

Para processar a personalização de conteúdo de modo assertivo e estabelecer correlações, os algoritmos acessam um grande volume de dados dos usuários que os envolve em uma comunidade comum e faz a mediação deste processo e da comunicação entre eles.

2.2 INTELIGÊNCIA ARTIFICIAL

> Um aplicativo pode fazer um texto adequado sobre os fundamentos da sociologia e seus três autores fundantes – Marx, Durkheim e Weber –, mas o preguiçoso aluno apreenderá algo ao pedir que a máquina faça seu trabalho? Graças ao aplicativo, até um imbecil pode escrever um romance, mas continuará um imbecil. Há uma diferença entre associar palavras dispersas e dar a isto um formato de um texto ou uma imitação de produção intelectual, porque esta implica a intencionalidade e a subjetividade do autor que ao contribuir com o saber coletivo engrandece a si mesmo (IASI, 2023, p. 5).

O desenvolvimento do estudo sobre IA começou após a Segunda Guerra Mundial e foi publicado no artigo *Computing Machinery and Intelligence,* pelo

matemático inglês Alan Turing. O nome foi sugerido por John McCarthy em 1956, em uma conferência de especialistas (COSSETI, 2018). Alan Turing é reconhecido por ser o criador da máquina utilizada para descriptografar as mensagens cifradas das frotas alemãs e pela tecnologia de cartões perfurados da IBM, utilizada para organizar e catalogar as informações em campos de concentração de judeus no holocausto conduzido pelo regime nazista. Grande parte do desenvolvimento tecnológico nascido em âmbito militar daquele período da história do mundo, foram posteriormente utilizadas nas universidades, setores comerciais e domésticos (BEZERRA *et al.,2019)*.

A IA se refere a programas, logaritmos, sistemas e máquinas que atuam em atividades que normalmente precisariam da inteligência humana e imitam parte do seu comportamento por meio de uso de tecnologias empregadas a aprendizagem de máquina.

Antigamente as empresas de marketing realizavam pesquisas de hábitos de consumo para planejamentos de vendas, hoje utilizam a aprendizagem de máquina (*machine learning)*, que por meio de coleta dos dados inseridos nas plataformas, como Facebook, Google, Amazon, Spotify e outras, constroem um perfil para cada usuário com informações básicas, porém precisas: idade, status de relacionamento, classe econômica, se trabalha, se participa de grupos, entre outros (BEZERRA *et al.,2019)*.

Após a obtenção desses dados, é comum que as empresas recorram a ferramentas analíticas, como a “Insights”, que, embora esteja disponível para empreendedores em várias plataformas, algumas empresas utilizam para filtrar informações de todas as redes sociais com a mesma ferramenta. Com os filtros aplicados, é oportuno catalogar as "bolhas" nas quais cada perfil está inserido e enviar o conteúdo direcionado a esses grupos específicos.

A personalização das mídias sociais é o resultado da interferência dos algoritmos da IA treinados com base nos dados coletados a partir do tempo de uso, compartilhamentos, likes e até conversas. Esse processo é baseado nos modelos de redes neurais denominados *deep learning,* uma subárea de *machine learning,* sendo ela também uma subárea da IA.

Os sofisticados algoritmos de IA “individualizam” as consultas o Google, em que os resultados variam de acordo com o perfil de quem está buscando a informação. No Facebook, algoritmos de IA são usados no gerenciamento de publicações que aparecem no *feed* de notícias de seus usuários. Para processar esta personalização de conteúdo de modo assertivo e estabelecer correlações, os algoritmos acessam um grande volume de dados dos usuários, chamado de *big data*, que os envolve em uma

comunidade comum e faz a mediação deste processo e da comunicação entre eles.

A IA tem sido utilizada para produzir e circular a desinformação de forma automatizada. A era das *deep fakes* é a combinação de desinformação com IA. A principal crítica a esses sistemas inteligentes é a propensão para a formação de "bolhas", que promovem a homogeneização das relações sociais, mantendo as pessoas em grupos fechado, formados por outros que pensam igual. No entanto, o marketing é apenas umas das diversas áreas que utilizam fortemente os algoritmos. A IA tem sido utilizada na disseminação de desinformação para atacar a ciência e na política alavancado por meio da disseminação de ódio e medo:

> Se o algoritmo de redes sociais é programado para oferecer ao usuário qualquer conteúdo capaz de atraí-lo com maior frequência e por mais tempo à plataforma o algoritmo do caos os força a sustentar não importa que posição, razoável ou absurda, realista ou intergaláctica, desde que ela intercepte as aspirações e os medos - principalmente os medos – dos eleitores (EMPOLI, 2020, p. 20).

Não devemos rejeitar a IA e suas outras soluções que fazem uso intensivo de dados somente porque as grandes plataformas (Amazon, Google, Facebook, atual Meta e outros) utilizam dessas tecnologias com fins execráveis, pois isso nos paralisaria neste momento crucial (MOROZOV, 2018). Não se pode esquecer que quem domina a tecnologia mais avançada, domina o mundo.

2.3 RECONHECIMENTO FACIAL

Em 1964 o matemático e cientista da computação, Woodrow Wilson Bledsoe, desenvolveu a tecnologia de reconhecimento facial, inicialmente desenhando manualmente as faces para o estudo das métricas. Com o surgimento de dispositivos móveis e aplicativos pessoais o reconhecimento facial se tornou mais visado nos últimos anos. Seu uso também é visto na indústria do entretenimento como Instagram, Facebook e videogame (MAGNO; BEZERRA, 2020; CONCEIÇÃO et al., 2020).

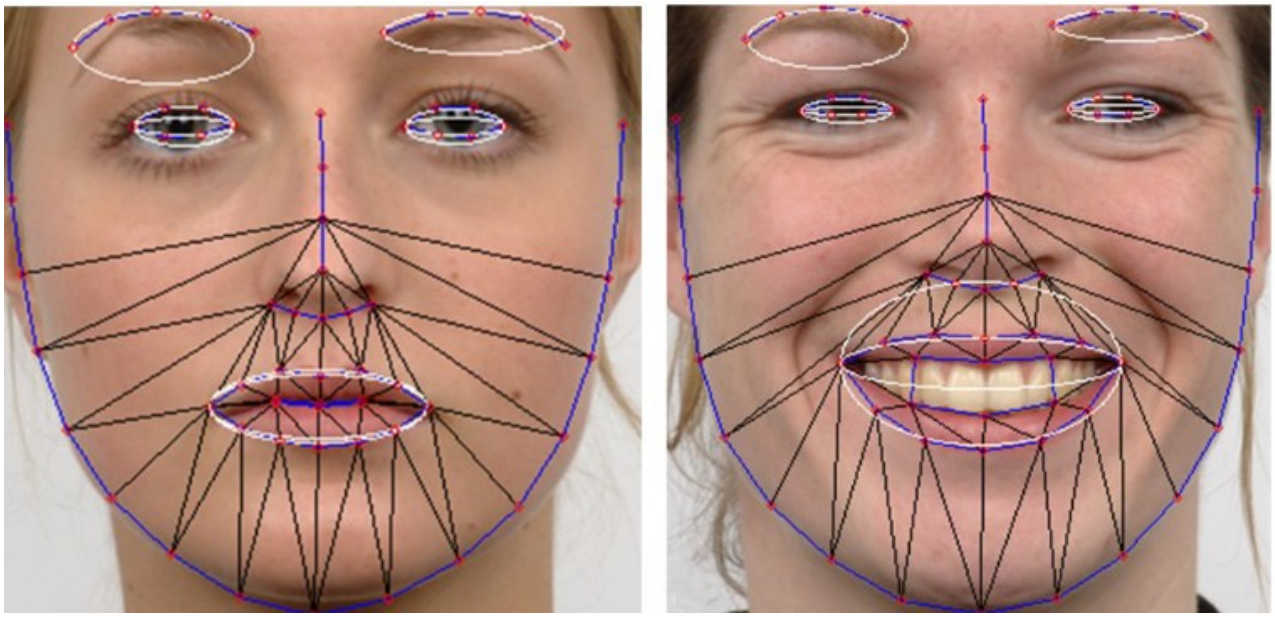
De modo geral, os métodos de reconhecimento facial funcionam comparando as características faciais selecionadas de uma determinada imagem com os rostos existentes num banco de dados. Embora a exatidão do sistema de RF, como tecnologia biométrica[8], seja inferior ao reconhecimento de íris oculares e de impressões digitais, ele é ainda amplamente adotado pela sua simplicidade (ORVALHO, 2019).

[8] Biometria tem origem nas palavras gregas *bios* (vida) e *metrikos* (medida).

O rosto humano apresenta características variáveis em cada pessoa, porém, existem combinações básicas, tornando-se pontos de referência, e essenciais, como os olhos e a distância entre eles, o nariz e o seu comprimento, a bochecha, a boca e o queixo, que podem ser lidos por softwares, por meio de algoritmos gravados e armazenados em bancos de dados, que têm como princípio detectar as formas geométricas da face, montar o quebra-cabeça (KOCH, 2012; BATISTA et al., 2017). A relação entre essas particularidades cria uma geometria espacial que é armazenada em forma de dados, o *template* ou *faceprint*. E quando uma nova imagem é apresentada, o *software* faz a comparação.

A figura abaixo demonstra um dos passos para a coleta completa de pontos nodais do rosto e modificações de acordo com a emoção.

Figura 1 - Definições de elipse inferior e superior da boca.



Fonte: Console et al., 2014.

Na ausência de outras informações, como por exemplo a fala, as expressões faciais podem transmitir emoções, opiniões e pistas sobre os estados cognitivos. Existem vários campos de investigação focados no desenvolvimento de sistemas automáticos para o reconhecimento de emoções faciais, principalmente para auxiliar no desenvolvimento e dignósticos de transtorno do espectro autista. Com a chegada da COVID-19, na China, foi intensificada o acoplamento de sistema de reconhecimento facial em veículos aéreos não tripulados como *drones,* para contribuir no combate à crise sanitária, identificando aglomerações e violação das normas de uso de máscara e

distanciamento social (CONTIN *et al*., 2021).

Pesquisadores como XIE *et al* (2006) demonstram como o reconhecimento facial pode ser utilizado como uma ferramenta de ensino e aprendizagem por meio da leitura labial e melhoria de compreensão do idioma Cantonês.

Outra esfera de possibilidade de utilização é a relatada por pesquisa de Sclaroof *et al* (2005). Eles demonstraram três domínios de reconhecimento da imagem do corpo por meio do reconhecimento facial, para melhorar a sociabilidade e evitar acidentes. São elas: Linguagem de Sinais Americana, sinais manuais como aqueles empregados por diretores de voo nas pistas de aeroportos e interfaces baseadas em gestos para usuários com deficiências graves. No caso dos diretores de voos das pistas de aeroportos, quando o avião está vindo, o algoritmo pode realizar a leitura da imagem da silhueta dos trabalhadores do aeroporto e suas indicações por meio de sinais para onde o piloto deve conduzir o avião, de forma mais precisa.

Wu e Chellappa (2012) criticaram a ineficácia dos algoritmos de reconhecimento facial que fazem o envelhecimento automático e propõe melhorias, em seu estudo, para que eles possam auxiliar em buscas de crianças desaparecidas de forma mais eficaz e em prol da segurança pública. No mesmo sentido em que essa ferramenta pode ser a solução de determinados problemas, ainda há discussões acerca da invasão de privacidade e liberdade das pessoas, e a suspeita do algoritmo possuir viés de quem o alimenta (ZAIDAN, 2019).

Como por exemplo o Projeto de Lei 9.736, de 2018, do deputado Júlio Lopes (PP/RS), que obriga o reconhecimento facial em presídios. O PL 11.140 de 2018, do líder do PSL, Delegado Waldir (GO), vai além, e determina registros não somente aos detidos, mas também a funcionários e até mesmo advogados que ingressem nas unidades de internação (VALENTE, 2019).

As tecnologias de reconhecimento facial baseadas em inteligencia artificial já estão em uso em muitos países, para dar mais precisão e agilidade à identificação de criminosos. O sistema pode, por exemplo cruzar dados sobre criminosos procurados em bases de dados mais amplas como em registros civis ou postagens nas redes sociais, pessoas flagradas por câmeras em cenas de crimes. Esses recursos, chamados no Brasil de “cerca eletrônica”, exigem processar dados em massa, esbarrando em questões éticas e legais a respeito da privacidade dos dados. Mas há também um problema sério de eficiência que reforça preconceitos instituídos (ENTLER, 2021).

O documentário *Coded Bias* (2020), dirigido por Shalini Kantayya, investiga o

viés racista e machista da IA por trás dos algoritmos de RF e aprofunda a análise de como as redes sociais e os algoritmos de *big techs* estão impactando os grupos a margem da sociedade. Na busca do proposto por Joy Buolamwini, uma mulher negra e cientista, que ao realizar pesquisas no *MIT Media Lab*, e posicionar rostos em frente a uma tela com dispositivo de captação de imagem por algoritmos de reconhecimento facial, detectou um problema neste sistema, consistente da falha frequente na análise de rostos, interferindo diretamente nos resultados, atribuindo a falha aos aspectos étnico-raciais. O documentário apresenta os resultados das pesquisas algorítmicas de Cathy O'Neil, que parte da premissa de que as aplicações matemáticas fomentadoras da economia dos dados, eram baseadas em escolhas feitas por seres humanos falíveis, independente das suas intenções.

> Esse problema aumenta dramaticamente quando as pessoas sujeitas a essa tecnologia pertencem a grupos historicamente vulneráveis, como mulheres, pessoas não brancas ou pessoas trans. Assim, a implantação de sistemas de reconhecimento facial acarreta a reprodução técnica do viés de exclusão social e, quando utilizada para fins de vigilância, ameaça o direito à dignidade, ao devido processo e à presunção de inocência, entre outros (VENTURINI; GARAY, 2021).

Muito antes de matemáticos desenvolverem um sistema para o reconhecimento facial, com medições faciais como informações para alimentar sistemas com catálogos de rostos, no século XIX, o médico Cesare Lombroso, argumentava que o comportamento delinquente inato tinha forte componente racial. A partir de milhares de retratos de criminosos e “uma rigorosa análise antropométrica”, defendia que a maior parte de incidencia de crimes em certas regiões da Itália era consequência de uma acentuada presença africana e oriental. Também detalhou características corporais de criminosos em geral que segundo ele, se assemelham aos traços observados no “selvagem” e nas “raças de cor” (LOMBROSO, 1887). Hoje conseguimos fazer a ligação destas declarações com a ideologia da supremacia racial, antes apresentada como “análise e estudo”. Soma-se a isso o fato histórico de que pessoas não brancas já foram sequer consideradas seres humanos.

Como previa Bauman (2014), as amarras se afrouxam à medida que os fragmentos de dados pessoais obtidos para um objetivo podem ser facilmente utilizados para outro fim. Os algoritmos têm um grande potencial para incrementar a desigualdade social (O’NEIL, 2017).

3 ESCOLHAS METODOLÓGICAS

Este estudo se dá pela relevância dos algoritmos no momento político que vivemos no país, destacado desde as eleições presidenciais de 2018 até as recentes denúncias de suspeitas de erros cometidos por algoritmos de reconhecimento facial. Além de vislumbrar o que de fato um algoritmo pode alterar na dinâmica da organização da vida em sociedade, como são catalogadas nossas atividades, características físicas, e o que disso tudo são mitos e respostas palatáveis a problemas sociais que o antecedem. Ou seja, buscar-se-á perceber as rupturas e continuidades de nossa sociedade com o advento dos algoritmos.

Para atender aos objetivos deste estudo, apresenta-se a metodologia de pesquisa bibliográfica; exploratória; qualitativa. A pesquisa exploratória de acordo com Gil (2007, p. 45) “têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses”.

O referencial teórico foi elaborado com base no material já publicado (trabalhos científicos e artigos de jornais e revistas) e constituído por autores que são referência sobre o assunto desta pesquisa. Este tipo de pesquisa é comumente elaborado com o propósito de fornecer fundamentação teórica ao trabalho, bem como a identificação do estágio atual do conhecimento referente ao tema” (GIL, 2007, p. 29). Segundo Severino (2007), o pesquisador, trabalha a partir das contribuições dos autores dos estudos analíticos constantes dos textos, decorrentes de pesquisas anteriores.

As estratégias de buscas foram as palavras-chaves específicas do tema; artigos em que seu conteúdo seja sobre reconhecimento facial e ciência da informação. Incluíram-se artigos indexados em periódicos científicos, para apresentar estudos e conceitos de interferência do reconhecimento facial na sociedade.

Foi realizada a busca de artigos e comunicações nas bases de dados Web of Science; Dimensions Analytics; DOAJ e LENS. Na avaliação da escolha pelos indexadores, as quatro bases foram selecionadas por possuírem a opção de refinamento de busca por campo de estudo/área de concentração: *Library and Information Science* (LIS), pois aumentam as chances de cobertura do assunto da área de estudo e por ser uma pesquisa com este objetivo específico.

A Web of Science é uma plataforma unificadora e multidisciplinar de conteúdo científico e desde de 2011 indexa inclusive livros científicos, foi levado em conta ser abrangente, unindo artigos e comunicações e organizando por campos de estudo. Pertence a Clarivate Analytics, atualmente sua sede é na Inglaterra. Dimensions

Analytics, atualmente é o maior indexador de publicações científicas, também se apresenta como uma plataforma multidisciplinar e pertence ao grupo Digital Science, uma empresa de tecnologia com sede em Londres. A plataforma Lens, é uma base de ciência aberta e multidisciplinar, sem fins lucrativos sediada na Austrália. E por fim a diretório DOAJ, também de acesso aberto, com diversos periódicos com artigos de acesso gratuito e de qualidade. Fundado em 2003 é mantido pela *Lund University Libraries* na Suécia.

Os termos de busca escolhidos para essa coleta: *"facial recognition"; "face recognition",* e para atender ao primeiro objetivo especifico a coleta foi restrita ao campo de estudo *Library and Information Science (LIS)*. Assim se evitam os artigos que se desdobram sobre o reconhecimento facial em áreas de conhecimento distantes, pois a pesquisa teve como foco o reconhecimento facial e ciência da informação.

Em um primeiro momento foram recuperados 93 os artigos nas bases de dados selecionadas por meio dos filtros aplicados.

Tabela 1 – Resultados da coleta e da 1ª triagem de artigos selecionados

Etapas	Base de dados	Total da coleta
Resultado da coleta de artigos	DOAJ	10
	WOS	22
	LENS	12
	DIMENSIONS	49
	Total	93
Resultado após 1ª triagem	DOAJ	8
	WOS	21
	LENS	8
	DIMENSIONS	20
	Total	57

Fonte: Elaborado pela autora (2023).

Com a primeira busca efetivada, foi realizada a retirada das duplicatas, textos que não correspondiam aos idiomas selecionados para esta pesquisa e documentos que não são artigos ou comunicações em eventos.

A partir desta etapa se iniciou o protocolo de leitura dos 57 artigos e uma análise de conteúdo que consiste em: 1) leitura do título; 2) leitura do resumo e palavras-chave.

Os artigos que não possuem a palavra “reconhecimento facial” em um destes dois itens foram retirados, assim como os textos que não possuem ligação com a área de ciência da informação também (BARDIN, 2010; MORAES, 1999).

Os 46 artigos que passaram da triagem anterior seguem no protocolo: 3) Leitura das considerações finais; 4) Leitura dos resultados da pesquisa; 5) Leitura dos procedimentos metodológicos e por fim 6) leitura da introdução (BARDIN, 2010; MORAES, 1999).

Para melhor visualização da relação entre a metodologia e os objetivos específicos, que estão atrelados ao objetivo geral, foi elaborado o Quadro 1:

Quadro 1 – Objetivos específicos e Escolhas metodológicas

O RECONHECIMENTO FACIAL IDENTIFICADO NA LITERATURA CIENTÍFICA EM CIÊNCIA DA INFORMAÇÃO		
Objetivo geral: Verificar a existência de impactos sociais gerados por algoritmos de reconhecimento facial.		
Objetivos Específicos	**Escolhas metodológicas**	**Resultados Esperados**
Identificar as pesquisas sobre reconhecimento facial na CI no Brasil e no âmbito internacional.	Busca restrita em área de estudo *Library and Information Science (LIS)* nas bases Web Of Science; DOAJ; LENS e DIMENSIONS. Palavras-chaves: “*Face recognition”; “facial recognition”.* Idiomas: Inglês, espanhol e português. Período: 2000-2022.	Apresentar uma listagem de artigos e como o reconhecimento facial é compreendido e quais são as tendências dos pesquisadores da Ciência da Informação, inteligência artificial e áreas complementares.
Caracterizar os efeitos sociais identificados na literatura científica derivados das aplicações de reconhecimento facial.	Busca restrita em área de estudo *Library and Information Science (LIS)* nas bases Web Of Science; DOAJ; LENS e DIMENSIONS. Palavras-chaves: “*Face recognition”; “facial recognition”.* Idiomas: Inglês, espanhol e português. Período: 2000-2022.	Identificar nos estudos se, e de que forma os algoritmos de reconhecimento facial afetam de forma positiva ou negativa à sociedade.

Categorizar o reconhecimento facial identificado no levantamento, agrupado por especificidade ou correlação	Com base na leitura dos trabalhos selecionados reconhecer os efeitos causados, agrupá-los por especificidade ou correlação e catalogá-los.	Desenvolver uma relação dos efeitos identificados na ciência. Por meio destes impactos criar categorias.

Fonte: Elaborado pela autora (2023).

3.1 ESCOLHAS METODOLÓGICAS PARA A CATEGORIZAÇÃO

A perspectiva metodológica a qual essa pesquisa se aproxima e um de seus objetivos é categorizar os efeitos identificados nos artigos, com base na análise de descrição de conteúdo que atue como uma forma de hierarquização mental de conceitos sobre a realidade, com vistas a facilitar a organização do conhecimento (ARANALDE, 2009). A análise de conteúdo permite o processo de categorização das informações identificadas nos estudos selecionados (MORAES, 1999). A categorização não é uma etapa obrigatória de toda análise de conteúdo, no entanto para realizar categorização ela é necessária.

Este trabalho utilizou da conceituação de Bardin para categorias:

> Classificar elementos em categorias compõem a investigação do que cada um deles tem em comum com os outros. O que vai permitir seu agrupamento é a parte comum existente entre eles. É possivel contudo, que outros critérios insistam noutros aspectos analogia, talvez modificando consideravelmente a repartição anterior (BARDIN, 2010 p. 146).

Verifica-se o uso da categorização como recurso utilizado na metodologia científica para análise de dados. No entanto, é necessário primeiro compreender e identificar essa abordagem na literatura de metodologia científica antes de aplicá-la. A categorização é um processo que envolve atividade humana e cognitiva, um recurso natural que os seres humanos realizam de forma automática (LIMA,2010).

A categorização é um processo que agrupa pessoas, objetivos e lugares em classes específicas com base em suas semelhanças, ou seja, ela envolve o reconhecimento das similaridades e diferenças, resultando na criação de conhecimento novo por meio do agrupamento de entidades de acordo com as observações de similaridade e diferença (LIMA, 2010; FERRARI, 2011).

Bardin (2010) ainda apresenta uma série de orientações e instruções para ajudar

na construção das categorias. O autor descreve cinco recomendações para categorias de qualidades: a) exclusão mútua; b) homogeneidade; c) pertinência; d) objetividade e fidelidade; e e) produtividade. Essas características essencialmente indicam que, ao elaborar as categorias, é necessário seguir um princípio de organização que deve ser mantido até o final. Os elementos categorizados não devem estar inseridos em mais de um tipo de categoria, pois cada categoria deve representar o conteúdo daquilo que foi analisado, com o objetivo de fortalecer os resultados obtidos (BARDIN,2010).

Com base nesses autores foram criados quadros e gráficos para facilitar a visualização de informações de categorização dos textos encontrados, para posterior criação de categorias acerca de elementos agrupadores de conteúdo.

4 ANÁLISE DA AMOSTRA

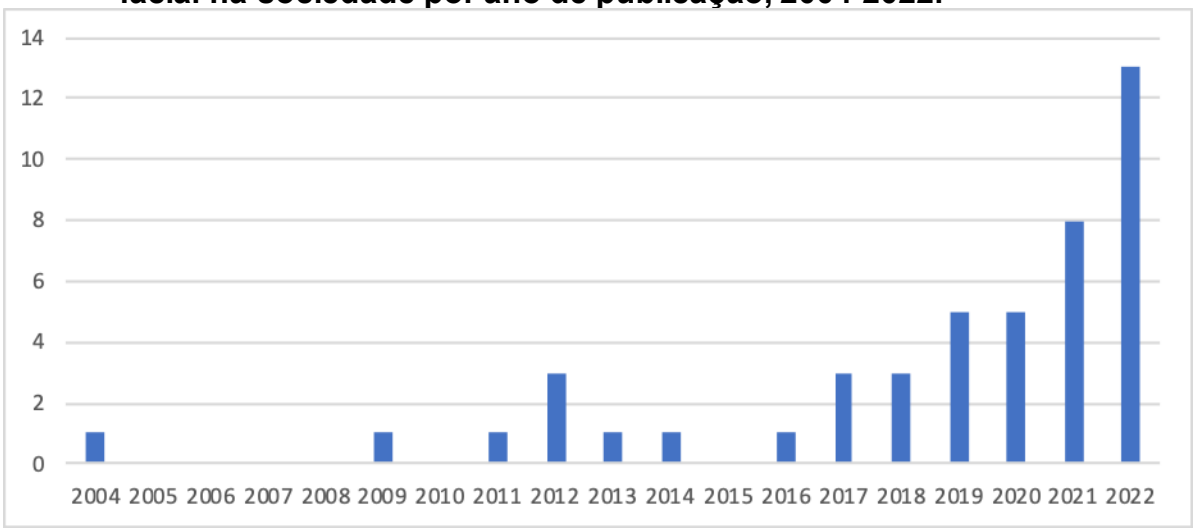
Nesta seção, discorre-se sobre os resultados da pesquisa; em que no primeiro momento é apresentado os efeitos dos algoritmos de reconhecimento facial na sociedade, identificados nos artigos científicos indexados na Web Of Science (WOS); Dimensions, Lens e DOAJ o segundo momento desenvolve sobre o processo de categorização.

A averiguação das pesquisas selecionadas nas variáveis ano, idiomas, autorias, países, agência financiadora/patrocinador do estudo, periódicos científicos são expostas na última subseção.

4.1 CARACTERIZAÇÃO DOS ARTIGOS SELECIONADOS

Após a filtragem pelos protocolos indicados na metodologia, foram selecionados 46 artigos publicados de 2004 a 2022. Foi percebido o crescimento de publicações, disponibilizadas nas bases indexadoras, sobre os efeitos sociais dos algoritmos de reconhecimento social, principalmente, a partir de 2016. Até esse ano as publicações eram esparsas, não sendo encontrado produções em 2005, 2006, 2007, 2008, 2010 e 2015. De 2016 (um artigo encontrado) para frente todos os anos retornaram ao minimo três publicações, e de 2019 (cinco artigos encontrados) em diante o número de publicações foi maior do que a média dos anos anteriores, com cinco em 2020, oito em 2021 e treze em 2022 (conforme Gráfico 1).

Gráfico 1 - Frequência de artigos sobre efeitos dos algoritmos de reconhecimento facial na sociedade por ano de publicação, 2004-2022.



Fonte: Dados organizados pela autora com base em artigos encontrados na Web of Science; Dimensions; Lens; DOAJ em abril de 2023.

Dos artigos resgatados destaca-se que apesar de termos pesquisadores de diferentes países e diversos idiomas (mandarim, grego, espanhol...) a maior parte dos artigos selecionados estão em inglês, apenas 2 em espanhol que aparecem nas bases indexadoras com títulos em inglês. O que pode indicar a concentração de publicações nesses indexadores acerca desse tema no idioma inglês e uma preponderância dos espaços para esse tipo de conhecimento produzido nesse idioma.

A maior parte (36) encontrada foi escrita no formato de artigos, seguido de Proceendings Paper (8), e material editorial (2) , conforme Tabela 2.

Tabela 2 - Frequência de tipos de documentos selecionados na Web of Science; Dimension, DOAJ e LENS entre 2004-2022.

Tipo de documento	Quantidade
Article	35
Proceedings Paper	8
Editorial Material	2
Total	45

Fonte: Dados organizados pela autora com base em artigos encontrados na Web of Science; Dimensions; Lens; DOAJ em abril de 2023.

No que diz respeito à publicação, há uma variedade de espaços e periódicos. Alguns deles contam com duas publicações no "Profesional de la informacion", "APOLLO" e "Journal of Information & Optimization Sciences". Além disso, outros nove artigos foram apresentados em conferências internacionais relacionadas a ciências sociais, humanidades e tecnologia.

Para melhor visualização da amostra foi elaborado o Quadro 1, para uma visão panorâmica dos títulos dos trabalhos e seu ano de sua publicação.

Quadro 2 - Título e ano dos artigos sobre efeitos dos algoritmos de reconhecimento facial na sociedade, 2004-2022.

Nº	ANO	Título	Autor
1	2004	Ethical aspects of facial recognition systems in public places	BREY, Philip
2	2009	Identificación facial biométrica	CALDERA-SERRANO; ZAPICO- ALONSO
3	2011	Roundup	Brown-Syed; Owens
4	2012	Gazela: social networks' digital advisor for teenagers	ISASI- ANDRIEU *et al*.,
5	2012	Mobile augmented reality applications for library services	HAHN, Jim
6	2013	Batch metadata assignment to archival photograph collections using facial recognition software	BANERJEE; ANDERSON
7	2016	Face Detection and Face Recognition in Android Mobile Applications	DOSPINESCU; POPA
8	2017	Facial Recognition in Multimodal Biometrics System for Finger Disabled Applicants	MAZLAN; HARUN; SULIMAN
9	2017	The importance of security for people and collections in libraries	Botez; Repanovici
10	2018	Design and Development of Facial Recognition-based Library Management System (FRLMS)	RAO *et al.*
11	2018	Factor Analysis in Unconstrained Viola-Jones Face Detection: Brightness, Contrast, Focus Measure, Eyewear, Gender, and Occlusion	Jafek *et al.*
12	2018	Recognizability of computer-generated facial approximations in an automated facial recognition context for potential use in unidentified persons data repositories: Optimally and operationally modeled conditions	Parks e Monson
13	2019	Ethical dimensions of quantification	Espeland e Yung
14	2019	IoT Solution for Smart Library Using Facial Recognition	Upala e Wong
15	2019	A Dataset for Comparing Mirrored and Non-Mirrored Male Bust Images for Facial Recognition	Gros e Straub
16	2020	I Don't Want Someone to Watch Me While I'm Working: Gendered Views of Facial Recognition Technology in Workplace Surveillance	STARK; STANHAUS; ANTHONY
17	2020	Dostroajan: Facial Recognition Based System Input Control Agent	AYATA *et al*.
18	2020	Public support for facial recognition via police body-worn cameras: Findings from a list experiment	BROMBERG; CHARBONNEAU; SMITH
19	2020	The ethical questions that haunt facial-recognition research	Van Noorden
20	2021	CNN based Face Recognition System for Patients with Down and William Syndrome	Setyati *et al*.

21	2021	Digital Right Protection Principles under Digitalization	Kirillova *et al.*
22	2021	Library Attendance System using YOLOv5 Faces Recognition	Mardiana, Muhammad e Mulyani
23	2021	Resistance to facial recognition payment in China: The influence of privacy-related factors	LIU; YAN; HU
24	2021	The ethics of inattention: revitalising civil inattention as a privacy-protecting mechanism in public spaces	SHARON; KOOPS
25	2021	Typologies of Mobile Privacy Behavior and Attitude: A Case Study Comparing German and American Library and Information Science Students	Havelka
26	2022	A novel approach for verifying selective user identity attributes online using open banking APIs	Pete *et al.*
27	2022	Cloud-Based System for Identifying Vaccinated Individual	Raj e Tajammul
28	2022	Detecting Hostellers Using Face Recognition	Mary *et al.*
29	2022	Facial recognition systems in policing and racial disparities in arrests	Johnson *et al.*
30	2022	Legal Regulation of Government Applications of Facial Recognition Technology: A Comparison of Two Approaches	Wang e Zhang
31	2022	Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance	Barkane
32	2022	Racial Bias in Customer Service: Evidence from Twitter	Gunarathne *et al.*
33	2022	Representation of Libraries in Artificial Intelligence Regulations and Implications for Ethics and Practice	Bradley
34	2022	Student Attendance using Face Recognition Technology	ASMITHA; SUNITHA
35	2022	Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy	Shore
36	2022	The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities	Eneman *et al.*
37	2022	Watching the watchers: bias and vulnerability in remote proctoring software	Burgess *et al.*

Fonte: Dados organizados pela autora com base em artigos encontrados na Web of Science; Dimensions; Lens; DOAJ em abril de 2023.

4.2 - CARACTERIZAÇÃO DOS ARTIGOS

Nesta seção, foi realizada à caracterização dos 37 artigos selecionados, com o intuito de elucidar os pontos de vista dos pesquisadores/as sobre a utilização do

reconhecimento facial e sua relação com a ciência da informação, que se entende tanto como a coleta quanto o uso de dados e informações e seus impactos. A caracterização é a descrição resumida do artigo de pesquisa relatado, algumas das descrições desta dissertação são mais longas do que outras, isso é devido ao próprio artigo descrito.

Ademais, serão expostas diferentes perspectivas dos autores/as que apontam para a possibilidade de aprimoramentos e reforço da segurança nos algoritmos de reconhecimento facial.

Durante a leitura dos artigos para caracterização nove artigos foram retirados, quatro por não serem relacionados exatamente a área de ciência da informação, dois eram apenas resumos e não o artigo com metodologia e resultados, e outros três artigos eram em revistas pagas e não foram localizados disponíveis em outro local. No total temos 37 artigos caracterizados e devidamente categorizados de acordo com os efeitos e impactos do reconhecimento facial sentidos na sociedade.

Para diferenciar melhor os artigos, se apresenta o título e responsáveis da autoria.

- **Detecting Hostellers Using Face Recognition - Mary *et al.***

O objetivo das tecnologias modernas é reduzir o trabalho humano e substituí-lo por algo mais eficiente e simples de usar. O potencial da inteligência artificial para preencher a lacuna entre as habilidades humanas e das máquinas cresceu muito. Pesquisadores e amadores se concentram em aspectos do campo para produzir resultados excepcionais, principalmente o campo da visão computacional (MARY *et al*., 2022).

Mary *et al*. (2022) sugere que os algoritmos de aprendizado de máquina de reconhecimento facial sejam utilizados para os registros de saída do aluno do campus e sejam mantidos em arquivos CSV[9]. Segundo a pesquisadora atualmente as moradias estudantis, albergues têm recebido um grande número de pessoas de diferentes cidades. E em grande parte esses estudantes saem do campus sem autorização de seus tutores.

O que torna difícil para as universidades identificarem se algum aluno fugir ou sumir do campus. O reconhecimento facial é um projeto viável por ser um método que não precisa de envolvimento humano, quando localiza o estudante envia mensagens

[9] Um arquivo de texto com formato específico para possibilitar o salvamento dos dados em formato de tabela.

aos tutores responsáveis. Segundo a autora um sistema totalmente automatizado e fácil de ser mantido.

O estudo se debruça ainda na utilização do reconhecimento facial para detectar os alunos na sala de aula, e assim controlar de forma automática a frequência. Sendo assim, uma câmera é instalada em cada sala de aula.

> A tecnologia de reconhecimento facial pode ser utilizada para detectar os *hostellers* como uma alternativa eficaz à forma tradicional. Como tudo é automatizado, este sistema não requer qualquer intervenção humana. O reconhecimento facial supera todos os outros sistemas biométricos em termos de desempenho. Este sistema não depende de uma base de dados, pelo que armazenar dados não é uma tarefa difícil. A implementação deste sistema nas universidades pode salvar a reputação da universidade. Pode potencialmente salvar a vida dos estudantes (MARY *et al.,* p.*3,* 2022, tradução nossa).

Para o gerenciamento de entrada e saída dos estudantes da moradia será utilizada as etiquetas RFID, o reconhecimento facial e impressões digitais. O RFID, é um método hoje utilizado inclusive em localização de livros e para leitura de estantes em bibliotecas. Conforme explicam os autores o software de reconhecimento facial é simples de configurar, de instalar e utilizar. Para implementar este sistema, basta câmaras de vigilâncias e um computador para executar o software (MARY *et al*., 2022).

- **A Dataset for Comparing Mirrored and Non-Mirrored Male Bust Images for Facial Recognition – GROS; STRAUB**

Há uma variedade de elementos para melhorias e segurança dos algoritmos de reconhecimento facial. Gros e Straub (2019) explicam que o reconhecimento facial tem sido usado na identificação de clientes de lojas de varejo, na segurança, na triagem de candidatos, e no aprendizado sobre o comportamento humano. Além de simplesmente reconhecer um indivíduo, as imagens faciais podem ser analisadas mais detalhadamente para aprender ou inferir sobre o sujeito. Seja a idade, o gênero, podem sugerir níveis de interesse e até o estado emocional dos indivíduos. Porém esses dados, informações coletadas, sofrem vários problemas relacionados ao estado do sujeito e devido ao alto custo da coleta desses dados para fins de treinamento.

O autor afirma que, as condições de iluminação, oclusão, distorção, desfoque atrapalham o reconhecimento facial e que se tem utilizado uma técnica de espelhamento de imagem em busca de reconhecer os dados ausentes ou ocluídos das

imagens, mas apesar do uso recorrente de espelhamento em aplicativos e outras ferramentar, apenas estudos limitados sobre sua eficácia foram realizados, ou seja se continua com um “benefício limitado”, como resume Gros e Straub (2019).

- **Ethical aspects of facial recognition systems in public places – Brey, Philip**

O pesquisador Brey (2004) aborda outro ponto de vista sobre o reconhecimento facial em seu texto, afirmando que desde os ataques terroristas de 11 de setembro de 2001, governos federais e aeroportos passaram a se interessar por essa tecnologia como instrumento de combate ao terrorismo internacional. O texto escrito em 2004 menciona que o reconhecimento facial estava em estágio experimental em diversos aeroportos na Europa e nos Estados Unidos, como o Aeroporto de Keflavik, na Islândia, Aeroporto Logan de Boston, Aeroporto Internacional de Dallas e Aeroporto Internacional de Palm Beach. Isso deu início à reforma da Lei dos Vistos.

O autor, ao discutir sobre "vigilância inteligente" por meio de vídeo, concentra sua abordagem nas câmeras de reconhecimento facial utilizadas em ambientes públicos. Muitas empresas comercializam essa tecnologia, algumas se especializando no desenvolvimento de softwares e outras na implementação de sistemas mais completos, que incluem tanto o hardware quanto o software. O software é responsável por analisar imagens digitais e reconhecer rostos. Ele pode ser usado para localizar rostos em uma imagem, mas seu uso mais comum é o reconhecimento facial, onde o sistema compara um rosto encontrado em uma imagem com um banco de dados de imagens faciais para verificar uma correspondência.

Conforme Brey (2004) analisa em sua pesquisa, para que essa comparação ocorra, o sistema analisa até oitenta pontos faciais ao redor do nariz, bochechas e olhos em uma única imagem. Isso pode ser feito por meio de uma técnica matemática chamada Análise de Características Locais (Local Feature Analysis- LFA). A LFA é baseada na ideia de que uma imagem facial é composta por diversos elementos de construção do rosto, que variam em cada pessoa. Esses elementos são identificados por algoritmos e, em seguida, codificados em uma fórmula chamada "faceprint" (impressão facial). O faceprint apresenta várias vantagens em relação a imagens faciais mais simples, como ser resistente a mudanças de iluminação, tonalidades de pele, penteados e até mesmo a presença de óculos, desde que os olhos estejam completamente visíveis.

O uso de câmeras de vigilância com reconhecimento facial, conhecido como

"Smart CCTV", é limitado a algumas áreas públicas ao redor do mundo. Em 2001, Londres (Iglaterra), Birmingham (Inglaterra) e Tampa (EUA) foram as primeiras cidades a adotar esse sistema. Essas câmeras são utilizadas para vigilância rotineira e identificação de criminosos procurados. O sistema em Tampa gerou desconforto, mas acabou sendo aprovado pelo conselho municipal e instalado em 2001. Ele utiliza um banco de dados de criminosos procurados e pessoas desaparecidas para realizar a identificação. Algumas pessoas expressaram preocupação com a privacidade, e protestos ocorreram, mas o contrato com a empresa desenvolvedora foi mantido (BREY, 2004).

O debate em torno da tecnologia de reconhecimento facial, especialmente em relação à privacidade versus segurança, tem gerado muita discussão. O sistema Tampa Smart CCTV, em particular, tem sido alvo de controvérsias. Os participantes desse debate incluem defensores e oponentes da tecnologia, com ênfase especial nos participantes baseados em Tampa. Os defensores argumentam que a tecnologia tem benefícios significativos para a segurança, enquanto os oponentes enfatizam a ameaça à privacidade. Alguns oponentes também levantam preocupações sobre a liberdade individual. A discussão em Tampa e na mídia em geral gira em torno desses aspectos. Os defensores destacam os benefícios da tecnologia na redução da criminalidade, na captura de criminosos e na localização de pessoas desaparecidas. Já os oponentes questionam a eficácia da tecnologia na prevenção do crime e levantam preocupações sobre a invasão de privacidade e possíveis erros de identificação. O debate também aborda questões legais, como a violação de direitos constitucionais.

Alguns defensores minimizam a preocupação com a privacidade, argumentando que a tecnologia não é diferente de outras formas de vigilância já existentes. Por outro lado, existem defensores que reconhecem as preocupações com a privacidade e propõem a implementação de salvaguardas adequadas. O debate sobre privacidade versus segurança continua gerando opiniões divergentes, com diferentes visões sobre o equilíbrio entre esses dois aspectos.

Por fim, o autor conclui que a implementação da vigilância inteligente por meio do CCTV, especialmente com o uso de reconhecimento facial, levanta preocupações significativas em relação à privacidade. As objeções incluem a violação da integridade contextual, onde as pessoas são expostas a uma vigilância em grande escala ao frequentar locais públicos, e a criação de equivalentes digitais das partes do corpo, o que pode levar ao acesso não autorizado e ao abuso das informações. Essas preocupações fundamentais são a base das objeções éticas e legais à tecnologia de

reconhecimento facial, gerando debates sobre sua regulamentação e uso responsável (Brey, 2004).

- **Student Attendance using Face Recognition Technology – ASMITHA; SUNITHA**

A pesquisa de Asmitha e Sunitha (2022) nos traz uma preocupação parecida com outros pesquisadores desta triagem (MARY *et al.*, 2022), a frequência dos estudantes no processo educacional e como ela afeta as taxas de graduação. Apresentam uma evolução dos sistemas de registro de frequência, que passaram de métodos manuais para abordagens intermediárias ou automatizadas, utilizando diversas tecnologias, como RFID, redes sociais, código de barras, impressões digitais e reconhecimento facial.

O reconhecimento facial é destacado neste artigo como uma tecnologia promissora para o registro de frequência dos estudantes em ambientes universitários. Ele utiliza câmeras e instrumentos para capturar expressões faciais humanas e utiliza uma base de dados de rostos dos alunos para identificação. Asmitha e Sunitha (2022) descrevem a metodologia proposta para implementar o sistema de participação dos alunos por meio do reconhecimento facial, que envolve etapas como captura de características faciais, aprendizado por meio de algoritmos eficientes e produtivos, e utilização de câmeras para reconhecimento e comparação com a base de dados de rostos.

Os impactos do reconhecimento facial e coleta de informações são diversos. Por um lado, a automação do registro de frequência pode facilitar e agilizar o processo, reduzindo a carga de trabalho dos professores e fornecendo dados mais precisos. Além disso, a utilização de tecnologias avançadas, como aprendizado de máquina e visão computacional, permite melhorias na identificação e previsão da presença dos estudantes.

A implementação bem-sucedida desse sistema de registro de presença utilizando reconhecimento facial traz várias vantagens. Primeiramente, reduz a dependência de métodos manuais de registro de frequência, como papéis e chamadas em sala de aula, o que economiza tempo e esforço dos professores. Além disso, a precisão do sistema de reconhecimento facial aumenta a confiabilidade dos dados de frequência, eliminando a possibilidade de fraude na presença dos alunos.

No entanto, após essa aplicação Asmitha e Sunitha (2022) possuem

perspectivas para aprimorar esse sistema. Uma delas é melhorar a precisão do algoritmo de reconhecimento facial, aperfeiçoando o treinamento do modelo e incorporando técnicas avançadas de aprendizado de máquina. Além disso, o sistema pode ser estendido para além do registro de presença, permitindo o monitoramento contínuo da participação dos alunos durante as aulas, o que pode ser útil para avaliar o envolvimento dos alunos e identificar possíveis áreas de melhoria no processo educacional.

E finalizam com outra possível perspectiva, a de explorar a integração desse sistema com outras tecnologias, como análise de sentimentos por meio do reconhecimento facial, para obter informações adicionais sobre o estado emocional dos alunos durante as aulas. De acordo com a pesquisa isso poderia fornecer ideias valiosas sobre o impacto do ambiente de aprendizado nas emoções dos alunos e ajudar os educadores a adaptarem suas abordagens de ensino (ASMITHA; SUNITHA, 2022).

- **Gazela: social networks' digital advisor for teenagers - ISASI- ANDRIEU *et al*.,**

Na pesquisa de Isasi-Andrieu *et al*. (2012) a preocupação aparece referente aos adolescentes e a crescente integração das novas tecnologias em nosso cotidiano. Eles observaram que, à medida que o acesso a serviços online se torna mais fácil, as redes sociais se popularizaram como meios de comunicação e compartilhamento de informações. No entanto, o problema frequentemente observado é a violação de direitos e leis relacionados ao conteúdo compartilhado, como a postagem de fotos de amigos sem obter permissão prévia. Além disso, os jovens usam a internet para compartilhar informações e estabelecer relacionamentos entre si, sem perceber que aspectos de sua intimidade e privacidade podem ser violados ao navegar nessas plataformas sociais. Essas informações podem ser usadas por terceiros sem consentimento e, em algumas ocasiões, como meio de chantagem, coerção ou agressão física ou moral. As redes sociais se tornaram um novo espaço para o *bullying* escolar.

Em 2012, os autores desenvolveram o projeto Gazela para abordar o problema da privacidade nas redes sociais. O projeto envolve uma empresa de tecnologia, um escritório de advocacia, um centro de formação e um centro tecnológico. O Gazela oferece conscientização, educação, proteção e orientação para adolescentes que compartilham informações nas redes sociais. A plataforma inclui serviços de vigilância,

proteção e aconselhamento jurídico para promover o uso responsável das redes sociais. Os serviços de vigilância têm como objetivo coletar informações publicadas pelos usuários, verificando se estão dentro do quadro legal em termos de conteúdo e permissões de publicação. Os serviços de proteção detectam e alertam se algo ofensivo foi publicado, notificando o infrator. Já os serviços de aconselhamento jurídico oferecem informações básicas sobre como lidar com situações específicas que podem ocorrer nas redes sociais, como assédio, chantagem ou *cyberbullying*.

A sensibilização busca promover boas práticas no uso das redes sociais, como solicitar permissão para publicar imagens de outras pessoas, respeitar a privacidade de outros usuários e evitar o envio de informações sensíveis. Além disso, é necessário educar os usuários sobre as implicações legais de suas ações na Internet e fornecer informações sobre como se proteger de possíveis ameaças.

A plataforma Gazela conta com serviços centralizados em um servidor, que realizam tarefas mais complexas que não requerem a intervenção direta do usuário. Esses serviços incluem o *miAbogado*, que fornece orientação sobre procedimentos a serem seguidos em determinadas situações nas redes sociais, e o *miInspector*, responsável por analisar os conteúdos publicados na Internet, tanto as informações escritas quanto as imagens, utilizando análise semântica e biométrica.

A análise facial identifica pessoas em imagens com base no reconhecimento de padrões biométricos, enquanto a análise semântica busca conteúdos ofensivos ou protegidos por direitos autorais. O *miGuardaespaldas* é responsável por estabelecer a interação com o usuário, configurando o Gazela para supervisionar adequadamente a navegação e enviar notificações e recomendações legais. A base de dados de usuários armazena todas as informações necessárias para o funcionamento dos módulos do Gazela.

Inicialmente, o Gazela se concentra no Facebook, pois em 2012 de acordo com os autores era a rede social com o maior número de usuários e onde existe uma grande quantidade de informações compartilhadas, especialmente fotografias. A plataforma é capaz de autenticar automaticamente o acesso às contas do Facebook dos usuários registrados, analisar as publicações em busca de infrações e dados protegidos, identificar pessoas em fotografias e se comunicar com o *miGuardaespaldas* e o *miAbogado* (ISASI-ANDRIEU et al., 2012).

O reconhecimento facial é uma forma amplamente difundida de reconhecimento biométrico, sendo pouco intrusiva e bem aceita pelos usuários. Em um estudo comparativo entre 6 modalidades biométricas, o reconhecimento facial obteve a melhor

pontuação. No entanto, os sistemas de reconhecimento facial ainda não são totalmente robustos a mudanças de iluminação, pose, expressão ou obstruções parciais do rosto.

Para melhorar a precisão do reconhecimento, diferentes técnicas foram desenvolvidas, como *SVM, boosting, HMM* e redes neurais. No entanto, o sistema Gazela adota uma abordagem diferente, concentrando-se na melhoria da qualidade da imagem antes de reconhecer. São aplicados algoritmos de processamento de imagem para corrigir a iluminação, tornando o reconhecimento facial mais resistente a brilhos e reflexos. Para lidar com poses diferentes, o sistema utiliza o enrolamento múltiplo, capturando perfis esquerdo, direito e frontal para melhorar a taxa de reconhecimento correto.

Outro ponto importante abordado pelos autores é que as imagens esperadas são de grupos de pessoas em situações variadas e ambientes não controlados. Isso requer treinamento contínuo, pois as características das pessoas mudam ao longo do tempo. Isso significa que o perfil biométrico de cada usuário precisa aprender as novas características de cada pessoa registrada no sistema. Gazela é um sistema de conscientização e orientação sobre o uso adequado das redes sociais ao publicar informações e fotografias, especialmente voltado para os jovens. Ele possui módulos capazes de identificar pessoas por meio de tecnologias de reconhecimento facial e analisar textos para determinar se estão sendo publicadas informações pessoais confidenciais ou se contêm expressões ofensivas que podem ser denunciadas legalmente.

No que diz respeito à análise de reconhecimento facial, Gazela permite a identificação de pessoas em fotografias previamente registradas (sistema de comparação de imagem). O trabalho continua em todo o processo para superar deficiências na detecção de poses diferentes e em condições de iluminação variadas.

Isasi-Andrieu et al.(2012) nos informam que, em 2012 estava em andamento o aprimoramento dos sistemas de reconhecimento facial, otimizando algoritmos e filtros de melhoria de imagem, buscando baixas taxas de erro em diferentes condições ambientais e integrando Gazela ao Tuenti e ao Twitter (ISASI-ANDRIEU *et al*., 2012).

- **Public support for facial recognition via police body-worn cameras: Findings from a list experiment - BROMBERG; CHARBONNEAU; SMITH**

Bromberg, Charbonneau e Smith (2020) trazem em sua pesquisa uma outra perspectiva sobre as câmeras de reconhecimento facial. As câmeras corporais (BWC:

Body-Worn Cameras) são uma tecnologia relativamente nova de câmeras acopladas aos uniformes ou capacetes de policiais ou autoridades militares. Grande parte dessa atenção foi desencadeada pela falta de evidências visuais no caso do tiroteio de Michael Brown em Ferguson, Missouri (EUA) em agosto de 2014.

Os autores apontam que a tecnologia de uso de câmeras corporais (BWC) na aplicação da lei recebeu pouca atenção da comunidade acadêmica, apesar de ter sido amplamente discutida na mídia e no contexto policial. Durante os incidentes em Ferguson (MO/EUA), não havia artigos revisados por pares que comprovassem os resultados do uso da força pelas BWCs. Embora houvesse relatórios, resumos e promessas, apenas em 2016, cerca de 47% das agências policiais nos Estados Unidos haviam adotado essas câmeras.

O reconhecimento facial converge com câmeras de tráfego e pedestres, vigilância aérea e câmeras corporais (BWC). A maioria das pesquisas sobre BWC está na criminologia e na gestão policial, analisando os efeitos na aplicação da lei, e nas revisões jurídicas para possíveis implicações legais. Poucos estudos em Administração Pública abordam especificamente a implementação das BWCs, exceto pela crítica foucaultiana de Adams e Mastracci (2017). Críticas semelhantes às BWCs e ao reconhecimento facial são encontradas em revisões jurídicas, levantando questões importantes sobre a vigilância generalizada resultante do rastreamento de terroristas. Neste estudo, os autores possuem uma perspectiva teórica e metodológica visando o futuro. Embora afirmem que o conhecimento é limitado sobre o reconhecimento facial no campo da justiça criminal, acabam por complementar com a literatura de Administração Pública sobre a aceitação de tecnologia (BROMBERG; CHARBONNEAU; SMITH, 2020).

O RF e a coleta de informações desempenham um papel importante no contexto das políticas públicas. A tecnologia de reconhecimento facial envolve vigilância por vídeo e análise automatizada de imagens em um banco de dados. As câmeras capturam imagens de pessoas, que são processadas por software para fazer correspondências com fotos já existentes. Essas fotos são obtidas a partir de um banco de dados que inclui serviços de análise facial fornecidos pelo FBI. Fotos do Departamento de Veículos Automotores (DMV) são comumente utilizadas, e em alguns estados, fotos de carteiras de motorista são compartilhadas com o FBI. Além disso, o banco de dados do FBI também inclui fotos de candidatos a visto, fotos de aplicação de passaportes de cidadãos americanos e fotos do "Centro de Triagem de Terroristas" e outras instituições.

A tecnologia de reconhecimento facial tem sido amplamente adotada por departamentos de polícia em várias cidades dos EUA. No entanto, questões de privacidade e constitucionalidade relacionadas ao uso de câmeras corporais com reconhecimento facial ainda não foram completamente abordadas pelos tribunais. O uso dessas câmeras apresenta desafios legais complexos em relação à privacidade e à Quarta Emenda da Constituição dos Estados Unidos, que é parte da Declaração de Direitos Fundamentais, é a que proíbe busca e apreensões não razoáveis e estabelece que essas ações precisam de um mandado judicial, baseado em causa provável e apoiado por juramento do requerente, e, precisa descrever o local sujeito à busca e as pessoas ou coisas a serem apreendidas.

O uso de tecnologia de vigilância por vídeo no policiamento e monitoramento varia de acordo com o propósito da atividade policial. A vigilância por vídeo pode ser empregada tanto para fins de inteligência, como no combate ao terrorismo, quanto para a aplicação da lei em investigações criminais. No entanto, mesmo quando o objetivo é a segurança pública, a instalação de câmeras nas ruas de uma cidade pode ser percebida como vigilância pelos cidadãos, mesmo que não seja essa a intenção (BROMBERG; CHARBONNEAU; SMITH, 2020).

O uso de câmeras corporais pela polícia, combinadas com a tecnologia de reconhecimento facial, tem o potencial de expandir ainda mais o alcance do reconhecimento facial. Fabricantes de câmeras corporais estão desenvolvendo tecnologias que permitem o armazenamento de imagens capturadas para uso futuro, o que levanta preocupações de organizações de defesa das liberdades civis. Já existem bancos de dados de reconhecimento facial para uso policial em várias cidades dos EUA, como Fresno, Califórnia, e o governo do estado de Michigan está investindo em melhorias para o banco de imagens faciais gerenciado pelo estado.

Essas questões destacam a rápida evolução da tecnologia em relação aos desafios legais e éticos associados ao reconhecimento facial e à coleta de informações por meio de câmeras. É crucial considerar as preocupações relacionadas à privacidade, aos direitos constitucionais e ao uso apropriado dessas tecnologias no contexto da aplicação da lei.

Bromberg, Charbonneau e Smith (2020) indicam como resultados de sua pesquisa que: há apoio público para o uso do reconhecimento facial em situações específicas, como identificação de suspeito de roubo no ambiente de trabalho e segurança em aeroportos. No entanto, a aceitabilidade varia de acordo com a finalidade e contexto de uso.

No geral, o estudo buscou fornecer informações sobre o apoio do público em relação ao uso do reconhecimento facial por meio de câmeras corporais. Ao considerar as normas sociais, preocupações com privacidade e avanços tecnológicos, o objetivo dos pesquisadores é que estes resultados de 2020 ajudem a moldar futuras políticas de vigilância e privacidade relacionadas ao uso dessas tecnologias.

- **The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities - Eneman *et al.***

O estudo de Eneman *et al.* (2022) discute o surgimento de tecnologias emergentes, como inteligência artificial (IA) e aprendizado de máquina, que estão criando capacidades de vigilância sem precedentes. Isso resulta em uma mudança paradigmática na "vigilância algorítmica". As tecnologias de vigilância atualmente são mais poderosas, generalizadas, automatizadas e em grande escala na coleta, análise, armazenamento e compartilhamento de dados. Isso leva a um monitoramento em tempo real do paradeiro dos cidadãos, tornando a vigilância onipresente.

O reconhecimento facial é uma das últimas inovações na vigilância e está sendo rapidamente adotado pelas autoridades policiais em todo o mundo. Embora seja justificado como uma forma de aumentar a segurança pública, o reconhecimento facial também levanta preocupações sobre riscos e ameaças aos valores democráticos e à privacidade das pessoas (ENEMAN; LJUNGBERG; RAVIOLA; ROLANDSSON, 2022).

A Clearview AI atraiu atenção por coletar imagens faciais da internet e construir um banco de dados biométricos, vendendo acesso a agências policiais e empresas de segurança. O estudo examinou documentos públicos das autoridades envolvidas, como a Autoridade Sueca de Proteção à Privacidade (IMY), a Polícia Sueca e o Tribunal Administrativo de Estocolmo. Os documentos foram analisados usando a análise temática para identificar padrões e temas relacionados à forma como as autoridades negociaram e raciocinaram sobre o uso da tecnologia de reconhecimento facial.

O diálogo institucional analisado revelou três tensões principais relacionadas aos trade-offs entre segurança e privacidade: (1) eficácia versus privacidade, considerando a sensibilidade da tecnologia de reconhecimento facial; (2) responsabilidade organizacional versus discrição profissional individual; e (3) tecnologia interna versus tecnologia externa (ENEMAN *et al.*, 2022).

A controvérsia em torno da legitimidade do uso da tecnologia de reconhecimento facial, como a Clearview AI, foi evidenciada nesse diálogo institucional. As autoridades envolvidas apresentaram diferentes perspectivas e justificativas para o uso da

tecnologia. Por um lado, a polícia destacou a capacidade de identificar vítimas desconhecidas e a eficiência na identificação e persecução de criminosos em casos complexos de abuso sexual infantil e criminalidade organizada. Por outro lado, a prática da Clearview de coletar dados da Internet levantou preocupações significativas em relação à privacidade das pessoas.

O caso analisado por Eneman *et al.* (2022) concluiu que tanto o IMY quanto o Tribunal Administrativo rejeitaram a justificativa da Polícia e consideraram ilegítimo o uso da tecnologia. Reconheceu-se a complexidade dos trade-offs entre segurança e privacidade, mas destacou-se a necessidade de identificar e institucionalizar aplicações tecnológicas que ofereçam um potencial legítimo. A complexidade institucional das assembleias de vigilância, envolvendo atores estatais e privados, foi destacada, assim como a importância de considerar as normas e lógicas que orientam essas infraestruturas digitais.

Em resumo, o estudo analisou o diálogo institucional entre a polícia sueca, o IMY e o Tribunal Administrativo sobre o uso da tecnologia de reconhecimento facial Clearview AI. Revelou as tensões entre segurança e privacidade e destacou a necessidade de uma abordagem mais cuidadosa e bem articulada no uso dessas tecnologias, levando em consideração as preocupações legítimas de privacidade e os trade-offs envolvidos (ENEMAN *et al.*, 2022).

- **Resistance to facial recognition payment in China: The influence of privacy-related factors - LIU; YAN; HU**

Liu, Yan e Hu (2021) discutem reconhecimento facial como uma tecnologia capaz de detectar e medir características faciais de forma precisa, para pagamentos por dispositivos móveis. Falam sobre a coleta e análise das informações faciais dos usuários que permitem comparar rostos com um banco de dados, mas também levanta dúvidas sobre a proteção de informações pessoais e invasão de privacidade.

Na China, houve um rápido desenvolvimento nas aplicações de reconhecimento facial, especialmente em pagamentos por dispositivos móveis. No entanto, apesar da disposição dos chineses em abrir mão de certa privacidade em troca de benefícios, há casos de resistência ao uso do reconhecimento facial devido a preocupações com a privacidade. Alguns cidadãos chineses estão preocupados com a coleta ilegal e venda de dados faciais, e há uma lacuna de pesquisa em relação aos fatores relacionados à privacidade que influenciam a resistência ao reconhecimento facial em pagamentos.

Existem também políticas e regulamentações relacionadas à privacidade e ao reconhecimento facial na China, e as principais plataformas de pagamento emitiram políticas de privacidade e acordos de serviço para garantir a proteção da privacidade dos usuários. O objetivo do texto apresentado pelos autores era de preencher essa lacuna e examinar o impacto das considerações de privacidade dos usuários chineses na resistência ao reconhecimento facial em pagamentos (LIU; YAN; HU, 2021).

Nos Estados Unidos, a falta de uma legislação abrangente sobre o uso dessa tecnologia levanta preocupações sobre a proteção da privacidade. Na União Europeia, o Regulamento Geral de Proteção de Dados (GDPR) restringe severamente o uso de dados de reconhecimento facial. Na China, o desenvolvimento do reconhecimento facial para pagamentos por dispositivos móveis tem sido liderado por empresas como Suning, JD.com, Alipay e WeChat (LIU; YAN; HU, 2021).

O país tem adotado uma abordagem prática para a legislação, com leis como a Lei de Segurança Cibernética e o Código Civil estabelecendo diretrizes para a coleta e proteção de informações pessoais. Além disso, foram publicadas normas nacionais relacionadas à tecnologia de reconhecimento facial. As empresas de pagamento também emitiram políticas de privacidade e acordos de serviço para proteger as informações faciais dos usuários. No entanto, há poucos estudos sobre o impacto dessas políticas na percepção de privacidade dos usuários em relação ao reconhecimento facial para pagamentos móveis.

Os autores afirmam que em estudos anteriores sobre o assunto, o reconhecimento facial permite que os usuários realizem pagamentos de forma conveniente, sem a necessidade de usar seus smartphones. Para efetuar o pagamento, o usuário precisa apenas ficar em frente à câmera em um terminal de autoatendimento e realizar gestos dentro de um quadro na tela para confirmar que é uma pessoa real. Um processo de identificação é realizado para comparar a imagem capturada com as informações armazenadas no banco de dados. O pagamento é concluído quando há uma correspondência bem-sucedida. Os estudos também mencionam que a aceitação do pagamento por reconhecimento facial está sujeita a fatores como usabilidade, segurança e disponibilidade.

Liu, Yan e Hu (2021) também observam que existem preocupações com relação à adoção de pagamentos biométricos, incluindo questões como a detecção de falsificação e autenticidade, preocupações com privacidade em relação aos dados biométricos pessoais e a confiança na segurança das infraestruturas utilizadas, como dispositivos de captura de faces especializados. Além disso, é destacado que a

privacidade é um fator importante a ser considerado, mas que há poucos estudos que abordam especificamente os aspectos relacionados à privacidade nesse contexto.

No contexto chinês, foram realizados estudos para verificar os fatores que afetam a intenção de uso dos pagamentos por reconhecimento facial. Alguns fatores identificados foram a percepção de segurança, imagem social, visibilidade e julgamentos esperados, que impactam diretamente a intenção de uso. Além disso, a utilidade percebida e a facilidade de uso foram identificadas como componentes-chave que afetam a intenção de uso desse sistema de pagamento. Por outro lado, o risco percebido teve uma influência negativa na aceitação desses pagamentos por reconhecimento facial.

Em relação às questões de privacidade, há leis, especificações e políticas de privacidade na China que abordam o uso do reconhecimento facial em pagamentos. Essas leis e especificações estabelecem definições de informações pessoais, princípios de processamento de informações pessoais, acesso e correção de informações, medidas de segurança para proteção de informações pessoais, entre outros aspectos relacionados à proteção de dados.

O artigo ainda apresenta o conceito de "privacy calculus" (cálculo de privacidade) e sua aplicação no contexto da coleta de informações e reconhecimento facial. O "privacy calculus" refere-se à análise individual de se os benefícios de divulgar informações pessoais superam os riscos associados a essa divulgação. Ele é utilizado para explicar a decisão individual de compartilhar dados pessoais, levando em consideração os custos e benefícios envolvidos (LIU; YAN; HU, 2021).

Além disso, o texto destaca que o "privacy calculus" tem sido amplamente utilizado em diversos contextos, como publicidade direcionada, sites comerciais, aplicativos móveis, dispositivos de saúde (como smart watch) e tecnologia da Internet das Coisas (IoT). Recentemente, sua aplicação também se estendeu ao campo das tecnologias financeiras móveis, como plataformas de pagamento e serviços bancários por meio de dispositivos móveis. No contexto específico do reconhecimento facial, o texto destaca a sensibilidade dos dados biométricos pessoais e a ansiedade gerada pela possibilidade de uso indevido e invasão de privacidade. Nesse sentido, as preocupações com a privacidade se tornam mais proeminentes, e os indivíduos tendem a ponderar os riscos e benefícios da divulgação de informações antes de tomar uma decisão (LIU; YAN; HU, 2021).

O texto também discute a resistência à inovação no contexto do reconhecimento facial, destacando que os estudos anteriores têm focado principalmente na disposição

dos usuários em adotar produtos ou serviços inovadores, negligenciando a resistência à adoção após a ponderação da privacidade. O texto destaca a importância de considerar os fatores relacionados à privacidade de maneira abrangente para entender os mecanismos psicológicos dos usuários. Nesse sentido, são considerados fatores relacionados às características do reconhecimento facial, como benefícios percebidos e eficácia percebida das políticas de privacidade, bem como percepções de privacidade dos usuários, incluindo preocupações com a privacidade, risco percebido e controle da privacidade.

Finalmente, o texto propõe a combinação da teoria da resistência à inovação com o "privacy calculus" como um novo modelo de pesquisa para entender a relutância dos usuários em usar o reconhecimento facial, considerando a privacidade.

A estrutura teórica proposta no estudo de Liu, Yan e Hu (2021), analisa justamente os fatores que influenciam a resistência dos usuários em relação ao uso de reconhecimento facial para pagamentos. Esses fatores incluem a eficácia percebida da política de privacidade, o risco percebido à privacidade, as preocupações com a privacidade, o controle de privacidade e os benefícios percebidos. A eficácia percebida da política de privacidade refere-se à crença dos consumidores de que a política de privacidade de uma empresa reflete práticas precisas e confiáveis. A existência de uma política de privacidade eficaz pode reduzir as preocupações com privacidade e aumentar os benefícios percebidos pelos usuários.

O controle de privacidade está relacionado à crença do usuário em sua capacidade de controlar a divulgação de informações pessoais. Maior controle de privacidade leva a menos preocupações com privacidade e resistência ao uso do reconhecimento facial para pagamentos. O risco percebido à privacidade refere-se à expectativa de potenciais consequências negativas ao divulgar informações pessoais. Um maior risco percebido à privacidade está relacionado a mais preocupações com privacidade e resistência ao uso do reconhecimento facial para pagamentos.

O estudo mostrou que a eficácia percebida da política de privacidade, o risco percebido à privacidade, as preocupações com a privacidade e os benefícios percebidos são fatores significativos que influenciam a resistência dos usuários ao uso do reconhecimento facial para pagamentos. No entanto, o controle de privacidade não teve influência significativa nessa resistência.

Por fim, o estudo dos autores ressalta a importância de políticas de privacidade eficazes e do controle de divulgação de informações pessoais para reduzir as preocupações e a resistência dos usuários em relação ao uso do reconhecimento facial

para pagamentos (LIU; YAN; HU, 2021).

- **Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance - Barkane**

Barkane (2022) discute a proposta de um regulamento chamado "AI Act", elaborado pela Comissão Europeia, que estabelece regras sobre inteligência artificial (IA) na União Europeia. O objetivo desse regulamento seria lidar com os riscos dos sistemas de IA para os direitos fundamentais. O texto destaca a preocupação com os sistemas de vigilância biométrica, como o reconhecimento facial, que podem afetar negativamente direitos importantes, como privacidade, liberdade de expressão e dignidade humana. O "AI Act" introduz novas regras para o uso desses sistemas, classificando-os com base nos riscos, proibindo certas práticas e estabelecendo requisitos legais. No entanto, o regulamento tem sido amplamente discutido e criticado por acadêmicos, sociedade civil e órgãos de proteção de dados.

O texto questiona se essa forma de regulamento "AI Act" realmente irá abordar os riscos para os direitos fundamentais causados pelo uso de sistemas de vigilância biométrica de IA e destaca os desafios e oportunidades para garantir a proteção adequada desses direitos. O regulamento busca conciliar o desenvolvimento e uso da IA com a proteção dos direitos fundamentais e valores da União Europeia, mas a abordagem baseada em riscos levanta preocupações. Ao longo do texto Barkane (2022) argumenta que a abordagem baseada em direitos humanos oferece um quadro normativo sólido para garantir que os sistemas de IA funcionem em benefício das pessoas e da sociedade, prevenindo danos. É importante que o "AI Act" seja capaz de garantir a aplicação efetiva dos direitos fundamentais existentes e não impeça os Estados membros de tomar medidas nesse sentido. Além disso, destaca que os sistemas de IA devem cumprir a legislação existente, como a proteção de dados pessoais e a lei antidiscriminação, mas que essas normas não são suficientes para lidar com as complexidades da IA e os danos potenciais que ela pode causar.

Por fim o artigo afirma que o projeto de lei é um passo significativo para abordar os riscos dos sistemas de IA e promover uma IA confiável, mas ainda são necessárias medidas corajosas para introduzir proibições claras no projeto de lei. Recomenda-se proibir o uso de sistemas de identificação biométrica remota, fortalecer requisitos legais de responsabilidade e transparência, aprimorar os padrões de proteção de dados, introduzir avaliações de conformidade de terceiros para todos os sistemas de IA de alto

risco e mecanismos de reclamação e reparação. Além disso, destaca-se a importância de realizar avaliações de impacto para os usuários de sistemas de IA de alto risco, a fim de avaliar o impacto desses sistemas nos direitos fundamentais, bem como em valores democráticos e no Estado de Direito (BARKANE, 2022).

- **The ethical questions that haunt facial-recognition research - Van Noorden**

No artigo de Van Noorden (2020) na revista Nature, ele relata que em setembro de 2019, quatro pesquisadores escreveram à editora Wiley para solicitar "respeitosamente" a retratação imediata de um artigo científico. O estudo, publicado em 2018, treinou algoritmos para distinguir os rostos dos uigures (Uyghur), um grupo étnico predominantemente muçulmano na China, dos rostos de coreanos e tibetanos. O estudo levantou preocupações éticas, uma vez que a China já havia sido condenada internacionalmente por sua intensa vigilância e detenções em massa de uigures na província de Xinjiang. Autoridades em Xinjiang utilizaram câmeras de vigilância equipadas com software para identificar os rostos dos uigures. Vários outros estudos foram publicados em revistas importantes, descrevendo o uso de reconhecimento facial para identificar uigures e membros de outros grupos minoritários chineses.

Essa reclamação levou a uma investigação em andamento e reflete um movimento crescente de cientistas e ativistas de direitos humanos para que a comunidade científica adote uma postura mais firme contra a pesquisa antiética de reconhecimento facial. Além de denunciar o uso controverso dessa tecnologia, os cientistas também devem reconhecer as bases moralmente questionáveis da maioria dos estudos acadêmicos nessa área, incluindo estudos que coletaram grandes conjuntos de dados de imagens de rostos sem consentimento, muitos dos quais contribuíram para o aprimoramento de algoritmos de vigilância comercial ou militar.

Segundo Van Noorden (2020) muitos algoritmos de reconhecimento facial dependem de grandes conjuntos de dados de imagens para funcionarem bem. No passado, cientistas costumavam obter voluntários para posarem para essas fotos, mas agora a maioria coleta imagens faciais sem pedir permissão. Grandes coleções de dados têm sido reunidas online, muitas vezes sem o consentimento dos indivíduos. Alguns conjuntos de dados foram compartilhados abertamente e usados para avaliar e aprimorar produtos comerciais de vigilância. Após a revelação dessas práticas, algumas empresas e universidades removeram seus conjuntos de dados. No entanto, pesquisadores frequentemente usam imagens públicas do Flickr que foram enviadas

com licenças de direitos autorais que permitem reutilização livre.

O texto (VAN NOORDEN, 2020) discute a preocupação crescente de cientistas e ativistas de direitos humanos em relação à pesquisa antiética de reconhecimento facial. Muitos estudos têm coletado grandes conjuntos de dados de imagens de rostos sem consentimento, o que levanta questões éticas. Além disso, revistas e conferências acadêmicas publicaram artigos que descrevem o uso de reconhecimento facial para identificar grupos minoritários chineses, como os uigures. Essa pesquisa tem sido criticada devido às violações de direitos humanos que alegadamente ocorrem na China, como a vigilância intensa e detenções em massa dos uigures. Os pesquisadores estão pedindo restrições no uso de conjuntos de dados e uma revisão ética mais rigorosa dos estudos nessa área.

O estudo também menciona casos específicos de pesquisas controversas, como a coleta de imagens de estudantes sem seu consentimento na China e a disponibilização de grandes conjuntos de dados online. Além disso, aborda os desafios legais relacionados à coleta de dados biométricos sem consentimento, incluindo as leis de proteção de dados da União Europeia e processos judiciais nos Estados Unidos contra empresas que usam dados biométricos sem consentimento (VAN NOORDEN, 2020).

Resumindo, o texto destaca preocupações éticas em relação à pesquisa de reconhecimento facial, incluindo a coleta de dados sem consentimento, a identificação de grupos minoritários e as violações de direitos humanos associadas. Ele também menciona esforços para restringir o uso de conjuntos de dados e melhorar a ética na pesquisa (VAN NOORDEN, 2020).

O Institute of Electrical and Electronics Engineers (IEEE) aprovou uma política que exige que os autores confirmem se obtiveram aprovação de um Comitê de Ética em Pesquisa ou equivalente local para pesquisas envolvendo seres humanos ou animais. No entanto, alguns argumentam que os editores devem se posicionar não apenas sobre os detalhes do consentimento, mas também sobre a ética mais ampla da pesquisa. Sugere-se que os editores estabeleçam conselhos independentes de ética para fornecer opiniões em situações como essas. Além disso, universidades e pesquisadores também podem expressar sua reprovação a abusos de direitos humanos ao romperem suas associações com empresas de tecnologia questionáveis (VAN NOORDEN, 2020).

A parceria de algumas universidades com empresas de vigilância em massa em Xinjiang tem sido alvo de escrutínio. Também são mencionadas controvérsias

envolvendo conferências acadêmicas e pesquisas questionáveis nos Estados Unidos. Alguns estudos baseados em reconhecimento facial têm recebido críticas por sua falta de fundamentação científica e potencial para agravar preconceitos existentes no sistema de justiça criminal. Os apelos são feitos aos editores para que evitem publicar estudos semelhantes e aos acadêmicos para que parem de colaborar com a polícia em algoritmos que supostamente ajudam a reduzir o crime, devido a preocupações com racismo sistêmico. Springer Nature enfrentou críticas por um artigo sobre detecção de "tendência criminal" em fotos de criminosos e não criminosos, que foi posteriormente retirado. O processo de revisão dos periódicos foi revisado, e agora são exigidas declarações de aprovação ética e consentimento dos autores ao enviar manuscritos.

Van Noorden (2020) comentou sobre os achados de um survay realizado pela Nature para obter uma visão mais ampla das opiniões acadêmicas sobre a ética no reconhecimento facial, com 480 pesquisadores que publicaram artigos sobre reconhecimento facial, inteligência artificial e ciência da computação. Em algumas questões, os entrevistados mostraram uma clara preferência. Quando questionados sobre estudos que aplicam métodos de reconhecimento facial para identificar ou prever características pessoais (como gênero, identidade sexual, idade ou etnia) a partir da aparência, cerca de dois terços afirmaram que tais estudos deveriam ser realizados apenas com o consentimento informado das pessoas cujos rostos foram utilizados, ou após discussão com representantes de grupos que possam ser afetados.

No entanto, em outras questões, os acadêmicos estavam divididos. Cerca de 40% dos cientistas na pesquisa acreditavam que os pesquisadores deveriam obter consentimento informado das pessoas antes de usar seus rostos em um conjunto de dados de reconhecimento facial, mas mais da metade achava que isso não era necessário. O dilema dos pesquisadores é que é difícil treinar algoritmos precisos de reconhecimento facial sem conjuntos de dados extensos de fotos, afirma Sébastien Marcel, que lidera um grupo de biometria no Instituto de Pesquisa Idiap, na Suíça (VAN NOORDEN, 2020).

A pesquisa da Nature, citada por Van Noorden (2020) também perguntou aos pesquisadores se eles achavam que a pesquisa de reconhecimento facial em populações vulneráveis, como refugiados ou grupos minoritários sujeitos a intensa vigilância, poderia ser eticamente questionável, mesmo com o consentimento informado dos cientistas. No geral, 71% concordaram; alguns observaram que pode ser impossível determinar se o consentimento das populações vulneráveis é informado, tornando-o potencialmente sem valor. Alguns dos que discordaram, no entanto,

tentaram fazer uma distinção entre a pesquisa acadêmica e o uso do reconhecimento facial. O foco deve ser condenar e restringir aplicações antiéticas do reconhecimento facial, e não restringir a pesquisa, disseram eles.

Van Noorden (2020) afirma que alguns pesquisadores estão começando a exigir que os pesquisadores tenham mais cuidado. Uma das principais conferências da área de IA, a NeurIPS (Neural Information Processing Systems), está exigindo considerações éticas pela primeira vez este ano. Os cientistas que enviam artigos devem adicionar uma declaração abordando preocupações éticas e possíveis resultados negativos de seu trabalho. A revista Nature Machine Intelligence também está testando uma abordagem em que solicita aos autores de alguns artigos de aprendizado de máquina que incluam uma declaração considerando impactos sociais mais amplos e preocupações éticas.

Para Van Noorden (2020) há esperança de que os acadêmicos no campo do reconhecimento facial estejam despertando para as implicações do que estão pesquisando e o que isso pode significar para sua reputação se não abordarem questões éticas no campo. "Parece ser um momento de verdadeiro despertar na comunidade científica", diz Karen Levy, socióloga da Universidade de Cornell, que trabalha com ética em tecnologia (VAN NOORDEN, 2020, p. 358 , tradução nossa). "As pessoas estão mais conscientes das maneiras pelas quais as tecnologias nas quais trabalham podem ser usadas politicamente - e sentem isso visceralmente" (VAN NOORDEN, 2020, p. 358 , tradução nossa).

- **Legal Regulation of Government Applications of Facial Recognition Technology: A Comparison of Two Approaches – WANG; ZHANG**

Wang e Zhang (2022) abordam em seu texto o uso do reconhecimento facial e a coleta sem permissão de informações pessoais relacionadas a essa tecnologia. Os autores mencionam que a tecnologia de reconhecimento facial é uma forma de identificação biométrica que utiliza as características faciais para identificar indivíduos.

Descrevem várias aplicações do reconhecimento facial, incluindo verificação de identidade em sites, prevenção e controle de segurança em shoppings, análise de fluxo de passageiros e gestão da segurança social por órgãos governamentais, como investigação e prisão de suspeitos e controle de entrada e saída de unidades-chave (WANG; ZHANG, 2022).

No entanto, afirmam que o uso indevido dessa tecnologia por parte de órgãos

governamentais coloca em risco a privacidade pessoal e a segurança das informações. No Reino Unido, um cidadão chamado Edward Bridges entrou com uma ação contra a Polícia de South Wales, que implantou câmeras de reconhecimento facial. Bridges alegou que duas câmeras de reconhecimento facial na rua comercial e na sala de exposições o filmaram sem sua permissão, violando seus direitos pessoais. Vários outros casos são citados, como a multa imposta à prefeitura de Skelleftea, na Suécia, por usar a tecnologia em uma escola para controlar ausência e presença em uma escola e o debate intenso na China sobre o uso da tecnologia de reconhecimento facial pela polícia de trânsito (WANG; ZHANG, 2022).

O texto destaca que diferentes países adotam abordagens regulatórias distintas em relação ao reconhecimento facial. Nos Estados Unidos, algumas leis estaduais foram promulgadas para restringir o uso da tecnologia, permitindo apenas em casos específicos, como investigação de crimes graves, identificação de pessoas desaparecidas e na gestão prisional (WANG; ZHANG, 2022).

Na China e na União Europeia, a abordagem é baseada na proteção de dados pessoais, com leis e diretrizes que estabelecem procedimentos para o processamento de informações faciais. Na China, as agências governamentais que coletam informações e dados por meio de tecnologia devem seguir várias leis, incluindo o Código Civil Chinês, a Lei de Segurança Cibernética, a Lei Antiterrorismo, a Lei de Segurança de Dados e a Lei de Proteção de Informações Pessoais. Na União Europeia, foram promulgadas leis e diretrizes para proteger os direitos das pessoas no processamento de informações faciais no contexto da aplicação da lei criminal.

A pesquisa conclui que a tecnologia de reconhecimento facial não é boa ou má, mas seu uso indevido pode representar ameaças aos direitos individuais. É importante regular adequadamente essa tecnologia desde o início para evitar dilemas éticos e desafios futuros. Embora, segundo os autores, os Estados Unidos tenham uma atitude mais cautelosa em relação ao uso da tecnologia de reconhecimento facial, a China e a União Europeia adotam uma postura neutra, buscando proteger as informações e dados pessoais. Uma atitude neutra em relação à tecnologia é considerada mais apropriada para o seu desenvolvimento. O texto enfatiza a importância de abordar essas tecnologias de forma aberta, identificar conflitos e desafios e encontrar soluções adequadas (WANG;ZHANG, 2022).

- **Digital Right Protection Principles under Digitalization - Kirillova *et al.***

No estudo em questão (KIRILLOVA *et al.*, 2021), são apresentados métodos científicos e jurídicos para investigar os direitos humanos no contexto do desenvolvimento das tecnologias digitais e analisar os problemas de proteção desses direitos. Os resultados demonstram que os direitos digitais são a concretização dos direitos humanos garantidos pelo direito internacional e constituições, relacionados às necessidades das pessoas em uma sociedade baseada na informação. Esses direitos englobam o acesso, uso, criação e publicação de obras digitais, acesso a dispositivos eletrônicos e redes de comunicação, como a Internet, além da propriedade, comunicação e circulação de dados pessoais.

A proteção eficiente dos direitos digitais requer uma avaliação jurídica detalhada e um equilíbrio entre direitos e restrições no ambiente digital. O fator tecnológico desempenha um papel crucial no surgimento e desenvolvimento dos direitos humanos digitais, e a disseminação das tecnologias digitais pode afetar significativamente esses direitos (KIRILLOVA *et al.*, 2021).

Kirillova *et al*. (2021) discutem as restrições à liberdade de expressão, restrições econômicas e restrições às liberdades políticas no contexto digital. O acesso à Internet é considerado essencial para a liberdade humana, e bloquear o acesso à Internet é visto como uma séria interferência nessa liberdade.

Os autores (KIRILLOVA *et al.*, 2021) identificam os princípios básicos de proteção dos direitos digitais: o princípio da igualdade digital, o princípio da autodeterminação digital, o princípio da comunicação anônima, o princípio da confidencialidade das comunicações privadas, o princípio da privacidade no ambiente digital, o princípio do sigilo da identificação digital, o princípio da segurança dos dados obtidos por meio de tecnologias de reconhecimento facial e o princípio do apagamento das informações pessoais digitalizadas.

E ao discutir os princípios de proteção dos direitos digitais, trazem a importância de considerar o uso de tecnologias de reconhecimento facial e a utilização das imagens resultantes dos cidadãos. Tais imagens devem ser protegidas de forma confiável, e, portanto, o princípio da segurança dos dados obtidos por meio do reconhecimento facial precisa ser estabelecido em lei, dada a sua importância (KIRILLOVA *et al*., 2021).

- **Dostroajan: Facial Recognition Based System Input Control Agent - AYATA *et al*.**

Ayata *et al* (2020), expõem a importância da segurança dos dados à medida que a quantidade de informações aumenta rapidamente. São mencionados diferentes métodos de proteção, como senhas, leitores de impressão digital, reconhecimento de voz, íris e facial. O uso da inteligência artificial em conjunto com a segurança da informação trouxe soluções inovadoras, como o reconhecimento facial.

O estudo foca na aplicação do reconhecimento facial usando redes neurais convolucionais (CNN - Convolutional Neural Networks) para evitar o acesso não autorizado a sistemas. Uma rede neural convolucional (CNN) é um tipo especial de computador que ajuda a entender e trabalhar com imagens. Ela é projetada para encontrar padrões e informações importantes nas imagens. A palavra "convolucional" vem de uma operação matemática chamada convolução, que é uma operação importante que a CNN usa para fazer seu trabalho (AYATA *et al*, 2020).

O processo envolve registrar previamente as imagens dos usuários autorizados e, quando alguém tenta acessar o sistema, sua imagem é capturada e comparada com as imagens registradas. Se houver correspondência, o acesso é concedido; caso contrário, é notificada a autoridade do sistema. O aplicativo funciona em segundo plano, consumindo poucos recursos do sistema e iniciando automaticamente quando o sistema é ligado (AYATA *et al*, 2020).

O sistema desenvolvido foi testado usando o banco de dados facial da FEI (Faculdade de Engenharia Industrial – São Bernardo do Campo), que contém várias imagens faciais capturadas no Brasil. Os resultados demonstraram altos níveis de sucesso na identificação em diferentes exposições (AYATA *et al*, 2020).

No geral, destacam os avanços no reconhecimento facial, especialmente com o uso de redes neurais convolucionais. Também mencionam a aplicação dessas técnicas para segurança de sistemas e apresentam um sistema protótipo de segurança para computadores pessoais, utilizando a câmera integrada para detecção e reconhecimento facial. O sistema alcançou altas taxas de sucesso nos testes com o banco de dados da FEI (AYATA *et al*, 2020).

- **The ethics of inattention: revitalising civil inattention as a privacy-protecting mechanism in public spaces - SHARON; KOOPS**

Sharon e Koops (2021) iniciam seu artigo com um cenário inicial: uma pessoa

entra em um bonde lotado e tenta preservar sua privacidade ao evitar invadir o espaço pessoal dos outros passageiros. Ela faz isso virando a cabeça para longe, olhando para a parede ou fingindo estar distraída com a lista de paradas do bonde. O texto levanta a questão de se a tecnologia de reconhecimento facial pode comprometer a privacidade nesse contexto, mencionando a possibilidade de alguém tirar uma foto e usar essa imagem para identificá-la em um banco de dados de rostos.

O texto destaca a importância da "atenção civil", que é a norma social de mostrar a quantidade adequada de indiferença em relação aos outros para preservar a privacidade. Essa atenção civil é uma prática rotineira que ajuda as pessoas a manterem sua privacidade em situações de proximidade física. No entanto, tecnologias como o reconhecimento facial, podem prejudicar essa prática e as normas associadas de discrição e não reconhecimento (SHARON; KOOPS, 2021).

Os autores (SHARON; KOOPS, 2021) defendem que a atenção civil pode ampliar nossa compreensão dos problemas de privacidade trazidos pelas tecnologias de vigilância, e destacam a importância das normas sociais na preservação da privacidade. Eles discutem os desafios apresentados pelo uso do reconhecimento facial baseado no consumidor e as limitações das abordagens teóricas e legais existentes para lidar com esses problemas.

Sharon e Koops (2021) propõe revitalizar o conceito de atenção civil nos debates acadêmicos e regulatórios sobre tecnologias de vigilância. Também sugerem a necessidade de cultivar novas práticas de atenção civil em ambientes digitalmente pervasivos para lidar com os desafios da vigilância digital ubíqua. A atenção civil é descrita como um mecanismo complexo que envolve não apenas mostrar desinteresse, mas também fazer parte de uma coreografia maior das relações interpessoais.

Se destaca a importância das normas correlacionadas, como reserva, discrição e não reconhecimento, na proteção da privacidade em espaços públicos. Trazem discussões de como os teóricos Georg Simmel e Thomas Nagel analisaram essas normas e sua relação com a privacidade (SHARON; KOOPS, 2021).

Em relação à tecnologia de reconhecimento facial, o texto aborda os desafios que ela apresenta para a atenção civil e a privacidade. A capacidade da tecnologia de identificar e rastrear indivíduos em espaços públicos desafia as normas de atenção civil e os limites de exposição pública. Além disso, a falta de meios claros de comunicar desinteresse ou indiferença por meio de smartphones dificulta a aplicação das normas de atenção civil (SHARON; KOOPS, 2021).

O artigo conclui que é necessário desenvolver abordagens além da regulação e

proibição estrita do reconhecimento facial para lidar com seus impactos sociais e de privacidade. Sugere-se o desenvolvimento de novas práticas sociais, normas de atenção civil e intervenções políticas para mitigar os desafios trazidos por essa tecnologia (SHARON; KOOPS, 2021).

- **Typologies of Mobile Privacy Behavior and Attitude: A Case Study Comparing German and American Library and Information Science Students – Havelka**

Havelka (2021) optou por outra estratégia de pesquisa, e realizou um estudo de caso. Seu texto inicia informando sobre dados quantitativos do uso de smartphone, e o quanto esses dispositivos se tornaram uma parte essencial de nosso cotidiano. Com o avanço dos smartphones, os aplicativos móveis, conhecidos como apps, se tornaram extremamente populares. Em maio de 2020, a Google Play oferecia 2,56 milhões de apps e a App Store da Apple oferecia quase 1,85 milhões de apps aos usuários.

Para Havelka (2021) os apps influenciaram nosso comportamento digital, sem dúvida, para melhor ou pior. No entanto, muitos usuários não estão cientes de que os apps podem capturar automaticamente uma ampla variedade de informações do usuário, incluindo localização precisa, número de telefone, lista de contatos, fotos, registros de chamadas, identificadores únicos do dispositivo e informações pessoais identificáveis. À medida que a tecnologia dos smartphones continua a se tornar mais poderosa a cada ano, o conceito de privacidade na era digital muda seus significados e limites. Segundo Scoble e Israel (2014), "a privacidade é complexa, fluida e granular. Quanto dela desejamos depende de muitas variáveis. O Facebook costumava permitir que as pessoas respondessem ao seu status de relacionamento como 'É complicado'. Achamos que a mesma opção pode ser usada para a privacidade".

As bibliotecas têm trabalhado para se manterem atualizadas sobre como seus usuários (e o público em geral) interagem com smartphones e outros dispositivos móveis, o que tem mudado o papel das bibliotecas na sociedade. Inúmeros artigos, livros e conferências testemunham isso. O mesmo pode ser dito sobre bibliotecas e privacidade, uma vez que bibliotecários e cientistas da informação também têm estado no centro dos debates sobre privacidade e tecnologia da informação. Por exemplo, a IFLA endossou uma declaração sobre privacidade no ambiente das bibliotecas em sua reunião anual de 2014, afirmando que

> a proteção de dados e a privacidade devem ser incluídas como parte do treinamento em alfabetização midiática e informacional para usuários de serviços de bibliotecas e informação. Isso deve incluir o treinamento em

> ferramentas para proteger sua privacidade (IFLA, p. 5, 2014, tradução nossa).

Os bibliotecários de serviços web e móveis na Biblioteca Leonard Lief do Lehman College, criaram e ministram sessões de alfabetização informacional móvel para estudantes do Lehman College a partir de 2011. Inicialmente, os estudantes pareciam não se preocupar ou não estavam interessados nas questões de privacidade relacionadas aos apps. No entanto, no ano acadêmico de 2013-2014, percebemos uma pequena mudança em relação ao compartilhamento de localização. De repente, alguns estudantes passaram a estar mais conscientes da privacidade e não desejavam que o rastreamento de localização dos apps ocorresse em seus telefones sem consentimento prévio e conhecimento (HAVELKA, 2021).

Os participantes do estudo de caso foram estudantes de biblioteconomia e ciência da informação da Escola de Comunicação e Informação da Universidade Estadual de Rutgers, nos EUA, e estudantes de biblioteconomia e ciência da informação da Escola de Biblioteconomia e Ciência da Informação de Berlim, na Alemanha. Os estudantes de biblioteconomia e ciência da informação foram escolhidos como entrevistados porque a educação em privacidade faz parte do currículo em muitos departamentos de biblioteconomia e ciência da informação, e os estudantes atuais cresceram usando tecnologias móveis. Como tal, eles podem ter sido expostos à aprendizagem móvel em sua educação básica (HAVELKA, 2021).

Os participantes do estudo foram recrutados por e-mail e assinaram o termo de consentimento informado no início da entrevista. A experiência de estudos de pesquisas anteriores ensinou Havelka (2021) que é mais fácil recrutar participantes se houver uma recompensa incluída. Os participantes receberam uma pequena quantia de compensação financeira: €10 para participantes alemães e 15 USD para participantes dos EUA, em dinheiro ou certificado de presente da Amazon no mesmo valor.

Foram realizados 2 campos de trabalho, um entre janeiro de 2017 e agosto de 2018, no total, dez estudantes americanos e dez estudantes alemães participaram deste estudo. Todas as entrevistas gravadas foram armazenadas com segurança, anonimizadas e importadas para um software de análise qualitativa para transcrição. Em seguida, a cada participante foi atribuído um pseudônimo.

Os resultados da pesquisa de Havelka (2021) revela que quase não há diferenças culturais no comportamento e na atitude em relação à privacidade móvel entre os participantes. Na verdade, o estudo descobre e distingue diferentes tipologias de privacidade móvel. Essas tipologias, que variam desde "objeção à privacidade

móvel" até "resignação aprendida em relação à privacidade móvel", revelam como elas afetam o comportamento e a atitude em relação à privacidade de estudantes alemães e americanos de maneira similar.

A falta de diferenças significativas entre os estudantes alemães e americanos de biblioteconomia e ciência da informação sugere que aconteça uma forte conscientização sobre privacidade, especialmente para computação móvel e tecnologias emergentes, como reconhecimento facial e inteligência artificial já que os estudantes demonstraram certa apatia ao tema (HAVELKA,2021).

- **Mobile augmented reality applications for library services - HAHN, Jim**

As aplicabilidades do reconhecimento facial se atrelam a outras funções da inteligencia artificial, como o da realidade aumentada. Hahn (2012) destaca que existem atualmente disponíveis softwares de código aberto capazes de identificar rostos. Além disso, é possível encontrar aplicativos com essa funcionalidade nas bibliotecas. Em 2012, a equipe da biblioteca da Universidade de Illinois (EUA) utilizava um computador de estação de trabalho completa conectado a um scanner de código de barras para registrar a identificação dos usuários. No entanto, o uso de scanners de código de barras pode não ser necessário se um funcionário puder utilizar um smartphone da biblioteca para escanear a identificação com foto do usuário. Nesse caso, a imagem escaneada poderá passar por um processo de detecção de recursos e reconhecimento do usuário, permitindo o registro dos itens que estão sendo retirados pelo usuário.

A implementação de um aplicativo desse tipo poderia resultar em uma economia de custos para a biblioteca, uma vez que muitas das transações realizadas no balcão de circulação não requerem todos os recursos de um computador de mesa. De fato, essas transações poderiam ser realizadas utilizando-se um pequeno computador tablet carregado com o software de reconhecimento facial da biblioteca, substituindo assim o paradigma tradicional do uso de desktops.

É importante ressaltar que a adoção desse tipo de solução traz consigo benefícios potenciais, como maior eficiência no atendimento aos usuários e redução de custos operacionais. No entanto, é fundamental realizar uma análise completa dos requisitos técnicos, considerar questões de segurança e privacidade dos dados dos usuários, além de avaliar a viabilidade financeira e a capacidade de integração com os sistemas existentes na biblioteca (HAHN,2012).

- **IoT Solution for Smart Library Using Facial Recognition – UPALA; WONG**

Para Upala e Wong (2019) as bibliotecas são uma parte essencial do sistema educacional para aprimorar nosso conhecimento. Com o avanço das tecnologias de informação e comunicação, a Internet das Coisas (IoT) surge como um desafio para as bibliotecas. Neste artigo os pesquisadores propõem um sistema de inteligência que permite aos usuários uma visão em tempo real dos recursos da biblioteca. A IoT tem potencial para criar um sistema de biblioteca inteligente, melhorando a eficiência operacional e a experiência do usuário, utilizando o reconhecimento facial. Uma pesquisa realizada em 2014 mostrou o interesse dos bibliotecários nas tecnologias de IoT, mas também levantou preocupações sobre privacidade e segurança.

A Internet das Coisas (IoT) é um conceito que estabelece conexões entre pessoas, processos, dados e objetos, e sua aplicação nas bibliotecas pode fornecer serviços convenientes e eficientes aos usuários. Este projeto propõe uma solução de IoT para bibliotecas inteligentes, com foco em tecnologia assistiva, acesso e autenticação, e disponibilidade de recursos físicos. A arquitetura do sistema é dividida em quatro níveis: físico, comunicação, sistema e usuário final. A plataforma IoT utilizada é o ThingSpeak, que permite a coleta e análise de dados em tempo real. Dispositivos de baixo custo, como o Up-Squared, são usados para conectar sensores e atuadores. O reconhecimento facial é introduzido para autenticação.

A autenticação é uma extensão do mecanismo de reconhecimento facial no contexto da IoT. Ela permite o acesso do usuário por meio do reconhecimento facial. O sistema autentica o usuário usando o reconhecimento facial, mas caso o reconhecimento falhe, o administrador tem a opção de registrar manualmente o usuário no banco de dados da biblioteca. A autenticação é realizada com o uso de um tipo de algoritmo especifico e de um banco de dados. A implementação também envolve o uso de sensores ultrassônicos conectados a um computador, que coletam informações em tempo real sobre o uso das salas da biblioteca. Os dados coletados são transmitidos para o ThingSpeak, uma plataforma de IoT, por meio de um *gateway*. O objetivo é permitir o acesso a um aplicativo de IoT que monitora a ocupação e uso das salas da biblioteca (UPALA; WONG, 2019).

A implementação de soluções de IoT pode enriquecer os serviços da biblioteca e melhorar a experiência do usuário. De acordo com Upala e Wong (2019), existem desafios a serem superados, como o custo dos dispositivos IoT e a adaptação às

normas técnicas. O reconhecimento facial ainda é um desafio, exigindo um conjunto de dados abrangente para obter resultados precisos. Pesquisas futuras descritas no artigo são necessárias para abordar questões de privacidade, compreender o uso do espaço físico da biblioteca e aprimorar a tecnologia de reconhecimento facial. A coleta de dados qualitativos e quantitativos pode ajudar a gerenciar o espaço da biblioteca de forma mais eficiente. A implementação de tecnologias IoT permitirá tomar decisões estratégicas e desenvolver um ambiente de biblioteca mais eficaz.

- **Roundup - Brown-Syed; Owens**

O estudo de Brown-Syed e Owens (2011) discorre sobre um caso específico de utilização do reconhecimento facial em uma biblioteca. O ocorrido em Boise, Idaho (EUA) que envolveu atos repetidos de danos intencionais aos livros de uma biblioteca, gerando repercussão midiática mundial. Durante um período de um ano, alguém vinha depositando condimentos, como xarope (*maple syrup*) e ketchup, entre os livros de uma caixa de devolução. Esses incidentes resultaram em danos estimados em cerca de US$ 2.500 para a biblioteca. A mídia internacional apelidou o caso de "ondas de crimes com condimentos", e o responsável pelos atos foi rotulado como o "vândalo da caixa de devolução de livros" ou "criminoso serial dos condimentos", porém não havia sido identificado (BROWN-SYED; OWENS, 2011, tradução nossa).

Para solucionar o problema, foram instaladas câmeras de segurança, permitindo que as autoridades da biblioteca identificassem um veículo suspeito. Através da análise das imagens e do reconhecimento facial, foi possível identificar a condutora como alguém que havia sido proibida de frequentar a biblioteca dois anos antes, devido ao assédio e ameaças a funcionários e outros usuários da instituição. Posteriormente, a suspeita foi detida e acusada de danos criminosos à propriedade e porte de arma oculta.

Visando evitar danos futuros, a biblioteca implementou medidas adicionais, como a programação de verificações regulares da caixa de devolução de livros pelos funcionários durante o período em que os incidentes ocorreram. Essa história peculiar de vandalismo deliberado em uma biblioteca evidencia a importância da atuação dos bibliotecários na manutenção da integridade dos acervos e destaca a identidade incomum do perpetrador, o que chamou a atenção da mídia.

Danos aos materiais de biblioteca são preocupantes, mas geralmente não recebem atenção da mídia. Influências diárias como luz, temperatura, umidade,

alimentos, água e pragas representam ameaças à conservação dos livros. Roubo deliberado de obras raras e remoção de páginas por motivos financeiros são preocupações para bibliotecários e arquivistas. No entanto, Brown-Syed e Owens (2011) afirmam que existem pesquisas e evidências que sugerem que as pessoas ao redor do mundo geralmente valorizam as bibliotecas públicas. Além dos atos ocasionais de vandalismo direcionados a qualquer prédio público, sabotagem deliberada de bibliotecas é tão rara a ponto de se tornar notícia (BROWN-SYED; OWENS, 2011).

- **The importance of security for people and collections in libraries - Botez; Repanovici**

O estudo de Botez e Repanovici (2017) teve como objetivo discutir a importância da segurança em bibliotecas, com enfoque na necessidade de encontrar um equilíbrio entre o acesso aos materiais e a proteção adequada das coleções, bem como a segurança dos usuários e funcionários. Destacam a relevância do planejamento e da implementação de medidas de segurança eficazes para lidar com os desafios contemporâneos nesse ambiente.

Para alcançar esse objetivo, foram realizadas pesquisas na Romênia e Moldávia, com a participação de bibliotecários. Os resultados obtidos revelaram que a maioria dos profissionais está disposta a adotar um sistema de reconhecimento facial e possui confiança nessa tecnologia. Adicionalmente, os sistemas de reconhecimento biométrico foram considerados mais seguros em comparação com o sistema RFID.

A análise estatística desta pesquisa e dos dados coletados demonstrou uma forte correlação entre a preocupação dos bibliotecários com a segurança das pessoas, a crença na adequação do sistema de reconhecimento facial, a confiança nos sistemas de reconhecimento facial e a concordância dos bibliotecários em implementar tal sistema. Entretanto, não foram encontradas associações estatisticamente significativas entre o tamanho da biblioteca, a função do bibliotecário, o nível de educação ou a experiência de trabalho, e a disposição dos bibliotecários em adotar um sistema de reconhecimento facial.

Em síntese, os resultados deste estudo ressaltam a importância da segurança em bibliotecas, a necessidade de equilibrar o acesso aos materiais com a proteção adequada das coleções e a segurança dos usuários e funcionários. Além disso, enfatizam a viabilidade e confiança dos bibliotecários na implementação de sistemas de

reconhecimento facial como medida de segurança, considerando-os mais seguros em comparação com outras tecnologias disponíveis (BOTEZ; REPANOVICI, 2017).

- **Identificación facial biométrica - CALDERA-SERRANO; ZAPICO- ALONSO**

Caldera-Serrano e Zapico-Alonso (2009) discutem a gestão documental nos meios de comunicação, especialmente na televisão, que enfrenta desafios devido ao elevado volume de trabalho e à complexidade da informação audiovisual. Nesse contexto, as tecnologias biométricas, como o reconhecimento automático de imagens e sons, surgem como ferramentas promissoras para auxiliar na indexação temática e onomástica. O reconhecimento facial, uma técnica biométrica amplamente utilizada, identifica pessoas com base em características físicas do rosto, como pontos nodais, permitindo a criação de um "faceprint" único para cada indivíduo. Softwares de reconhecimento facial, como Visionics e FRS Access II, são exemplos de sistemas que capturam e comparam rostos com base em bancos de dados.

No contexto da indústria televisiva e cinematográfica, a aplicação dessas tecnologias tem sido explorada, embora haja desafios a serem enfrentados. A necessidade de atualizar constantemente os bancos de dados com imagens e lidar com outros elementos presentes no material audiovisual são questões relevantes. A identificação facial biométrica mostra-se útil na indexação de pessoas, lugares e temas em serviços de documentação audiovisual. A aplicação mencionada no texto demonstrou um alto grau de acerto ao reconhecer o ator Tom Hanks em fotografias, devido à semelhança na posição da cabeça e nas condições de iluminação. Entretanto, quando apresentadas imagens de Tom Hanks em anos posteriores, com mudanças físicas e posições diferentes, a aplicação falhou em identificá-lo corretamente. Esse resultado inadequado poderia ter sido evitado por meio da atualização do banco de dados e da inclusão de mais imagens em diferentes posições do personagem (CALDERA-SERRANO; ZAPICO-ALONSO, 2009).

Embora tenham sido feitos esforços na Espanha por parte de redes de televisão privadas no desenvolvimento de aplicativos semelhantes e tenham sido conduzidos testes com outro tipo de software na *Televisión Española*, até o momento, não há evidências de que alguma rede de televisão no país tenha implementado essa tecnologia (CALDERA-SERRANO; ZAPICO-ALONSO, 2009).

O reconhecimento facial e de voz apresentam um grande potencial para a indexação automática e podem agilizar o trabalho dos documentalistas. As pesquisas

nessa área estão focadas em aprimorar os resultados em condições não controladas e em tempo real, uma vez que os resultados atuais são menos confiáveis nessas situações (CALDERA-SERRANO; ZAPICO-ALONSO, 2009).

Portanto, é evidente que o uso dessas tecnologias para esta aplicação não se trata apenas de uma ideia futurista, mas sim de uma realidade que as redes de televisão podem enfrentar. No entanto, é necessária a participação ativa das televisões ou de empresas externas para manter os bancos de dados de imagens padrão atualizados, incluindo os personagens mais populares e famosos em diferentes posturas, posições, ângulos e iluminação, com o objetivo de melhorar o reconhecimento facial (CALDERA-SERRANO; ZAPICO-ALONSO, 2009).

Em síntese, conclui-se que o reconhecimento facial e de voz possuem um potencial significativo no campo da televisão, mas várias características devem ser consideradas, como a presença de múltiplos personagens em uma imagem, a posição da câmera, a iluminação, a atualização constante do banco de dados e a influência do fundo nos resultados do sistema e é necessário um esforço contínuo para aprimorar a confiabilidade e a precisão do reconhecimento facial em condições não controladas (CALDERA-SERRANO; ZAPICO-ALONSO, 2009).

- **Batch metadata assignment to archival photograph collections using facial recognition software - BANERJEE; ANDERSON**

Para Banerjee e Anderson (2013) as coleções de fotografias arquivadas ocupam um lugar central nas iniciativas digitais. Essas imagens estabelecem conexões visuais poderosas com a história institucional, impressionando administradores e financiadores, além de servir a propósitos que vão desde relações públicas até pesquisas acadêmicas intensivas. Essas fotografias chegam aos arquivos em formatos analógicos ou como objetos digitais nativos, provenientes de departamentos institucionais e doações individuais, em quantidades que podem chegar a centenas ou milhares.

Essas fotografias atraem diversos grupos de usuários, e os pesquisadores esperam que as coleções arquivadas sejam facilmente encontradas e pesquisáveis por palavras-chave online. No entanto, fornecer esse acesso usando métodos tradicionais requer uma equipe especializada com conhecimento das coleções arquivadas, habilidades para criar metadados originais e realizar pesquisas históricas. Quando se lida com uma grande coleção de fotografias, equilibrar as expectativas dos pesquisadores com as limitações de pessoal se torna um desafio (BANERJEE;

ANDERSON, 2013).

Sem um planejamento cuidadoso em todas as etapas, os projetos de digitalização de fotos arquivadas podem se tornar um gargalo na criação de metadados. Mesmo gestores experientes em outros projetos de digitalização frequentemente subestimam o tempo necessário para criar metadados especializados para as fotografias arquivadas, resultando em imagens digitalizadas acumuladas sem metadados descritivos. Esses acúmulos também podem ser gerados pela digitalização para uso interno, exposições ou solicitações de pesquisadores. À medida que doadores contribuem com coleções de fotografias digitais, muitas vezes sem qualquer descrição além do nome do arquivo, o acúmulo de imagens nativas digitais aumenta. Para torná-las acessíveis, é necessário fornecer metadados completos e hospedá-las em uma plataforma pública. Caso contrário, essas imagens são armazenadas em servidores, discos rígidos externos, redes ou computadores dos funcionários, onde ficam efetivamente ocultas tanto para a equipe quanto para os pesquisadores (BANERJEE; ANDERSON, 2013).

A pesquisa sugere a colaboração entre arquivistas e equipes de sistemas, com o objetivo de automatizar a criação e coleta de metadados de forma mais eficiente. Este artigo demonstra como uma equipe com habilidades técnicas modestas pode utilizar técnicas de automação simples para aproveitar os metadados já existentes em fotografias digitais e digitalizadas, bem como informações obtidas de softwares de reconhecimento facial, para atribuir metadados de forma mais rápida, precisa e abrangente (BANERJEE; ANDERSON, 2013).

A maioria dos sistemas utilizados pelas bibliotecas para armazenar fotografias digitais não aproveita os metadados incorporados nos arquivos de imagem digital. Em vez disso, essas informações são gerenciadas em um banco de dados externo. No entanto, é mais eficiente encontrar as imagens por meio de mecanismos de busca quando os metadados estão incorporados nos arquivos. Além disso, os metadados incorporados nas imagens garantem que as informações associadas sejam transportadas junto com as fotografias, independentemente de como elas são utilizadas (BANERJEE; ANDERSON, 2013).

O uso de software de reconhecimento facial pode auxiliar no processamento de fotografias digitais, identificando pessoas nas imagens. Essa tecnologia desempenha um papel importante ao determinar o assunto, horário e localização das fotos. Mesmo quando o software não consegue identificar indivíduos específicos, a extração de rostos facilita a identificação e organização manual. Vários aplicativos e serviços de software

oferecem recursos de reconhecimento facial, como o Picasa do Google (BANERJEE; ANDERSON, 2013).

O Picasa era um software, citado na pesquisa Banerjee e Anderson (2013), que utilizava o reconhecimento facial e armazenava informações sobre pessoas identificadas em arquivos separados. O software detecta rostos, faz correspondências com pessoas conhecidas e permite que a equipe confirme ou rejeite essas correspondências. No entanto, a precisão depende de vários fatores, e a revisão manual ainda é necessária. Embora a automação possa agilizar a criação de metadados, é importante envolver arquivistas para garantir a interpretação correta, organização adequada e considerações éticas durante o processo.

Em resumo, o texto destaca os benefícios dos padrões de metadados de imagens e da tecnologia de reconhecimento facial para melhorar o processamento e a organização de fotografias digitais em bibliotecas e arquivos (BANERJEE; ANDERSON, 2013).

- **Library Attendance System using YOLOv5 Faces Recognition - MARDIANA, MUHAMMAD; MULYANI**

A pesquisa de Mardiana, Muhammad e Mulyani (2021) teve como objetivo solucionar problemas nas bibliotecas. Para os autores embora a automação tenha auxiliado nas tarefas dos bibliotecários, a detecção visual de usuários ainda é um desafio. Atualmente, a presença dos visitantes é registrada por meio de cartões RFID e códigos de barras na entrada das bibliotecas, mas esses métodos apresentam problemas de segurança. Para resolver esses problemas, é necessário utilizar tecnologia computacional e algoritmos capazes de reconhecer objetos.

Uma das abordagens utilizadas é o uso do algoritmo YOLO (You Only Look Once), que é uma rede neural desenvolvida para detectar objetos em tempo real. Diversos estudos foram realizados para detectar objetos usando o YOLO, e os resultados têm sido promissores. Por exemplo, o algoritmo YOLO pode detectar placas de sinalização de trânsito com uma precisão de 74% e objetos esféricos em robôs humanoides de futebol com uma precisão de 60%. No contexto do sistema de registro de presença em bibliotecas, o algoritmo YOLOv5 é utilizado devido às suas vantagens em relação às versões anteriores. Com o YOLOv5, o sistema será capaz de reconhecer o rosto do usuário e armazenar os dados no banco de dados, facilitando o

processamento dos dados de presença pelos bibliotecários (MARDIANA; MUHAMMAD; MULYANI, 2021).

O sistema de registro de presença em bibliotecas é composto por três subsistemas: Serviço de API, Reconhecimento facial usando YOLOv5 e sistema de identificação de visitantes. O desenvolvimento desses subsistemas envolve a construção de um serviço de API, a implementação do YOLOv5 para reconhecimento facial e o desenvolvimento de um sistema de identificação de visitantes. Além disso, é realizado um teste abrangente do sistema para avaliar a integração dos subsistemas (MARDIANA; MUHAMMAD; MULYANI, 2021).

O sistema de registro de presença em bibliotecas proposto na pesquisa de Mardiana, Muhammad e Mulyani (2021) utiliza o algoritmo YOLOv5 para reconhecimento facial, permitindo o registro e armazenamento dos dados de presença dos usuários, o que representa um avanço tecnológico que simplifica e aprimora a gestão de bibliotecas. A detecção e reconhecimento facial automatizados oferecem maior precisão e eficiência no registro de presença dos usuários, proporcionando benefícios tanto para os bibliotecários quanto para os visitantes (MARDIANA; MUHAMMAD; MULYANI, 2021).

- **Representation of Libraries in Artificial Intelligence Regulations and Implications for Ethics and Practice - Bradley**

Bradley (2022) alerta que a sociedade contemporânea encontra-se imersa em uma realidade algorítmica, na qual as políticas e regulamentações relacionadas à IA estão emergindo em paralelo ao crescente conhecimento sobre as implicações do viés em conjuntos de aprendizado de máquina, os riscos de vigilância em cidades inteligentes e o reconhecimento facial, bem como a tomada de decisões automatizadas pelo governo, entre outras aplicações da IA e do aprendizado de máquina. Cada um desses aspectos suscita preocupações no que diz respeito à ética, privacidade e proteção de dados.

O artigo de Bradley (2022) teve por objetivo apresentar alguns dos principais desenvolvimentos regulatórios no campo da IA até o momento, bem como a participação das bibliotecas nesses processos. Embora muitas aplicações da IA nas bibliotecas sejam predominantemente emergentes e hipotéticas, é possível identificar exemplos mais consolidados na literatura de pesquisa, como a busca em bases de dados, ferramentas linguísticas para análise textual e acesso a dados de coleções. O

artigo oferece um resumo de como essas atividades bibliotecárias são representadas nos planos nacionais de IA, além de abordar a maneira pela qual as bibliotecas têm se envolvido com outros aspectos da regulamentação da IA, o que inclui o desenvolvimento de estruturas éticas.

Embora existam muitas aplicações positivas de IA em bibliotecas e pesquisas, também existe uma variedade de preocupações. Dada a amplitude das aplicações de IA que afetam a vida diária e a falta de transparência, não é surpreendente que os debates até o momento sobre IA na área de biblioteca e informação tenham sido extremamente abrangentes. Esses debates abrangem desde direitos humanos e dilemas éticos, preocupações com a vigilância estatal e privada, o surgimento de cidades inteligentes e reconhecimento facial, até questões sobre como as pessoas desenvolverão a alfabetização algorítmica (BRADLEY, 2022).

As bibliotecas criam e fornecem acesso a enormes quantidades de informações em vários conjuntos de dados e possuem uma quantidade significativa de dados pessoais. Métodos de IA já estão sendo promovidos como um recurso de muitos produtos fornecidos por fornecedores de bibliotecas. No entanto, exemplos como o caso Robodebt, quando centenas de milhares de pessoas receberam cartas falsas afirmando que deviam grandes dívidas ao governo. O erro foi atribuído a um algoritmo usado para identificar incorretamente os beneficiários de pagamentos assistenciais que foram associados erroneamente a outros conjuntos de dados no escritório de impostos (HENRIQUES-GOMES, 2021), devem servir como um alerta de que a combinação de conjuntos de dados para criar novas percepções usando métodos de IA requer grande cuidado e habilidade. No entanto, poucas declarações dedicadas sobre IA, reconhecimento facial e ética foram emitidas até o momento na profissão de bibliotecário. A declaração da IFLA é um exemplo que reflete tanto os valores éticos de longa data em relação à liberdade intelectual e privacidade, quanto abre espaço para um debate adicional dentro da profissão (BRADLEY, 2022).

O artigo (BRADLEY, 2022) apresenta um panorama das atividades e iniciativas das bibliotecas na regulamentação da IA em um ambiente em constante mudança. As bibliotecas têm sido ativas na moldagem e influência do desenvolvimento de leis de direitos autorais, proteção de dados e outras que criaram a base para as aplicações contemporâneas de IA e aprendizado de máquina. Essas regulamentações ajudaram as bibliotecas a abrir seus dados e coleções, mas também possibilitaram uma maior agregação e análise de dados por parte de empresas e governos.

Conforme evidenciado por Bradley (2022), o setor já está participando de

consultas e processos para garantir que o futuro da IA seja baseado em direitos, ético e transparente. Embora haja uma representação limitada dos serviços de biblioteca nos planos nacionais e estruturas existentes de IA até o momento, a regulamentação da IA ainda está em estágio inicial, o que sugere prováveis oportunidades para as bibliotecas em muitos países se envolverem no futuro.

Os riscos de viés algorítmico e tomada de decisões automatizada têm levado a pedidos de regulamentação governamental, pressão da sociedade civil sobre empresas privadas e a necessidade de uma reflexão significativa sobre a prática ética. Regulamentações futuras podem impactar os serviços de biblioteca de maneiras ainda desconhecidas, assim como as leis de direitos autorais e proteção de dados têm impactado positiva e negativamente os serviços de biblioteca no ambiente digital (BRADLEY, 2022).

Portanto, em vez de apenas considerar as respostas à IA através de uma perspectiva centrada na biblioteca, a amplitude e a inserção da IA em quase todos os aspectos da vida diária significam que o setor deve contribuir e se apoiar em iniciativas nacionais e setoriais (BRADLEY, 2022).

- **Design and Development of Facial Recognition-based Library Management System (FRLMS) – RAO *et al.***

O reconhecimento facial (RF) é uma abordagem biométrica que utiliza métodos automatizados para identificar ou reconhecer um rosto individual, analisando e comparando padrões de características fisiológicas (impressão digital, padrão da íris e rosto) e padrões comportamentais (caligrafia e voz). A tecnologia de reconhecimento facial está evoluindo gradualmente para se tornar uma solução biométrica universal devido à sua facilidade de uso em comparação com outras opções biométricas. Para RAO et al. (2018) o reconhecimento facial é não intrusivo e verifica a identificação humana de maneira eficiente, de forma natural e amigável.

Em relação às atividades estudantis e acadêmicas, o RF foi implementado com sucesso em sistemas de controle de presença de estudantes. Além dos sistemas de controle de presença, estudantes e membros do corpo docente também enfrentam problemas ao acessar a biblioteca. Todo estudante e membro do corpo docente espera um serviço de atendimento eficiente e acesso fácil aos recursos da biblioteca. A maioria das bibliotecas acadêmicas espera que os estudantes sejam totalmente independentes e de acordo com RAO et al. (2018) procurarão reduzir ao máximo a comunicação entre estudantes e bibliotecários.

Por outro lado, os bibliotecários também enfrentam problemas, pois estão ocupados com suas atribuições e podem perder dados ao rastrear o histórico de empréstimo de um estudante/leitor na biblioteca. Por exemplo, um bibliotecário ou estudante pode não estar atualizado com o status de empréstimo e devolução, e assim pode ultrapassar a data de vencimento e ser cobrado com uma taxa extra a pagar (RAO et al., 2018).

Além disso, os estudantes frequentemente perdem ou danificam seu cartão de identificação devido a situações imprevistas. Isso causaria dificuldades ao acessar a biblioteca e utilizar seus recursos quando necessário. Por exemplo, na Universidade Taylor's (Indiana/ USA), há uma multa por cartão de identificação perdido na primeira ocorrência e o dobro do valor na segunda. Isso é um problema para estudantes com orçamento reduzido (RAO et al., 2018).

Assim, o objetivo do artigo (RAO et al., 2018) foi desenvolver um protótipo de sistema de gerenciamento de biblioteca baseado em RF, chamado Sistema de Gerenciamento de Biblioteca com Reconhecimento Facial (FRLMS, Facial Recognition-based Library Management Systems). O foco dos autores era projetar um sistema que pudesse identificar com precisão o rosto do estudante. Além disso, o sistema proposto mostrará se há multas a serem pagas devido à devolução atrasada de livros ou qualquer outro registro relacionado a assuntos da biblioteca.

Os sistemas de reconhecimento facial (RF) se tornaram muito populares e desempenham um papel vital em diversas aplicações, como controle de acesso a prédios, engajamento móvel e controle de imigração. Na vigilância, o RF é usado para detectar crimes em cidades. Para verificação de identidade, é aplicado em documentos de identificação, passaportes, carteiras de motorista, cartões de funcionários e carteiras de estudante. Também é utilizado em sistemas de justiça criminal, classificação de gênero, reconhecimento de emoções e cuidados de saúde (RAO et al., 2018).

A pesquisa de Rao et al. (2018) mostra outros estudos sobre somo o uso do reconhecimento facial poderia solucionar problemas como o uso de cartões de identificação falsos por estudantes para entrar na biblioteca. Além disso, há relatos de cartões roubados sendo utilizados para empréstimo de livros.

A coleta de dados do usuário é realizada por meio de um sistema de reconhecimento facial que armazena os dados em um banco de dados na nuvem. A autenticação de entrada substitui os leitores de cartão de acesso por câmeras, e a autenticação de empréstimo de livros permite que os estudantes escaneiem os livros apenas olhando para a câmera (RAO et al., 2018).

O FRLMS (Sistema de Gerenciamento de Biblioteca Baseado em Reconhecimento Facial) utiliza uma combinação de hardware e software. O sistema foi testado com três participantes voluntários do sexo masculino, e o experimento foi dividido em duas fases: coleta de dados e teste. Durante a coleta de dados, os participantes seguiram certas restrições em relação à aparência, como não usar óculos, maquiagem ou joias. Durante os testes, não havia restrições quanto à aparência (RAO et al., 2018).

Os resultados do teste de Rao et al. (2018) mostraram a precisão do sistema para identificação dos participantes. Cada participante foi testado cinco vezes, e os resultados indicaram taxas de precisão variadas. Algumas falhas ocorreram devido a fatores como cabelo cobrindo as sobrancelhas, olhar para o lado, uso de barba e plano de fundo brilhante. No geral, a precisão média variou de 97,5% a 98,33% para os participantes.

O estudo conclui que o sistema FRLMS, com seu modelo de reconhecimento facial baseado em aprendizado de máquina, pode facilitar o acesso aos recursos da biblioteca para estudantes universitários. No futuro, os pesquisadores pretendem impor mais regras e funcionalidades e adiciona-las ao sistema para melhorar a segurança, como identificar multas por devolução atrasada de livros e monitorar o cumprimento das regras da biblioteca. Isso pode levar a restrições de acesso para estudantes que violarem repetidamente as regras estabelecidas pelos bibliotecários (RAO et al., 2018).

- **Recognizability of computer-generated facial approximations in an automated facial recognition context for potential use in unidentified persons data repositories: Optimally and operationally modeled conditions – PARKS; MONSON**

De acordo com Parks e Monson (2018), nos Estados Unidos, há uma quantidade significativa de restos mortais não identificados que estão armazenados em instituições médicas, de aplicação da lei e forenses em todo o país. Para lidar com essa questão, foram estabelecidos diversos repositórios de dados digitais, cujo objetivo é organizar e disseminar informações sobre esses casos de indivíduos não identificados, sendo que alguns desses repositórios também mantêm registros de pessoas desaparecidas. Embora existam referências cruzadas de dados textuais entre os registros de pessoas desaparecidas e os registros de indivíduos não identificados em alguns desses repositórios, até o momento não há conhecimento de nenhum repositório que faça uso

da tecnologia de análise de imagem para realizar o cruzamento de dados de imagens.

Conforme os resultados sugeridos por Parks e Monson (2018), é evidente que as aproximações faciais geradas por computador, quando utilizadas em um contexto de reconhecimento facial automatizado, apresentam consistência ao serem incluídas em listas de candidatos priorizados. Os autores realizaram dois estudos simultâneos, com o objetivo de explorar um caso de uso específico discutido em sua pesquisa. No primeiro estudo, foi utilizada uma galeria de imagens faciais em condições ideais, composta por 6159 imagens faciais altamente consistentes. Essa abordagem permitiu estabelecer o desempenho máximo resultante do uso combinado de dois programas de software empregados. No segundo estudo, por sua vez, uma galeria contendo 1816 imagens faciais de pessoas desaparecidas, compilada a partir de um conjunto de dados do mundo real, foi utilizada, a fim de informar sobre o desempenho operacional potencial quando se lida com imagens faciais altamente variadas, geralmente encontradas em bancos de dados públicos.

Parks e Monson (2018) demonstram que, de forma geral, nas maiores análises modeladas de forma ideal, 53% das aproximações faciais para os 159 indivíduos de teste examinados foram correspondidas com suas respectivas fotos de vida, estando entre as 50 principais imagens de uma lista de candidatos gerada por uma busca cega em uma galeria altamente consistente, composta por 6159 imagens. No estudo, aproximadamente 31% das aproximações faciais dos 16 indivíduos de teste foram correspondidas com suas respectivas fotos de vida, estando entre as 50 principais imagens de uma lista de candidatos gerada por uma busca cega em uma galeria preenchida com imagens de um conjunto de dados operacional, contendo 1816 imagens. Conforme previsto, as taxas de inclusão nas listas de candidatos foram aprimoradas com o uso de filtros demográficos. Não foram observadas diferenças significativas nas taxas de inclusão entre os grupos de sexo ou idade examinados, no entanto, foram observadas diferenças significativas entre os grupos populacionais.

Parks e Monson (2018) sugerem que entidades responsáveis pela curadoria de registros de pessoas desaparecidas e de indivíduos não identificados podem se beneficiar da implementação conjunta da tecnologia de reconhecimento facial e das aproximações faciais geradas por computador, como parte de uma estratégia investigativa abrangente para o caso de uso específico discutido em sua pesquisa (PARKS; MONSON, 2018).

- **Watching the watchers: bias and vulnerability in remote proctoring software - Burgess *et al.***

Na pesquisa de Burgess *et al.* (2022) é relatado que os educadores estão adotando rapidamente o uso de software de monitoramento remoto e exames para avaliações, devido à pandemia de COVID-19 e à crescente virtualização da educação. No entanto, o uso dessas soluções complexas levanta três preocupações principais: integridade do exame, imparcialidade dos procedimentos do exame e segurança e privacidade do examinado.

O texto trata de um estudo de caso que analisa 4 formas de monitoramento usadas em faculdades de direito nos Estados Unidos e em exames para licenciamento de advogados estaduais. Ao realizar engenharia reversa de um destes monitoramentos, descobrimos que, apesar das promessas de alta segurança, todas as medidas antifraude pode ser facilmente contornadas, representando riscos significativos para a segurança do usuário. Com base nessa análise, apresentaram recomendações para melhorar a integridade e a imparcialidade dos exames monitorados remotamente (BURGESS *et al*., 2022).

Para Burgess *et al.* (2022) essas práticas de monitoramento remoto têm um impacto negativo em grupos marginalizados. O viés embutido nos softwares de exame em relação ao tom de pele cria uma barreira invisível, resultando em taxas mais altas de identificação de minorias como suspeitas de fraude ou, inversamente, taxas substancialmente mais baixas de identificação. Isso perpetua o racismo estrutural e prejudica a representatividade desses grupos na profissão jurídica. Os autores recomendam que instituições educacionais e licenciadoras investiguem e realizem pesquisas para prevenir a discriminação nos exames.

A privacidade e a ética também são preocupações importantes. O software de monitoramento possui recursos invasivos e esses recursos, normalmente associados a malware, levantam preocupações sobre a segurança e a privacidade do examinado. A imposição do software de monitoramento em um contexto educacional limita a capacidade dos estudantes de consentir e complica a dinâmica de confiança institucional. Recomendam que os educadores ofereçam alternativas razoáveis, como testes em hardware fornecido ou cópias impressas com monitoramento ao vivo, sempre que possível. Além disso, é fundamental fornecer suporte para a desinstalação adequada do software e informar os estudantes sobre os riscos envolvidos (BURGESS *et al*., 2022).

Diante das preocupações significativas com a justiça dos sistemas de reconhecimento facial, recomendam evitá-los sempre que possível. Quando seu uso for inevitável, é fundamental manter a revisão humana como parte central do processo, com a participação de revisores diversos para reduzir os preconceitos (BURGESS *et al*., 2022).

É necessário um diálogo aberto sobre as diferenças nas características faciais entre grupos raciais e considerar esses fatores na configuração dos sistemas, buscando reduzir a ocorrência de identificações falsas (BURGERSS *et al*., 2022).

A pesquisa de Kirillova *et al.* (2021) aborda a necessidade de atualizar as regulamentações legais para se adequarem ao ambiente digital moldado pela tecnologia da informação. Destaca-se a importância dos "direitos digitais" nas novas relações jurídicas nesse contexto, e menciona-se os esforços internacionais e nacionais para o reconhecimento e regulamentação desses direitos, citando exemplos de países como Itália, Nova Zelândia, França e Brasil.

- **I Don't Want Someone to Watch Me While I'm Working: Gendered Views of Facial Recognition Technology in Workplace Surveillance - STARK; STANHAUS; ANTHONY**

Pela sua parte Stark, Stanhaus e Anthony (2020) realizaram uma pesquisa sobre câmeras de reconhecimento facial e gênero no trabalho. Iniciam seu texto trazendo que a vigilância tem sido uma prática histórica, por poderosos atores na sociedade, como instituições religiosas, governos e corporações. No entanto, o avanço das tecnologias de informação e comunicação (TICs) e sua disseminação global têm possibilitado uma vigilância mais detalhada de grupos, atividades e espaços. Atualmente, quase todas as pessoas vivenciam algum tipo de vigilância em suas vidas diárias, desde o uso generalizado de câmeras nas ruas do Reino Unido até o monitoramento digital massivo realizado por governos e empresas de tecnologia.

A vigilância desempenha um papel fundamental no exercício do poder, especialmente no "governo privado" das empresas (ANDERSON, 2017). Desde os primeiros industriais, que usavam relógios e automação para controlar o tempo dos trabalhadores, até os empregadores modernos, que utilizam tecnologias digitais para monitorar o comportamento dos funcionários, a vigilância no local de trabalho tem sido uma prática estabelecida. Estima-se que cerca de 75% das empresas nos Estados Unidos monitorem as comunicações e atividades dos trabalhadores, afetando aproximadamente 27 milhões de funcionários em todo o mundo.

Embora a vigilância no local de trabalho seja frequentemente justificada com base na produtividade e segurança, ela também pode ter efeitos indesejados, como aumento da insatisfação no trabalho, rotatividade e resistência dos trabalhadores. Além disso, os efeitos da vigilância tendem a ser assimétricos, ampliando as desigualdades sociais existentes em relação a raça, classe e gênero. Em contextos já marcados por relações de poder sexistas e racistas, as tecnologias de vigilância tendem a agravar a desigualdade de gênero e racial. Por exemplo, as mulheres são cada vez mais monitoradas em espaços públicos e privados por meio de câmeras, sem que isso necessariamente as proteja contra assédio ou agressão. Embora as câmeras possam ver todos, as pessoas que monitoram as imagens selecionam o que observar.

Stark, Stanhaus e Anthony (2020) indicam que homens e mulheres têm percepções diferentes em relação à vigilância. No entanto, são necessárias mais evidências para compreender o impacto das tecnologias de vigilância em diferentes grupos, especialmente em grupos marginalizados e com menor status social. No survey conduzido pelo *Pew Research Center* para identificar se homens e mulheres têm atitudes diferentes em relação à vigilância no local de trabalho. Os resultados mostraram que as mulheres são significativamente menos propensas do que os homens a aprovar o uso de câmeras com tecnologia de reconhecimento facial no local de trabalho. Além disso, o estudo investigou se homens e mulheres têm visões diferentes sobre a privacidade e se essas atitudes mediavam as opiniões em relação à vigilância por câmeras. Em suma, a vigilância no local de trabalho é um fenômeno crescente impulsionado pelo avanço das tecnologias de informação e comunicação, apresentando desafios em termos de privacidade, desigualdade social e impacto nas atitudes e comportamentos dos trabalhadores (STARK; STANHAUS; ANTHONY, 2020).

- **Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy - Shore**

Para Shore (2022) a Tecnologia de Reconhecimento Facial (TRF ou FRT Facial Recognition Technology), uma forma de inteligência artificial, ganhou popularidade após os ataques de 11 de setembro de 2001, quando seu potencial para capturar terroristas e criminosos foi reconhecido. No entanto, seu uso tem sido criticado por viés e falta de precisão, especialmente contra grupos minoritários e pessoas jovens e de cor.

O texto recente de 2022 traz a luz que existem 23 leis nos Estados Unidos que

proíbem o uso da TRF até que suas consequências sejam melhor compreendidas. Diante do movimento legislativo e da possibilidade de regulamentação federal, é importante entender como a mídia influencia as preocupações com a privacidade e o apoio governamental às políticas restritivas de TRF. Um estudo realizado com estudantes universitários busca explorar suas percepções e desempenhar um papel importante no futuro da política de tecnologia (SHORE, 2022).

O estudo investigará as perspectivas da TRF em espaços públicos e privados, considerando que os estudantes universitários têm usado a tecnologia em contextos privados, como filtros de mídia social e desbloqueio de telefones. No entanto, espera-se que os participantes apoiem mais políticas proibitivas de TRF em espaços públicos em comparação com contextos privados (SHORE, 2022).

Foram conduzidos experimentos com 150 participantes, todos estudantes universitários entre 18 e 24 anos. Eles foram expostos a excertos de notícias abordando diferentes contextos públicos e privados de TRF e responderam a perguntas sobre suas preocupações com privacidade e apoio a políticas proibitivas de TRF. O estudo utilizou um design fatorial misto para controlar as diferenças individuais (SHORE, 2022).

- **Facial recognition systems in policing and racial disparities in arrests - Johnson *et al.***

Johnson et al. (2022), dissertam sobre como os sistemas de reconhecimento facial se tornaram cruciais para o controle de crimes nos Estados Unidos, desde a identificação de vítimas de tráfico humano até suspeitos de homicídio. A tecnologia de reconhecimento facial automatiza a detecção e identificação de rostos, comparando imagens capturadas com fotos digitais de diversas fontes, incluindo imagens de vigilância, fichas policiais e a internet. Em teoria, essa inovação impulsionada pela inteligência artificial deveria ajudar a facilitar a detecção de crimes e a captura de criminosos de maneira mais eficiente e justa.

> No entanto, apesar de suas promessas, as imprecisões relatadas do reconhecimento facial ao identificar grupos demográficos, aliadas à ameaça de automação do critério policial pelas tecnologias de IA, levantam questões sobre sua adequação para a aplicação da lei (JOHNSON et al., 2022, p. 1, tradução nossa).

O estudo mostra que o reconhecimento facial apresenta inconsistências ao

identificar pessoas não brancas e de pele mais escura, com maior probabilidade de identificações errôneas. Segundo Johnson et al. (2022) a falta de diversidade racial entre os programadores e nas imagens de treinamento contribui para essas disparidades. Além disso, a aplicação e interpretação dos resultados do reconhecimento facial ficam a cargo dos operadores, o que pode levar a decisões tendenciosas.

A polícia utiliza o reconhecimento facial de três maneiras principais: 1) consultas de reconhecimento facial no local para identificar pessoas paradas ou detidas, 2) busca investigativa de imagens de vídeo e 3) análise em tempo real de pessoas que passam por câmeras de vigilância. Em grande parte das operações policiais, são realizadas pesquisas de um-para-muitos para gerar uma lista de suspeitos em potencial. Se dados biométricos suficientes forem semelhantes, o software declara uma correspondência entre as imagens faciais. Geralmente, é produzida uma pontuação de similaridade, sendo que valores mais altos indicam uma maior probabilidade de uma correspondência positiva.

Os sistemas de reconhecimento facial podem fornecer correspondências precisas para identificar corretamente ou rejeitar positivamente uma correspondência. No entanto, nem sempre retornam resultados corretos. Em alguns casos, o reconhecimento facial pode erroneamente associar duas imagens diferentes, chamado de falso positivo. Alternativamente, um falso negativo indica a falha em associar a mesma pessoa em duas fotos diferentes. Ambos os tipos de erros têm consequências prejudiciais para a governança democrática. Falsos positivos podem levar a acusações falsas, resultando em tratamento de uma pessoa inocente como fugitiva (JOHNSON et al., 2022).

O reconhecimento facial também apresenta menor precisão ao lidar com jovens e pode levar a erros de identificação, o que agrava ainda mais as disparidades raciais já existentes nas prisões de jovens.

Neste estudo (JOHNSON et al., 2022) foi utilizado um método chamado "Regressão de Mínimos Quadrados Ordinários" para analisar o efeito do uso do Reconhecimento Facial em tempo real (FRT - Facial Recognition Technology) na taxa de prisões. Com o intuito de ver se o FRT estava relacionado ao número de prisões. Para fazer isso, eles compararam agências de polícia que usam o FRT com aquelas que não usam. No entanto, havia um problema. Às vezes, as agências que escolhem usar o FRT podem ser diferentes das que não o usam em outros aspectos, e isso poderia afetar os resultados. Para lidar com isso, os pesquisadores usaram uma

abordagem chamada "escore de propensão robusta". Essa abordagem ajuda a ajustar as diferenças iniciais entre as agências que usam o FRT e as que não usam, para que os resultados sejam mais precisos.

Para compensar o fato de que os algoritmos de reconhecimento facial não são representativos o suficiente e são treinados principalmente com fotos de homens caucasianos, o estudo fez ajustes nas contagens de prisões levando em consideração a proporção de residentes negros na cidade. Isso significa que eles levaram em conta a população de diferentes raças ao analisar as prisões, para que os resultados fossem mais justos. Também foi necessário fazer ajustes algoritmicos.

O estudo de Johnson et al. (2022) buscou controlar várias covariáveis na análise, como fatores relacionados às agências policiais (composição racial e de gênero, força policial, atividades de patrulha, investigações, chamadas de serviço, capacidade fiscal, profissionalização e políticas de policiamento tendencioso), medidas de crime ajustadas para níveis de criminalidade subjacentes e determinantes estruturais, incluindo população, composição racial, residentes imigrantes, composição de gênero, jovens, nível de educação, locatários e desvantagem econômica.

No entanto, é importante notar que os resultados desse estudo específico foram apresentados em termos de métodos e análises estatísticas utilizados, mas não foram mencionados resultados específicos das regressões ou efeitos do uso do FRT nas disparidades raciais nas taxas de prisão. Este estudo investigou se a adoção da tecnologia de reconhecimento facial pelas agências de aplicação da lei contribui para as disparidades raciais nas prisões. Foram utilizados dois modelos estatísticos: o modelo de tratamento ou propensão e o modelo de resultado (JOHNSON et al., 2022).

Foram realizadas análises estatísticas para avaliar o equilíbrio das covariáveis entre os grupos que adotaram e os que não adotaram o reconhecimento facial. Mesmo após a ponderação inicial com base no escore de propensão estimado, diferenças residuais significativas foram encontradas na distribuição das covariáveis iniciais. O modelo foi reespecificado e ajustes de covariáveis foram feitos para obter um melhor equilíbrio, mantendo a direção e a magnitude das estimativas iniciais do efeito médio do tratamento.

Os resultados da pesquisa de Johnson et al. (2022) mostraram que a adoção do reconhecimento facial está associada a um aumento nas disparidades raciais nas prisões. As agências que adotaram essa tecnologia apresentaram taxas de prisão mais altas para pessoas negras e taxas mais baixas para pessoas brancas, em comparação com aquelas que não adotaram o reconhecimento facial.

As agências que adotaram o reconhecimento facial tendem a servir jurisdições maiores, com residentes mais ricos e mais educados. Elas também são mais diversas racialmente, possuem mais recursos e câmeras de vigilância, acesso a bancos de dados de computadores em campo e suporte técnico. Além disso, essas agências registraram níveis mais baixos de crimes relatados e uma maior disparidade racial nas prisões.

Esses resultados ressaltam a necessidade de considerar as implicações das tecnologias de reconhecimento facial nas disparidades raciais e enfatizam a importância de abordar essas disparidades nas políticas e práticas de aplicação da lei. Este estudo investigou o uso do Reconhecimento Facial pela polícia e suas associações com as disparidades raciais nas prisões nos Estados Unidos. Os resultados revelaram que o uso dessa tecnologia contribuiu para aumentos nas disparidades de prisões entre pessoas brancas e negras. Os efeitos do reconhecimento facial foram significativamente positivos nas taxas de prisão de pessoas negras e negativos nas taxas de prisão de pessoas brancas, resultando em uma disparidade geral. Esses efeitos foram mais pronunciados nas prisões de adultos, sugerindo que elas são as principais impulsionadoras da disparidade (JOHNSON et al., 2022).

Os resultados podem ser explicados por vários fatores, incluindo o desequilíbrio na distribuição policial, a alta carga cognitiva enfrentada pelos policiais, os efeitos automatizados das tecnologias de IA nas decisões policiais e a intensificação da atividade de aplicação da lei associada a essas tecnologias. A distribuição policial desigual, particularmente em áreas urbanas economicamente desafiadas e com população predominantemente não branca, resulta em um maior encontro entre a polícia e pessoas negras. Isso pode levar a uma maior incidência de prisões desproporcionalmente direcionadas a esses grupos (JOHNSON et al., 2022).

Além disso, os desafios geográficos e as desigualdades estruturais podem afetar o desempenho do reconhecimento facial e outros instrumentos de controle de crime algorítmico. A exposição desigual às desigualdades sociais e ao racismo pode resultar em uma classificação mais alta de pessoas negras nas escalas de risco usadas por esses algoritmos. A carga cognitiva enfrentada pelos policiais, juntamente com o tempo limitado e a necessidade de tomar várias decisões simultaneamente, pode levar a atalhos cognitivos baseados em estereótipos raciais, influenciando a percepção e o monitoramento de indivíduos suspeitos (JOHNSON et al., 2022).

Há uma tendência humana a confiar excessivamente em algoritmos, mesmo quando há evidências contraditórias. Os policiais podem ser influenciados pelas

percepções compartilhadas sobre a superioridade da IA, confiando nas listas de suspeitos geradas pelo Reconhecimento Facial que se alinham com estereótipos raciais. Isso pode levar a perfis investigativos sem arbitragem adequada (JOHNSON et al., 2022).

O estudo de Johnson et al. (2022) destaca a relação entre o uso do Reconhecimento Facial pela polícia e as disparidades raciais nas prisões. Os resultados indicam que pessoas negras são policiadas de forma mais punitiva do que pessoas brancas quando se trata do uso dessa tecnologia. Isso pode resultar em distúrbios psicológicos e minar a legitimidade da polícia, levando os cidadãos a evitar o contato com as autoridades. O estudo reconhece algumas limitações e sugere pesquisas futuras, incluindo desenhos experimentais e consideração de fatores não observados. Ressalta-se a importância de considerar fatores estruturais, políticas e diretrizes governamentais ao implementar o Reconhecimento Facial, além de treinamento adequado e políticas de supervisão para os policiais.

- **Racial Bias in Customer Service: Evidence from Twitter - Gunarathne *et al.***

A pesquisa realizada por Gunarathne *et al.* (2022) aborda um tema até então não mencionado em nossa triagem: o viés racial. Identificar e relatar o viés racial é essencial para combater a discriminação racial na sociedade. Para isso, os autores argumentam que é necessário que membros da sociedade compartilhem suas experiências, enquanto os pesquisadores documentam evidências estatísticas desse viés racial. Essa abordagem é respaldada por estudos anteriores que documentaram exemplos de discriminação racial contra consumidores afro-americanos em diferentes contextos comerciais.

O estudo ressalta a existência de viés racial no mercado digital, distinguindo-o do viés encontrado em plataformas de compartilhamento entre pares (peer-to-peer). O viés em plataformas digitais P2P ocorre quando indivíduos atuam de forma independente, enquanto o viés B2C ocorre quando funcionários agem em nome de uma empresa e os clientes são afetados por esse viés (GUNARATHNE *et al*., 2022).

É de extrema importância combater o viés racial em plataformas digitais, a fim de garantir um tratamento igualitário aos consumidores e responsabilizar as empresas por práticas discriminatórias. No contexto de plataformas P2P, geralmente não há responsabilização das plataformas pelo comportamento discriminatório de seus

usuários, enquanto o viés B2C pode levar à responsabilização das empresas por ações discriminatórias de seus funcionários.

Como uma estratégia para minimizar o viés racial Gunarathne *et al.* (2022), sugerem a adaptação do software de atendimento ao cliente em redes sociais, ocultando as fotos de perfil dos clientes dos agentes de atendimento. Essa medida tem como objetivo evitar a influência visual e reduzir o preconceito racial no atendimento ao cliente nessas redes.

Estudos empíricos anteriores sobre discriminação racial do consumidor concentraram-se principalmente no viés B2C em ambientes off-line. Por exemplo, pesquisas anteriores mostraram evidências de discriminação racial na negociação de preços em concessionárias de automóveis, no aluguel de imóveis e em lojas de varejo. No entanto, à medida que as interações sociais e comerciais se tornam cada vez mais digitais, os pesquisadores começaram a investigar a detecção de preconceito racial em plataformas digitais.

Estudos recentes em que se basearam os autores examinaram o viés racial em plataformas online, como empréstimos entre pares, leilões de cartões de beisebol no eBay, compartilhamento de viagens (Uber, Lyft), hospedagem no Airbnb e financiamento coletivo no Kickstarter. Essas pesquisas constataram a presença de discriminação racial, como menor probabilidade de financiamento, tempos de espera mais longos, cancelamentos frequentes e menor aceitação de solicitações para minorias étnicas (GUNARATHNE *et al.*, 2022).

A pesquisa em questão aborda o viés racial no atendimento ao cliente nas redes sociais, com foco no Twitter. Os pesquisadores utilizaram um conjunto de dados com mais de 57.000 reclamações direcionadas às contas oficiais de sete grandes companhias aéreas dos EUA. Através do reconhecimento facial utilizando as fotos de perfil das redes sociais, eles identificaram grupos raciais e encontraram evidências de que clientes afro-americanos têm menos probabilidade de receber respostas das marcas em suas reclamações nas redes sociais, em comparação com clientes brancos de perfil semelhante.

Para fortalecer a validade do estudo, os autores realizaram um teste de falsificação, utilizando um método de aprendizado profundo para inferir atributos demográficos latentes dos usuários do Twitter a partir do texto. O teste confirmou que a detecção de preconceito racial estava fortemente relacionada à pista visual de rostos humanos nas fotos de perfil.

Os resultados da pesquisa mostraram que os clientes afro-americanos apresentaram aproximadamente 12% menos chances de receber uma resposta da companhia aérea em comparação com os clientes brancos. Esses resultados indicam a presença de viés racial no atendimento ao cliente no Twitter, com implicações significativas para a equidade no tratamento dos consumidores nas interações online. Com base nesses resultados, os pesquisadores sugerem a adaptação do software de atendimento ao cliente em redes sociais para ocultar as fotos de perfil dos clientes dos agentes de atendimento, a fim de reduzir o viés racial. Essas descobertas destacam a importância de estudar o viés racial em plataformas digitais e a necessidade de abordagens específicas para combater a discriminação online (GUNARATHNE *et al*., 2022).

- **Ethical dimensions of quantification - Espeland e Yung**

Os autores Espeland e Yung (2019) abordam em sua pesquisa a ética da quantificação e destacam três dimensões éticas relacionadas: poder, atenção e oportunidade. Exemplos contemporâneos são mencionados, incluindo classificações universitárias, classificação racial no censo dos EUA e algoritmos de reconhecimento facial. É ressaltada a importância de examinar suposições e preconceitos nos números, bem como o desenvolvimento desigual das fontes de dados. As consequências éticas da quantificação também são destacadas.

A criação de algoritmos de reconhecimento facial envolve processos de quantificação que podem introduzir vieses, especialmente relacionados a raça e gênero. Esses vieses são influenciados por uma série de fatores, incluindo o desenvolvimento de câmeras, a composição dos conjuntos de dados usados para treinar os algoritmos e a implementação dos algoritmos em contextos específicos. Esses algoritmos podem perpetuar preconceitos sociais, o que levou a pedidos de maior transparência e prestação de contas. No entanto, entender e contestar esses algoritmos é difícil, pois eles são frequentemente caixas-pretas complexas e de propriedade privada (ESPELAND; YUNG, 2019).

Os algoritmos de reconhecimento facial moldam a atenção, definindo indicadores e características a serem otimizados. No entanto, eles tendem a se concentrar em indicadores facilmente mensuráveis, excluindo formas mais complexas de dados qualitativos. Isso pode resultar em invisibilidade para aqueles que não são adequadamente representados pelos indicadores escolhidos (ESPELAND; YUNG, 2019).

A visibilidade é uma manifestação do poder e os números estão envolvidos em relações de poder. A vigilância e o controle são usos proeminentes dos números, refletindo os interesses dos poderosos. Os números também afetam a participação nas decisões e excluem conhecimento local. A medição atual não considera como as condições surgiram, resultando em viés e tomadas de decisão influenciadas (ESPELAND; YUNG, 2019).

Grupos de defesa cientes de que a representação política e a alocação de bem-estar social são jogos numéricos podem fazer lobby por mudanças na forma como são contados pelo censo. Quando integrados a rotina de policiamento preditivo, os algoritmos de reconhecimento facial que têm baixo desempenho em indivíduos de pele mais escura podem fortalecer as oportunidades das minorias de serem vigiadas e rastreadas (ESPELAND; YUNG, 2019).

Os números moldam a atenção e as oportunidades[10]. Eles tornam visíveis certos aspectos da realidade e estruturam o que é notado. No contexto universitário, os

[10] Trecho original: “Algorithms shape attention by defining a set of indicators to model and optimize and define a space of features to encode the model. And attention is often paid to indicators that are the easiest to measure, render quantitative, or for which data already exists. In the realm of educational learning analytics, for example, datafication has led to a form of reactivity, whereby the data produce the learners as much as the learners produce the data (Williamson, 2015). Thicker forms of qualitative data that are difficult to quantify are excluded. With biased sources of data, facial recognition algorithms render visible those who are adequately represented as target indicators and render invisible those who are not. For commercially available recognition systems, those who are invisible may simply become cases of uncorrected error unless explicitly addressed. Algorithms shape opportunities – in the case of facial recognition systems, the opportunity to be surveilled and tracked. In an age of data-driven policing, where big data analytics are seen as a solution to racially discriminatory practices (Davis et al., 2016), commercially available facial recognition systems appear to provide a promising corrective to discriminatory policing. However, given that facial recognition systems perform poorly for darker-skinned individuals, the fairness and effectiveness of this form of policing is dubious. The adoption of statistical software to incentivize police activity and mediate police–civilian interaction has created an environment receptive to the implementation of such systems (Ratcliffe, 2016). Yet it is unclear whether these technologies have made policing more effective, more efficient, and more equitable. For example, the use of predictive analytics in policing heightens surveillance in a positive feedback loop that may not only predict crime but also contribute to its future occurrence (Brayne, 2017). Minorities and individuals living in lower-income neighbourhoods have a higher probability of falling into these surveillance loops. The

rankings afetam a percepção das instituições e a competição, prejudicando a diversidade e o acesso à educação superior. O censo desempenha um papel importante na formação e visibilidade da identidade asiático-americana (ESPELAND; YUNG, 2019).

De acordo com a pesquisa de Espeland e Yung (2019), os algoritmos de reconhecimento facial são poderosos atores sociais que podem ser enviesados e discriminatórios. Eles afetam setores econômicos e devem ser responsabilizados. A criação desses algoritmos pode introduzir vieses relacionados a raça e gênero. Eles influenciam a atenção e moldam oportunidades, mas tendem a se concentrar em indicadores facilmente mensuráveis.

Em resumo, o texto explica que a quantificação algorítmica pode ter consequências éticas e moldar relações sociais. Os números podem facilitar mudanças no poder, afetar a visibilidade e criar relações de visibilidade e invisibilidade, podem impactar oportunidades previstas e imprevistas. É fundamental considerar a transparência, a prestação de contas e as implicações éticas ao desenvolver e implementar algoritmos de reconhecimento facial e outras formas de quantificação (ESPELAND; YUNG, 2019).

- **Facial Recognition in Multimodal Biometrics System for Finger Disabled Applicants - MAZLAN; HARUN; SULIMAN**

Mazlan, Harun e Suliman (2017) trazem luz à facilidade que seria usar o reconhecimento facial no caso de pessoas com deficiências nas mãos. Muitas agências governamentais em todo o mundo utilizam sistemas biométricos para governar, monitorar, controlar e gerenciar os dados dos cidadãos. A Malásia começou a utilizar o sistema biométrico para gerenciar os dados dos cidadãos desde 2001, por meio de sua agência governamental, o Jabatan Pendaftaran Negara (JPN) ou Departamento de Registro Nacional. O JPN é responsável por manter registros de todos os cidadãos malaios e emitir o cartão de identificação nacional chamado MyKad para os cidadãos malaios. O documento obrigatório para cidadãos com 12 anos de idade ou mais. Para

---

occasion for surveillance that algorithmic misidentification affords is unlikely to break these self-fulfilling digital prophecies, exacerbating inequalities in terms of who is surveilled and who is tracked.” (ESPELAND; YUNG, 2019).

gerenciar esse processo, o departamento atualmente utiliza o Sistema Automático de Identificação de Impressões Digitais. Para os candidatos de primeira viagem, é necessário a certidão de nascimento, ter suas impressões digitais registradas e tirar uma foto para serem registrados no departamento. Essas informações são então representadas no cartão de identificação, que, ao ser lido no leitor de cartões inteligentes, mostrará os detalhes mencionados anteriormente. Aqui a pesquisa ressalta que, em relação à privacidade dos dados, o uso de leitores de cartões inteligentes para extração de dados do cartão de identificação é regulamentado pelo governo e permitido apenas para agências governamentais específicas.

O processo simples de solicitação do cartão de identificação permite que a aprovação e a retirada do cartão estejam prontas em até duas horas. No entanto, o mesmo não pode ser aplicado aos cidadãos com problemas nas impressões digitais ou com deficiências nos dedos. Cidadãos com impressões digitais ilegíveis ou amputação de dedos/mãos são obrigados a fornecer relatórios policiais, relatórios médicos e documentos de comissão de juramentos para comprovar sua identidade. Esses documentos precisam ser revisados, certificados e aprovados pelo departamento, o que pode levar até três meses para ser concluído. Esse longo tempo de espera deixa muito a desejar e parece ser desfavorável para usuários com deficiências (MAZLAN;HARUN;SULIMAN, 2017).

O sistema biométrico utiliza características biométricas – como dados faciais, impressões digitais e muitas outras – que são integradas para a identificação. Vendo que o departamento de registros já possui dados faciais úteis, mas subutilizados, é visto como um potencial da aplicação do sistema biométrico no contexto do reconhecimento facial para verificar a identidade de uma pessoa. Isso ocorre porque o sistema biométrico multimodal tem uma taxa de precisão melhor, pode lidar com semelhanças entre classes e não universalidade, além de reduzir a falsificação e dados ruidosos. Mazlan, Harun e Suliman (2017) ainda trazem um estudo semelhante às suas preocupações que foi realizado no contexto da região de Mianmar, o qual mostrou resultados promissores de confiabilidade. No entanto, é preocupante entender se a biometria facial é realmente viável dentro do ambiente de identificação nacional. Com base nos resultados, foi constatado que a o reconhecimento facial apresenta uma taxa de precisão aceitável, com uma taxa de falsa aceitação e uma taxa de falsa rejeição dentro dos limites aceitáveis. A taxa de erro igual também se manteve dentro de uma faixa aceitável, indicando a precisão do sistema. O que sugere que a integração da biometria facial como parte de um sistema biométrico multimodal pode melhorar o

processo de verificação para indivíduos com deficiências nos dedos, facilitando a identificação dos mesmos (MAZLAN; HARUN; SULIMAN, 2017).

- **CNN based Face Recognition System for Patients with Down and William Syndrome - Setyati *et al*.**

Os textos coletados nesta triagem trazem inúmeras possibilidades de uso e a pesquisa de Setyati *et al*. (2021) nos apresenta uma aplicação relacionada a síndrome de Down e síndrome de Williams.

A síndrome de Down é também conhecida como trissomia, é uma condição genética que afeta muitas pessoas. A síndrome de Williams é um distúrbio hereditário que pode afetar qualquer pessoa desde o seu nascimento. Ela apresenta problemas de saúde física e cognitivos, como doenças cardiovasculares, atrasos no desenvolvimento e dificuldades de aprendizado. Isso é acompanhado por habilidades verbais excepcionais, um comportamento sociável e uma paixão pela música. A síndrome de Down e a síndrome de Williams são doenças genéticas, mas podem ser distinguidas pela estrutura do cromossomo 21. Além disso, a identificação dessas síndromes pode ser feita através do reconhecimento facial, observando características faciais específicas.

Portanto, o texto de Setyati *et al*. (2021) desenvolve arquiteturas de Redes Neurais Convolucionais (CNN - Convolutional Neural Network) para reconhecer a síndrome de Down e a síndrome de Williams usando uma abordagem de reconhecimento facial.

O estudo utilizou um total de 480 fotos faciais no estudo, sendo 390 imagens usadas para dados de treinamento e 90 imagens usadas para dados de teste. A classe de identificação é dividida em três categorias: síndrome de Down, síndrome de Williams e "normal[11]". Cada classe de paciente possui 160 fotos. Foi apresentado duas formas diferentes de reconhecimento facial, duas arquiteturas de CNN usando uma imagem em escala de cinza de 256x256 pixels. A primeira arquitetura de CNN possui 12 camadas, enquanto a segunda possui 15 camadas, sendo que a primeira apresentou uma precisão média de 91% e a segunda, de 89%. A primeira forma de reconhecimento mostrou-se mais precisa (SETYATI *et al*., 2021).

[11] "In this study, three categories of data were used: Down Syndrome, William Syndrome, and Normal. Input data or datasets, as well as test data, are retrieved via the website. The Down Syndrome, William Syndrome, and Normal classifications were created due to this research" (SETYATI *et al*., 2021, p.139).

- **Cloud-Based System for Identifying Vaccinated Individual - RAJ; TAJAMMUL**

Na pesquisa de Raj e Tajammul (2022), tratou sobre questões emergentes da situação da pandemia de Covid-19. Como várias instituições, faculdades, empresas, instalações de saúde e universidades, que passaram a exigir que apenas alunos vacinados ingressem em suas dependências, de acordo com as regulamentações governamentais da Índia. No entanto, verificar individualmente o status de vacinação de cada aluno demandaria muito tempo e exigiria um grande número de funcionários. Portanto, o objetivo de estudo de Raj e Tajammul (2022) foi fornecer à instituição um sistema automatizado que indique se o aluno foi vacinado ou não. Para isso, será utilizado um aplicativo da web que coletará informações sobre o status de imunização dos alunos e funcionários. Eles deverão fornecer seu nome, número de telefone, número de identificação e indicar se foram vacinados ou não. O sistema contará com uma etapa de reconhecimento facial usando uma câmera e um banco de dados do tipo MYSQL no Raspberry Pi. É necessário ter um sistema eficiente e relevante para autenticar e gerenciar os registros de comparecimento das pessoas em uma instituição ou empresa, verificando se elas foram vacinadas. Existem diferentes tipos de sistemas que podem ser utilizados, como um sistema baseado em métodos convencionais, um sistema baseado em verificações manuais ou um sistema automatizado.

A implementação de um sistema manual de verificação (SMV) pode ser complicada, pois exigiria que cada pessoa anotasse e salvasse seus registros de verificação de vacinação sempre que visitassem a instituição. Isso seria tedioso, demorado e propenso a erros humanos, comprometendo a precisão dos registros. Portanto, Raj e Tajammul (2022) sugeriram o uso de um sistema automatizado baseado no Reconhecimento Facial Humano (RFH) para identificar se uma pessoa foi vacinada ou não.

O sistema de Raj e Tajammul (2022) utiliza uma abordagem que se baseia nas características faciais e no brilho para reconhecer e autenticar as pessoas. Os dados do usuário são coletados por meio de uma interface e armazenados em um banco de dados. Em seguida, o reconhecimento facial é realizado usando recursos da Amazon Web Services (AWS), como o Amazon Rekognition. Se a pessoa for identificada como vacinada, ela receberá autorização para acessar o local e seu registro de entrada será registrado.

Com a implementação desse sistema, poderemos obter registros de

comparecimento precisos e eficientes, substituindo os métodos manuais. O uso do Reconhecimento Facial Humano facilita a identificação e autenticação das pessoas, garantindo a segurança e o controle de acesso com base na vacinação (RAJ; TAJAMMUL, 2022).

- **Face Detection and Face Recognition in Android Mobile Applications - DOSPINESCU; POPA**

Partindo de um ponto de vista de software Dospinescu e Popa (2016) falam sobre como o reconhecimento facial e a coleta de informações têm tido um impacto significativo em várias áreas. Inicialmente, os computadores começaram a demonstrar habilidades de reconhecimento facial no final da década de 1960, e desde então, os sistemas robustos de reconhecimento facial têm se mostrado cada vez mais úteis em diversos campos.

Esses sistemas são aplicados no combate ao terrorismo, no combate ao crime e na autenticação de usuários em espaços reais ou virtuais, visando melhorar a segurança. No entanto, a identificação precisa de uma pessoa a partir de uma fotografia ainda é um desafio complexo devido à diversidade dos rostos humanos e às várias condições em que podem ser encontrados, como expressões faciais, iluminação, maquiagem, óculos e outros fatores.

Dospinescu e Popa (2016), explicam que a precisão dos sistemas de reconhecimento facial pode ser prejudicada por variações nas condições mencionadas, especialmente quando se lida com grandes bancos de dados de pessoas. Isso tem sido uma das principais razões pelas quais esses sistemas ainda não são amplamente utilizados com confiança. Além da segurança, o reconhecimento facial também tem impacto no setor de marketing, pois a aparência visual é um dos principais canais de comunicação com os clientes. A capacidade de reconhecer e entender expressões faciais pode ajudar os profissionais de marketing a criar estratégias mais eficazes.

O processo de reconhecimento facial envolve várias etapas, como a captura da imagem, a detecção do rosto, a extração de características, a comparação dos modelos e a declaração da identidade. Para isso, são utilizadas técnicas matemáticas, como a Análise de Componentes Principais (PCA- Principal Component Analysis) e o Método do Histograma de Padrões Binários Locais (LBPH - Local Binary Patterns Histogram), que permitem a identificação e comparação das características faciais.

Existem diversas bibliotecas e ferramentas disponíveis para facilitar o processo

de reconhecimento facial, como OpenCV, Rekognition, CERT, FaceRect, Face++ e FaceReader. Essas bibliotecas oferecem recursos para detecção, reconhecimento e análise facial, utilizando tecnologias avançadas de visão computacional e mineração de dados.

Os resultados obtidos podem variar dependendo das condições de iluminação e da posição dos rostos na câmera. Geralmente, a detecção de rostos funciona de forma rápida e eficiente, enquanto o reconhecimento facial apresenta melhor desempenho quando há menos rostos na cena e as condições de iluminação são constantes.

Em resumo, o reconhecimento facial é uma área em constante desenvolvimento, com desafios complexos relacionados à diversidade dos rostos humanos e às condições variáveis. As técnicas matemáticas desempenham um papel crucial no processamento e análise das imagens, permitindo a identificação e comparação de características faciais para fins de reconhecimento. Essa tecnologia tem um grande potencial de aplicação em diversos setores, como educação, medicina, marketing, segurança internacional, transporte, governos, entre outros. Com avanços futuros, espera-se que os sistemas de reconhecimento facial possam operar em tempo real e em condições menos limitadas, expandindo ainda mais suas possibilidades de uso (DOSPINESCU; POPA, 2016).

- **A novel approach for verifying selective user identity attributes online using open banking APIs - Pete *et al.***

O artigo de Pete *et al*.(2022) trata sobre o uso de serviços financeiros de bancos, e como compartilhamos nossas informações com eles. Eles propõe uma solução para a verificação online de identidade em plataformas digitais, utilizando APIs bancárias abertas. A ideia seria verificar os atributos de identidade em tempo real, compartilhando apenas o status de verificação, em vez dos dados completos. Isso trará confiabilidade aos dados, maior liberdade e anonimato aos usuários da internet, além de reduzir a dependência das grandes empresas de tecnologia. A implementação envolve um aplicativo da web que autentica o usuário com senha e reconhecimento facial, verifica os dados nos bancos e compartilha os atributos de identidade necessários com o site externo (PETE *et al*., 2022).

Para o autor o uso de reconhecimento facial como autenticação de dois fatores é explicado, assim como possíveis melhorias e aplicações futuras. E visa garantir dados confiáveis, segurança e anonimato na verificação de identidade online nos app bancários (PETE *et al*., 2022).

- **Factor Analysis in Unconstrained Viola-Jones Face Detection: Brightness, Contrast, Focus Measure, Eyewear, Gender, and Occlusion - Jafek *et al.***

Em Jafek *et al.* (2018) descreve-se que os seres humanos têm habilidade natural para detectar e reconhecer rostos no ambiente ao seu redor. No entanto, compreender os elementos que tornam um rosto reconhecível é um desafio, e estudos sobre o cérebro humano têm revelado que a detecção de rostos depende da ativação de milhões de neurônios em seis regiões cerebrais distintas. Tanto o cérebro humano quanto as redes neurais artificiais precisam realizar intensos cálculos para executar essa tarefa. A detecção de rostos por meio de identificação de padrões de áreas claras e escuras em imagens tem sido eficaz, mas não é tão robusta quanto o reconhecimento facial humano.

O estudo de Jafek *et al.* (2018) teve como objetivo investigar o impacto de diversos fatores no reconhecimento facial em ambientes não cooperativos ou seja: janelas, clima nublado e na pesquisa especificamente o para-brisa de carro. Para isso, utilizou-se o algoritmo Viola-Jones para analisar seis fatores específicos: brilho, contraste, medida de foco, uso de óculos, gênero e oclusão. Todos esses fatores são informações coletadas do ambiente e da pessoa na imagem para o reconheciento facial.

Os resultados indicaram que a oclusão foi o fator que mais afetou negativamente a detecção facial, com uma redução de até 54% na taxa de detecção em casos mais graves. Por outro lado, o gênero e o uso de óculos tiveram pouco impacto na detecção facial, embora seja necessário um estudo mais aprofundado para determinar seu efeito no reconhecimento (JAFEK *et al.*, 2018).

Foi observado que a otimização adequada dos fatores de brilho, contraste, medida de foco e oclusão pode levar a um aumento significativo na taxa de detecção de rostos, chegando de 44% a 86% no conjunto de dados analisado (JAFEK *et al.*, 2018).

Com base nesses achados, Jafek *et al.* (2018) oferecem recomendações para otimizar as imagens utilizadas na detecção e reconhecimento facial. Isso inclui a otimização do brilho, contraste, medida de foco e minimização da oclusão por meio de escolhas adequadas de localização da câmera. Além disso, sugere-se a integração desses resultados com algoritmos existentes que podem remover óculos, restaurar pontos de referência faciais ocultos e normalizar problemas de brilho e contraste, com

potencial para aprimorar significativamente os métodos de detecção e reconhecimento de rostos.

Por fim, o estudo destaca a importância de compreender como esses fatores afetam a detecção facial, o que pode levar a uma melhor compreensão de seus efeitos no reconhecimento facial. Com uma detecção facial confiável e uma classificação precisa da qualidade da imagem, ajustes podem ser feitos para otimizar o processo de reconhecimento facial, como a remoção de óculos e a reconstrução de rostos ocultos. Isso permitiria o desenvolvimento de tecnologias de reconhecimento facial mais eficazes em ambientes diversos, contribuindo para uma análise automatizada de grandes conjuntos de dados e aumentando a confiança nas conclusões e inferências obtidas a partir desses dados (JAFEK *et al.* 2018).

4.3 CATEGORIZAÇÃO DA AMOSTRA

Nesta seção, apresentaremos as diferentes categorias dos efeitos identificados dos algoritmos de reconhecimento facial. Com o objetivo de facilitar a apresentação dos resultados, optamos por categorizar os impactos do reconhecimento facial aplicado na sociedade em cinco grupos distintos: 1-Vigilância e Privacidade; 2- Biblioteca e Arquivo; 3- Gênero e Raça; 4- Saúde; 5-Software. Se justifica a escolha das categorias, seguida por um quadro que detalha os efeitos e uma citação do artigo que justifica a inserção do artigo na categoria correspondente. Para uma leitura mais aprofundada, o leitor poderá localizar o texto nas referências ao final desta pesquisa.

4.3.1 Categoria 1 – Vigilância e Privacidade

A categoria Vigilância e Privacidade foi estabelecida devido à presença de uma identificação comum entre os textos fornecidos. No contexto do big data e dos dados pessoais, a vigilância é entendida como a prática ou sistema de observar, monitorar e supervisionar ativamente pessoas, grupos ou ambientes, com o objetivo de obter informações, prevenir ou detectar comportamentos indesejados, ameaças ou atividades suspeitas. Essa categoria abrange uma variedade ampla de contextos e abordagens, incluindo vigilância física, eletrônica, tecnológica e em massa.

Diversos agentes podem exercer vigilância, como governos, empresas, instituições de segurança e até mesmo indivíduos. A preocupação com a privacidade está intimamente ligada a essa vigilância e seus excessos, uma vez que a privacidade trata da forma como os dados coletados dos usuários são utilizados (ZUBOFF, 2020).

A vigilância pode ter diferentes motivações, como garantir a segurança, combater crimes, preservar a ordem social ou exercer controle e poder sobre determinados grupos ou indivíduos. Foucault (1994) explora como a vigilância se tornou um instrumento de poder disciplinar.

Nesse sentido, a categoria Vigilância e Privacidade mostra-se como um tema relevante e complexo, com implicações éticas, políticas e sociais significativas. Os artigos que compõem essa categoria compartilham o mesmo propósito ou a mesma preocupação: a vigilância como forma de proteção, preservação da privacidade ou controle da população.

Nos artigos de Mary et al. (2022) e Asmitha e Sunitha (2022), é discutido o uso do reconhecimento facial para o controle de presença de estudantes em diferentes contextos. Ambos os estudos destacam a eficiência e os benefícios dessa tecnologia para a monitorização da presença dos alunos. Mary et al. (2022) propõem um sistema de reconhecimento facial para monitorar a presença de estudantes em um dormitório, detectando saídas não autorizadas do campus. O sistema notifica os responsáveis por meio de SMS e registra as saídas dos estudantes em um histórico de dados, fornecendo assim um controle eficiente de presença.

Da mesma forma, Asmitha e Sunitha (2022) exploram o uso do reconhecimento facial para o monitoramento dos estudantes em sala de aula. Eles destacam a automação do registro de frequência por meio dessa tecnologia, o que agiliza o processo, reduz a carga de trabalho dos professores e fornece dados mais precisos. Além disso, o reconhecimento facial diminui a dependência de métodos manuais, aumenta a confiabilidade dos dados e elimina a possibilidade de fraude. Ambos os estudos também sugerem melhorias para a tecnologia de reconhecimento facial. Eles propõem aprimorar a precisão do algoritmo utilizado e estender o sistema para monitorar a participação contínua dos alunos ao longo das aulas. Outra sugestão é explorar a integração do reconhecimento facial com a análise de sentimentos, fornecendo informações valiosas sobre o estado emocional dos alunos durante as aulas e auxiliando os educadores na adaptação de suas abordagens de ensino.

Gros e Straub (2019), Brey (2004) e Isasi-Andrieu et al. (2012) se alinham às pesquisas mencionadas anteriormente, abordando questões relacionadas à vigilância, privacidade e ética no contexto do RF. Gros e Straub (2019) enfatizam a ampla adoção do reconhecimento facial em diferentes setores, como varejo, segurança e estudos sobre comportamento humano. No entanto, eles também apontam desafios associados à coleta de dados para o treinamento dos sistemas, incluindo problemas relacionados à

iluminação, obstruções e distorções.

Brey (2004) discute o uso do reconhecimento facial em aeroportos e sistemas de vigilância, colocando em destaque o debate sobre o equilíbrio entre privacidade e segurança. Por sua vez, Isasi-Andrieu et al. (2012) concentram-se no uso do reconhecimento facial para a vigilância online de adolescentes, com o objetivo de proteger sua segurança e privacidade nas redes sociais. Além disso, o estudo de Eneman *et al.* (2022) exploram o surgimento da "vigilância algorítmica" com o avanço da inteligência artificial e do aprendizado de máquina. Esse estudo ressalta as tensões entre segurança e privacidade decorrentes do uso do reconhecimento facial e outras tecnologias de vigilância.

A preocupação com a privacidade também é abordada no estudo de Liu, Yan e Hu (2021), que discute o uso do reconhecimento facial em pagamentos móveis e as questões relacionadas à proteção de informações pessoais.

No contexto das regulamentações e proteção dos direitos, o artigo de Barkane (2022) destaca o "AI Act" como um regulamento proposto para lidar com os riscos da inteligência artificial, incluindo o reconhecimento facial. O texto enfatiza a importância de uma abordagem baseada em direitos humanos na regulamentação dessas tecnologias. A preocupação com a coleta e o uso de dados é abordada no estudo de Van Noorden (2020), que destaca as questões éticas e de privacidade relacionadas às pesquisas de reconhecimento facial e a necessidade de restrições no uso de conjuntos de dados.

No texto de Wang e Zhang (2022), o reconhecimento facial é discutido como uma tecnologia biométrica que utiliza características faciais para identificação de indivíduos. Diversas aplicações são mencionadas, como verificação de identidade em sites, segurança em shoppings, análise de fluxo de passageiros e controle governamental. No entanto, o uso indevido dessa tecnologia levanta preocupações sobre privacidade e segurança. A pesquisa relata alguns casos em que ocorreram processos por violação de direitos pessoais que resultaram em multa imposta a instituição estatal do caso, que evidenciam os problemas decorrentes do uso inadequado. Regulamentações variam entre países, com abordagens restritivas nos Estados Unidos, proteção de dados na China e na União Europeia. Os autores destacam a importância de regular adequadamente a tecnologia desde o início para evitar dilemas éticos e desafios futuros, enfatizando a necessidade de abordar essas tecnologias de forma aberta e buscar soluções adequadas.

Kirillova *et al.* (2021) discutem a necessidade de atualizar as regulamentações

legais para lidar com o ambiente digital e tecnológico, incluindo a proteção dos direitos digitais no contexto do reconhecimento facial. Por fim, o estudo de Ayata *et al*. (2020) destaca a importância da segurança dos dados e privacidade no contexto do rápido aumento na quantidade de informações, e menciona o reconhecimento facial como uma tecnologia que combina inteligência artificial e segurança da informação.

No geral, esses estudos abordam dimensões do reconhecimento facial voltados para vigilância, privacidade e segurança, e destacam a importância de equilibrar esses aspectos para garantir o uso responsável e ético dessa tecnologia.

Quadro 3 – Citações que exemplificam a Categoria 1: Vigilância e Privacidade.

Citação	Autor
"Facial recognition is used in this paper to detect students in the classroom and track attendance. This paper also stores data in an excel sheet, but it must be maintained on weekly or monthly basis. A camera will be installed in the classroom, and each subject's attendance will be recorded."	Mary *et al.*, (2022, p. 2)
"A variety of techniques have been proposed for identification and classification. Neural networks are commonly used for this purpose. Facial and human data also suffers from numerous problems relating to subject state and collection. Thus, a variety of techniques for dealing with a wide number of issues, including lighting conditions, distortion, and occlusion, as well as having only limited training data and subjects' facial expressions, have been developed. One particular use of facial recognition is to identify an individual for security purposes. Recognition can be used to grant access or validate identit. When used for security applications, the system must be robust to attacks that may try to confuse or deny recognition capabilities."	(GROS; STRAU, 2019, p.1).
"The problem of error is mentioned repeatedly by opponents of facecams. This is the problem that with face recognition technology, incorrect matches can occur that cause innocent citizens to become subjected to harassment by police. Problems of error are not unique to facial recognition technology, but may occur with any database system that stores personal information […]"	(BREY, 2004, p. 104)
"Similarly, professors may use class attendance data to calculate the exact assessment score. Not only does this cut down on the amount of instructional time spent due to the participation procedures, but it's also critical for sessions with limited facial expression time. The positives of designing a platform using a facial recognition detector may boost attendance accuracy & cut the amount of fraud that sometimes occurs via human absenteeism management. This user can detect and supervise lecturer participation and students' exams visibly and realistically as the foundation for the administration of educational activities."	(ASMITHA; SUNITHA, 2022, p. 2)
Desde un punto de vista tecnológico, Gazela se basa en tres elementos	

principales: – Servicios de vigilancia: orientados a recabar la información publicada por el usuario, comprobando que está dentro del marco legal en cuanto a contenidos, permisos de publicación, etc. – Servicios de protección: para detectar y alertar si se ha publicado algo que pueda ser ofensivo para el usuario, notificándoselo al infractor. – Servicios de asesoramiento jurídico: información básica sobre cómo actuar ante determinadas situaciones que puedan darse en las redes sociales, como acoso, chantaje o *cyberbullying*	(ISASI-ANDRIEU *et al.*, 2012, p. 516)
"The concerns around video surveillance and privacy are real, but the manner in which surveillance is utilized often dictates the magnitude of those concerns. […] Pollitt (2011) opined that surveillance technologies shape differentiated models of citizenship, where all citizens are not treated the same but could be "(instantly) graded against a whole range of factors, as belonging to different levels of risks" (p. 385). […] Newell (2014) unpacks surveillance in terms of power structures and concludes surveillance supports our current power structures, but we should be aware that privacy may not be the appropriate response. "	(BROMBERG; CHARBONNEAU; SMITH, 2020, p. 2)
"The analysis focuses on the trade-offs in the use of facial recognition technology between enhancing public security and, at the same time, protecting the individual's right to privacy (Solove, 2006; Richards, 2013), forging logics of action that underpins the recognition of police surveillance as legitimate. […] Thus, the notions of technological affordances and legitimacy emerge as especially important here. Over the last two decades we have witnessed a convergence of earlier discreet surveillance technologies into a ubiquitous surveillance assemblage that operates by "abstracting human bodies from their territorial settings and separating them into a series of discrete flows [...] reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention" (Haggerty & Ericson, 2000, p. 606). […] This transformation of discreet surveillance technologies into a ubiquitous surveillance assemblage is strongly linked to privacy concerns, (Solove, 2006). This article analyses how regulatory conditions for maintaining privacy (Hildebrandt, 2020) depend on the interplay between the emergence of digital technologies affording an assemblage of surveillance practices (Lyon, 2018), and the institutional forces that condition the realization of those affordances."	(ENEMAN *et al.*, 2022, p. 221)
"From supermarkets, shopping malls, and vending machines to transportation, the facial recognition applications have been continually expanding. Meanwhile, as the biometric technology has been applied to payment scenarios, the previous privacy policy for mobile payments has been insufficient to deal with	

the new payment methods. While consumers may enjoy the convenience that the new technology brings, they may also be confronted with serious threats to their portrait rights, personality rights and property rights (Allen, 2019) […] **Privacy calculus** has been widely applied to explain the individual's decision as the result of weighing the costs and benefits of information disclosure (Laufer & Wolfe, 1977). It refers to an individual's evaluation of whether the benefits of information disclosure outweigh the risks of information disclosure (Culnan & Armstrong, 1999). This concept provides an explanation that personal information can be regarded as the economic value of the transaction, and individuals tend to compare competing elements according to the expected outcomes (Dinev et al., 2008; Xu et al., 2009). Among them, the two opposing concepts (costs and benefits) are conceptualized as two key variables, namely, the cost of losing personal privacy (perceived privacy risk) (Dinev & Hart, 2006) and the expected gain in a specific situation (perceived benefits) (Pentina et al., 2016)."	(LIU; YAN; HU, 2021, p. 2)
"The increasing use of AI biometric surveillance systems raises serious concerns as to fundamental rights. Remote biometric recognition is linked to deep interference with the right to privacy, including people's autonomy, their right to establish details of their identity and psychological integrity (Muller & Dignum, 2021). It negatively impacts freedom of expression, association and freedom of movement (EDPB & EDPS, 2021). Remote biometric identification and predictive tools may lead to discrimination, violate the values of equality and justice due to biased data sets and errors as well as undermine the rights to liberty and to a fair trial (OHCHR, 2021)."	(BARKANE; 2022, p. 150)
"Nature's survey also asked researchers whether they felt that facial-recognition research on vulnerable populations — such as refugees or minority groups that were under heavy surveillance — could be ethically questionable, even if scientists had gained informed consent. Overall, 71% agreed; some noted it might be impossible to determine whether consent from vulnerable populations was informed, making it potentially valueless. Some of those who disagreed, however, tried to draw a distinction between academic research and how facial recognition is used. The focus should be on condemning and restricting unethical applications of facial recognition, not on restricting research, they said."	(VAN NOORDEN; 2020, p. 358)
"Modern privacy scholarship began in 1890 (McClurg, 2007, p. 1875), and Samuel Warren and Louis Brandeis (1890) defined privacy as the "right to be let alone" (p. 193). According to them, this right is not absolute, and if a person exposes his privacy to the general public, or if the privacy involves the public or general interest, he will lose this right. However, as surveillance and camera technology became more widely	(WANG;ZHANG, 2022, p. 260)

available, this viewpoint was challenged (Rothenberg, 2000, p. 1158). In Daily Times Democrat v. Graham 2, the court in the US recognized the existence of privacy in public places. […] In contrast to commercial applications, the use of facial recognition technology in government social administration is likely to pose a greater threat to individual rights and freedoms."	
"When discussing the principles of protecting digital rights, one should consider the use of facial recognition technologies and the use of the resulting images of citizens and such images should also be reliably protected. Therefore, the principle of security of data obtained through facial recognition technologies needs to be enshrined in law as the principle is important. […] The authors identify the basic principles of protecting digital rights: the digital equality principle; the digital self-determination principle; the anonymous communication principle; the principle of confidentiality of private communications; the principle of privacy in the digital environment; the principle of secrecy of digital identification; the principle of security of data obtained through facial recognition technologies; the principle of erasure of digitalized personal information."	(KIRILLOVA *et al.*, 2021, p. 926)
"Along with the developments in artificial intelligence, many solutions (such as endpoint security, network security, password management, log management, e-mail security, system access controls) are offered in the field of information security. Advances in image processing, which is a common ground of the fields of artificial intelligence and information security bring along innovative solutions."	(AYATA *et al.*, 2020, p. 83)
"Our portrayal of how civil inattention becomes increasingly difcult to enact in data-rich environments strengthens recent calls to strictly regulate or even ban FR technology, contributing to these an additional and heretofore neglected dimension of the privacy problem raised by FR. Furthermore, our analysis may help to point out some directions, pending strict regulation or outright bans, in which coping strategies can be sought. Indeed, the crucial role of social norms and practices in preserving privacy in public suggests that prohibitive laws or other command-and-control based forms of regulation are likely insufcient to prevent the impact of disruptive technologies on social relations in public space, and that a signifcant means of addressing this disruption will have to come from social practices."	(SHARON; KOOPS, 2021, p. 341)

Fonte: Elaborado pela autora.

4.3.2 Categoria 2 - Bibliotecas e Arquivos

O reconhecimento facial tem sido amplamente utilizado como uma solução

eficaz para garantir a segurança e melhorar os serviços em bibliotecas e arquivos. No caso descrito por Brown-Syed e Owens (2011), o reconhecimento facial foi utilizado para identificar uma pessoa que estava vandalizando uma biblioteca em Boise, Idaho. As câmeras de segurança instaladas permitiram a identificação de um veículo suspeito, e por meio da análise das imagens e do reconhecimento facial, descobriu-se que a condutora era uma pessoa proibida de frequentar a biblioteca. Esse caso ressalta a importância do papel dos bibliotecários na preservação dos acervos e destaca a eficácia do reconhecimento facial como uma ferramenta de segurança.

A pesquisa de Havelka (2021) revelou que as bibliotecas têm enfrentado desafios relacionados à privacidade móvel, uma vez que os aplicativos móveis podem capturar informações pessoais sem o conhecimento do usuário. Nesse sentido, é fundamental que as bibliotecas e profissionais da área de biblioteconomia estejam envolvidos na educação sobre privacidade e nas adaptações às mudanças tecnológicas. O estudo também ressaltou a importância de aumentar a conscientização sobre questões de privacidade, incluindo tecnologias emergentes como o reconhecimento facial e a inteligência artificial.

No contexto de arquivos, o reconhecimento facial e de voz surgem como ferramentas promissoras para auxiliar na indexação temática e onomástica, conforme destacado por Caldera-Serrano e Zapico-Alonso (2009). Embora o reconhecimento facial tenha mostrado resultados precisos na identificação de pessoas em certas condições, ainda há desafios a serem superados, como mudanças físicas e posições diferentes nas imagens. A colaboração entre arquivistas e as redes de televisão é essencial para atualizar os bancos de dados e aprimorar os resultados em condições não controladas. Outro aspecto relevante é o uso de softwares de código aberto para identificação facial nas bibliotecas, como mencionado por Hahn (2012). Esses softwares permitem a substituição de scanners de código de barras por smartphones, agilizando o processo de identificação de usuários e registro de itens retirados. Essa implementação pode resultar em economia de custos para as bibliotecas, além de se adaptar às mudanças tecnológicas e oferecer uma experiência mais eficiente aos usuários.

Além disso, o reconhecimento facial também pode ser aplicado na gestão de coleções fotográficas arquivadas, como discutido por Banerjee e Anderson (2013). A identificação de pessoas nas imagens por meio do reconhecimento facial auxilia na organização e indexação das fotografias, melhorando o acesso e a pesquisa. A colaboração entre arquivistas e equipes de sistemas é fundamental para automatizar a

criação e coleta de metadados, garantindo a interpretação correta e considerações éticas.

Por fim, a implementação de soluções de Internet das Coisas (IoT) nas bibliotecas, como proposto por Upala e Wong (2019), pode trazer benefícios adicionais. O uso do reconhecimento facial como forma de autenticação para os usuários, juntamente com sensores para coletar informações sobre o uso das salas da biblioteca, permite melhorar a eficiência e a experiência do usuário. No entanto, é importante abordar questões de privacidade e aprimorar a tecnologia de reconhecimento facial para garantir um ambiente de biblioteca mais eficiente.

O estudo de Botez e Repanovici (2017) destaca a importância da segurança em bibliotecas, equilibrando o acesso aos materiais com a proteção adequada das coleções e a segurança dos usuários e funcionários. Pesquisas realizadas na Romênia e Moldávia revelaram que os bibliotecários estão dispostos a adotar sistemas de reconhecimento facial, considerando-os mais seguros do que o sistema RFID. A análise estatística mostrou uma correlação entre a preocupação dos bibliotecários com a segurança, a confiança na tecnologia de reconhecimento facial e a disposição em implementar tal sistema. Os resultados ressaltam a viabilidade e confiança na implementação de sistemas de reconhecimento facial como medida de segurança em bibliotecas.

A pesquisa de Mardiana, Muhammad e Mulyani (2021) propõe um sistema de registro de presença em bibliotecas que utiliza o algoritmo YOLOv5 para reconhecimento facial. Isso soluciona desafios na detecção visual de usuários, substituindo métodos tradicionais, como cartões RFID e códigos de barras, por tecnologia computacional avançada. O YOLOv5 permite o reconhecimento facial e o armazenamento dos dados, simplificando a gestão das bibliotecas. Essa abordagem automatizada oferece maior precisão e eficiência no registro de presença, beneficiando tanto bibliotecários quanto visitantes.

O artigo de Bradley (2022) aborda a realidade algorítmica da sociedade contemporânea, destacando questões relacionadas aos algoritmos, reconhecimento facial e o papel das bibliotecas nesse contexto. Ele ressalta a importância de políticas e regulamentações que considerem o viés nos conjuntos de aprendizado de máquina, os riscos de vigilância em cidades inteligentes e o uso do reconhecimento facial, assim como a tomada de decisões automatizadas pelo governo. O artigo discute a participação das bibliotecas nos desenvolvimentos regulatórios da IA, apresentando exemplos de aplicações consolidadas, como busca em bases de dados e acesso a

coleções, além de abordar a ética e a proteção de dados. Também são mencionadas preocupações sobre direitos humanos, vigilância e alfabetização algorítmica. Apesar disso, poucas declarações específicas sobre IA e ética foram feitas pela profissão de bibliotecário até o momento. O artigo enfatiza a importância das bibliotecas se envolverem nas discussões e regulamentações da IA, visto que elas têm desempenhado um papel ativo na formação das leis de direitos autorais e proteção de dados. O futuro da IA deve ser baseado em direitos, ética e transparência, e as bibliotecas têm a oportunidade de contribuir nesse processo. A regulamentação da IA pode impactar os serviços de biblioteca de maneiras ainda desconhecidas, assim como as leis de direitos autorais e proteção de dados já tiveram impacto positivo e negativo no ambiente digital.

Na pesquisa de Rao et al. (2018), o reconhecimento facial (RF) é uma abordagem biométrica que utiliza métodos automatizados para identificar rostos, sendo uma solução biométrica universal de fácil uso. O RF foi implementado com sucesso em sistemas de controle de presença estudantil e enfrenta problemas de acesso à biblioteca. Os bibliotecários também enfrentam dificuldades ao rastrear o histórico de empréstimo dos estudantes. O objetivo do artigo foi desenvolver um sistema de gerenciamento de biblioteca baseado em RF, chamado FRLMS, que identifica o rosto dos estudantes e mostra multas e registros relacionados à biblioteca. O RF é amplamente utilizado em várias aplicações, como controle de acesso, vigilância e verificação de identidade. O uso do RF na biblioteca solucionaria problemas como o uso de cartões falsos e roubados, substituindo-os pela autenticação facial. Os resultados do teste mostraram alta precisão do sistema, e o estudo concluiu que o FRLMS pode facilitar o acesso à biblioteca.

Quadro 4 – Citações que exemplificam a Categoria 2: Bibliotecas e Arquivos.

Citação	Autor
“Libraries have worked to stay ahead of how their patrons (and the public in general) interact with smartphones and other mobile devices, and this has changed the library’s role in society. Numerous articles, books, and conferences attest to this. The same can be said about libraries and privacy, since librarians and information scientists have also been at the center of privacy and information technology	(HAVELKA, 2021, p. 43)

debates. For example, the International Federation of Library Associations and Institutions (IFLA) endorsed its Statement on Privacy in the Library Environment at its 2014 annual meeting. It stated that "data protection and privacy protection should be included as a part of the media and information literacy training for library and information service users. This should include training on tools to use to protect their privacy."	
"The library's barcode scanners for scanning a patron ID may not be necessary, if a clerk can use a library smart phone in order to scan a patron's picture ID. The picture that is scanned will then do feature detection and patron recognition in order to charge out the patron's items"	(HAHN, 2012, p. 435)
"Authentication is an extension to a face recognition mechanism. The IoT framework offers access to the user using their face. So, user-verification is required to be able to successfully gain access. According to the authentication feature implementation, when an user appears in front of the system, the system authenticates the user through the face recognition process as discussed earlier but if the user was not recognized by facial recognition procedure, then an functionality is added for the administrator which allows him/her to register the user to the library database by using the LBPH algorithm as well as adding the user manually using SQLiteStudio database manager, else any random user access would be rejected. […] So immediately after the authentication procedure or registration procedure in case of new user, the smart library user is verified to gain access to the "Library room occupancy" IoT application over ThingSpeak channel"	(UPALA; WONG, 2019, p. 6)

“The camera originally installed had been incapable of resolving the numbers on license plates, so the library purchased a better one and positioned it to capture both plate numbers and the faces of drivers. The incidents continued. Staff were able to determine that they were occurring over the weekends, so they began narrowing the search. […] The surveillance eventually lead to the identification of a single vehicle. Examining the video, DeWalt tentatively identified the driver as someone who had been banned from the library two years earlier for harassing and threatening staff and other patrons. Repeated verbal warnings had had no effect, and the library had been forced to take more drastic measures. [...] Facial recognition and tagging software are another example of a powerful new networked technology that could have vast benefits to researchers and librarians and to law enforcement and intelligence gathering.”	(BROWN-SYED; OWENS, 2011, p. 120)
[…] the more librarians think the most appropriate biometric recognition system for the security of collections and individuals is facial recognition, the more they are willing to implement a facial recognition system, and vice versa. The hypothesis that librarians who believe that the most appropriate biometric recognition system for the security of collections and individuals is facial recognition would agree with the implementation of such a system in the library in which it operates is confirmed.	(BOTEZ; REPANOVICI, 2017, p. 17)
“Las tecnologías biométricas aún no están muy desarrolladas en la gestión de los archivos de televisión. No obstante parece oportuno reflexionar sobre la potencialidad que nos ofrece el reconocimiento automático de imágenes y de sonido, lo que nos podrá ayudar a realizar labores de indización temática y onomástica. […] El uso de estas tecnologías no es un futuro, sino una	(CALDERA-SERRANO; ZAPICO-ALONSO, 2009, p. 427)

realidad que puede ser afrontada por las televisiones. El reconocimiento facial y el de voz ayudarían a la indización automática, agilizando el trabajo de Figura 5. Identificación incorrecta: a la derecha foto mostrada al sistema; a la izquierda foto respuesta los documentalistas al llevar a cabo el análisis documental.”	
“Using facial recognition software in conjunction with creative approaches to automation offers intriguing possibilities for making social metadata a more reliable source of descriptive information. Staff and researchers alike sometimes recognize individuals who are not identified in photographs. […] Creating metadata for archival collections will never be an entirely automated process – the interpretation and organization of content as well as legal and ethical issues will always require an archivist’s judgment. While metadata for digital archival collections can not be entirely automated, our example illustrates that more of it can be automated than one might assume. This is a critical consideration for archives faced with large image backlogs requiring detailed item-level metadata. Archivists would be well-served to work with systems staff to identify ways in which metadata creation can be automated, giving archives staff time to focus on those areas where human judgment is most valuable.”	(BANERJEE; ANDERSON, 2013, p.1)
“Various kinds of research in the field of image processing, especially those related to face detection and face recognition, have been carried out. This research can be applied to help overcome problems that exist in libraries. Most of the librarian's works in libraries has been assisted by library automation systems [...] The Attendance System library pulls information from the Face recognition sub-system provided via a web	(MARDIANA; MUHAMMAD; MULYANI, 2021, p. 68)

service. The information available through the API is retrieved using JavaScript which is then displayed on the visitor identification sub-system. The information that has been processed and presented on the visitor identification sub-system can be seen [...]	
“The library profession will need to engage with a range of definitions and frames when implementing AI technologies in practice and influencing AI regulation.[…] While there are many positive applications of AI in libraries and research, there are also a range of concerns. Given the breadth of AI applications that affect daily life and the lack of transparency, it is unsurprising that debates to date about AI in the library and information profession have been extremely wide-ranging. These range from human rights and ethical dilemmas, concerns about state and private surveillance, the rise of smart cities and facial recognition, to questions about how people will develop algorithmic literacy (Bradley, 2019; Cox, 2020; Fister, 2020; Hernandez-Perez, 2019;IFLA FAIFE, 2020; Padilla, 2019). […] IFLA’s statement is one example that reflects both longstanding ethical values on intellectual freedom and privacy, while making space for further debate within the profession (IFLA FAIFE, 2020)”	(BRADLEY, 2022, p. 190)
“FR is a technology that is becoming more common nowadays as it provides an attractive solution for easier identification and verification. Thus, more functions and applications can be integrated into this system to cover all the requirements possible in a university environment. The current system will deny student access to the library due to overdue books. In the future, more rules will be added to enhance the security of the system.	(Rao et al., 2018, p. 122)

For example when the system scans the student's face, details will show on whether there's fines to pay due to overdue book returns. […] Librarians often face problems in keeping the library clean and a quiet place to study, this is due to some students not being able to follow the common library rules such as “no food allowed” or “keep your voice down”. Thus in the future, in the cloud storage there will be a set of rules recorded by the librarians for the students to follow, if the student is spotted violating these rules, the librarian can set a number of times for the repeated offences, if it exceeds that number, then the student will be banned from entering the library for a certain period of time.”	
Two of the larger national unidentified decedent repositories are the Federal Bureau of Investigation’s (FBI) National Crime Information Center (NCIC) Unidentified Persons (UP) File and the U. S. Department of Justice’s (DOJ) National Missing and Unidentified Persons System (NamUs). Both repositories maintain data bases containing the details of thousands of active unidentified decedent cases (approximately 8000 and 10,000, respectively). In addition to unidentified decedent records, these repositories also maintain missing persons’ cases, which are automatically cross-referenced for data similarities with the unidentified decedents’ records. Facial images, if available, are also included in both the missing and unidentified decedent repositories. The facial images in the missing persons’ records are typically provided by relatives, the department of motor vehicles, or local law enforcement agencies.	(PARKS;MONSON,2018,p.273)

Fonte: Elaborado pela autora.

4.3.3 Categoria 3 - Genêro e Raça

Here comes the story of the Hurricane
The man the authorities came to blame
For somethin' that he never done
Put in a prison cell
But one time he could'a been
The champion of the world

(DYLAN; LEVY, 1975)

A categorização de Gênero e Raça surgiu ao longo do desenvolvimento desta dissertação, evidenciando a necessidade de sua existência com base nos artigos coletados e descritos até o momento. Gênero e raça desempenham um papel crucial na vida das pessoas e na forma como são tratadas na sociedade.

Gênero é um conceito que abrange características socialmente construídas, comportamentais e culturais associadas aos papéis e expectativas atribuídos a homens e mulheres na sociedade. Trata-se de uma construção social que varia entre diferentes culturas e inclui diversas identidades, como homem, mulher, não binário, entre outras.

Por outro lado, raça é uma categoria social utilizada para classificar as pessoas com base em características físicas distintas, como cor da pele, textura do cabelo e traços faciais. Ao longo da história, a raça tem sido utilizada para justificar a discriminação e a opressão de grupos minorizados, assim como ocorre com a opressão de gênero. Essa forma de discriminação pode se manifestar de maneira sutil ou implícita, porém ambos os grupos (além de outros citados na introdução dessa dissertação) enfrentam desigualdades sociais presentes na sociedade de classes (DAVIS, 2022).

Os diversos estudos categorizados nesta subseção abordaram questões relacionadas ao reconhecimento facial, viés racial, gênero e ética, trazendo evidências sobre cada um desses temas como o estudo de Burgerss *et al*. (2022) que revela que o uso de software de monitoramento remoto e exames em educação levantam preocupações sobre a integridade do exame, a imparcialidade dos procedimentos e a segurança e privacidade dos examinados. Além disso, o estudo destaca o viés embutido nos softwares em relação à cor da pele, resultando em taxas desproporcionais de identificação de minorias como suspeitas de fraude. Essa situação prejudica a representatividade e perpetua o racismo estrutural. Recomenda-se que

instituições investiguem e previnam a discriminação nos exames, buscando alternativas e oferecendo suporte adequado aos estudantes.

No contexto do gênero e da vigilância no local de trabalho Stark, Stanhaus e Anthony (2020) destacam que a vigilância no local de trabalho, incluindo câmeras de reconhecimento facial, pode ampliar as desigualdades sociais existentes. O estudo aponta que as mulheres são mais monitoradas por câmeras, no entanto, isso não as protege contra o assédio. Uma descoberta importante é que as mulheres são menos propensas a aprovar o uso de câmeras com reconhecimento facial no ambiente de trabalho. Essa vigilância apresenta desafios em termos de privacidade, desigualdade social e impacto nas atitudes e comportamentos dos trabalhadores.

No estudo de Shore (2022), a Tecnologia de Reconhecimento Facial (TRF) é abordada em relação às preocupações éticas. O autor destaca que a TRF ganhou popularidade após os ataques de 11 de setembro de 2001, sendo reconhecida por seu potencial na captura de terroristas e criminosos. No entanto, seu uso tem sido alvo de críticas devido ao viés e à falta de precisão, especialmente contra grupos minoritários e pessoas jovens e de cor. A pesquisa realizada com estudantes universitários revela que os participantes tendem a apoiar mais políticas proibitivas de TRF em espaços públicos do que em contextos privados. Esses resultados fornecem insights sobre o impacto do enquadramento da TRF na mídia e contribuirão para a elaboração de mensagens mais eficazes, considerando as preocupações com privacidade e o apoio governamental às políticas restritivas de TRF.

Em relação ao reconhecimento facial e suas implicações na aplicação da lei, o estudo conduzido por Johnson *et al*. (2022) revela que o uso dessa tecnologia pela polícia nos Estados Unidos está associado a aumentos nas disparidades raciais nas prisões. O reconhecimento facial apresenta imprecisões ao identificar pessoas não brancas, devido à falta de diversidade racial entre os programadores e nas imagens de treinamento. As agências que adotaram o reconhecimento facial apresentaram taxas de prisão mais altas para pessoas negras e taxas mais baixas para pessoas brancas. Essas disparidades podem ser explicadas pelo desequilíbrio na distribuição policial, carga cognitiva enfrentada pelos policiais e efeitos automatizados das tecnologias de IA nas decisões policiais. Os resultados ressaltam a importância de abordar as implicações do reconhecimento facial nas políticas e práticas de aplicação da lei, considerando fatores estruturais e governamentais, treinamento adequado e supervisão policial.

A pesquisa conduzida por Gunarathne *et al.* (2022) concentra-se na existência de viés racial e discriminação em plataformas digitais, com foco no atendimento ao cliente no Twitter. Ao analisar mais de 57.000 reclamações direcionadas a grandes companhias aéreas dos EUA, os pesquisadores identificaram evidências de que clientes negros têm menos probabilidade de receber respostas das marcas em comparação com clientes brancos de perfil semelhante. Essa descoberta destaca a necessidade de combater o viés racial nessas plataformas e ressalta a importância de ocultar as fotos de perfil dos clientes dos agentes de atendimento como medida para reduzir o preconceito racial. Esses resultados evidenciam a discriminação racial presente nas interações online e reforçam a importância de abordagens específicas para promover a equidade e combater a discriminação em plataformas digitais.

Por fim, Espeland e Yung (2019) abordam as questões éticas relacionadas à quantificação algorítmica, com ênfase nos algoritmos de reconhecimento facial. Os autores destacam as dimensões éticas do poder, atenção e oportunidade, ressaltando a importância de examinar suposições e preconceitos nos números. A criação desses algoritmos pode introduzir vieses raciais e de gênero, perpetuando preconceitos sociais e levando a pedidos de transparência e prestação de contas. Os algoritmos também moldam a atenção, excluindo formas complexas de dados qualitativos, e podem influenciar o poder e as relações sociais. Os números têm autoridade e impacto nas decisões e instituições sociais, afetando a participação e excluindo conhecimento local. Além disso, os algoritmos de reconhecimento facial podem fortalecer a vigilância e o rastreamento de minorias. A quantificação algorítmica afeta a visibilidade, molda oportunidades e pode ter consequências éticas, exigindo transparência e consideração das implicações ao desenvolver e implementar tais algoritmos.

Esses estudos evidenciam a importância de combater o viés racial, promover a equidade de gênero e considerar os aspectos éticos ao aplicar o reconhecimento facial em qualquer área da sociedade. As pesquisas ressaltam a necessidade de políticas mais inclusivas, transparência, treinamento adequado e supervisão para garantir que o uso do reconhecimento facial seja realizado de maneira justa, ética e responsável.

Quadro 5 – Citação que exemplifica a Categoria 3: Gênero e Raça.

Citação	***Autor***
“We see significant variations in the performance of the ‘face-api.js’ classifiers depending on the race of the subject with some minority groups being disadvantaged in LFWA+ and VGGFace2 datasets. This	

suggests that the automated facial recognition system may be unfairly disadvantaging certain students based on their race by not allowing them to take their exam or by presenting their exam to a human proctor for review at a higher rate than other non-minority students in certain cases. Given the variability and bias in the facial recognition steps, we believe a human based verification model is a significantly fairer approach to insuring exam integrity.	(BURGERSS *et al.*, 2022, p. 12)
"Together with the quantitative findings that women are less accepting of workplace surveillance using cameras with facial recognition software, and that it is specifically women who do not want to be monitored at work who say that such surveillance is unacceptable, these qualitative findings indicate that women may have particular concerns about workplace surveillance. According to scholars like Zureik (2003), the unwanted male gaze often underlies concerns about workplace surveillance: "In the case of the workplace, surveillance and privacy are associated with authority structures, body representation and consequent sexual harassment and discrimination"	(STARK; STANHAUS; ANTHONY, 2020, p. 1083)
"Concern about safety and potential for harm has been previously linked to and cited as justification for policymaking (Keum et al., 2005). While more government intervention may imply less privacy in some circumstances, prohibitive policy against FRT would promote individual privacy and signal that privacy is a key value of the government. Thus, it would be significant to measure the privacy concerns in conjunction with support for prohibitive FRT policy. Research on social perception has found when news is framed in terms of a group, or thematically, the issue is perceived as less severe since it is collective (Gamson & Iyengar, 1992). As a result, people are less concerned about this type of messaging. Studies have shown that people view human beings as a coherent and unified psychological unit, causing them to be more concerned at the episodic than thematic level (Hamilton & Sherman, 1996; Susskind et al.,1999)"	(SHORE, 2022, p. 3)
"This novel study examined the association between police FRT deployment and racial differences in arrests across 1136 U.S. cities in 2016. Our findings revealed that police FRT use contributed to increases in B-W arrest disparities. Significant and positive FRT	

effects on Black arrest rates and negative effects on White rates underpinned our main disparity finding. We also observed more sizeable and significant impacts for adult arrests, indicating that FRT's relationship with adult rates primarily drives the overall disparity. […] Similar geographic challenges compromise other purportedly raceneutral algorithmic crime control instruments. With risk assessments, for example, uneven exposure to systemic inequities and racism, and not necessarily differential offending, makes Black persons more likely to score "higher" on risk scales (Eckhouse, Lum, Conti-Cook, & Ciccolini, 2019). That is, they often find themselves in higher-risk categories because many risk algorithms strongly weigh criminal history. And since police disproportionately concentrate in areas where minoritized people live, work, and play, Black and Hispanic persons, on average, have lengthier criminal records (Eckhouse et al., 2019; Katzenstein & Waller, 2015; Omori & Petersen, 2020; Smith & Holmes, 2003)."	(Johnson *et al*., 2022, p. 8)
"The empirical results provide evidence suggesting racial bias against African American customers in social media customer service. Given the particularly severe consequences of B2C racial bias, it is of vital importance that companies carefully examine the root causes of such bias so that they can take appropriate actions accordingly and promptly. Whether the bias is implicit or explicit, the company has the responsibility to be aware of the discriminatory aspects of behavior resulting from these biases (Holroyd 2015)."	(GUNARATHNE *et al.*, 2022, p. 53)
"Recent scholarship highlights how such powerful implicit biases can be both hardand soft-coded into computer vision. The 'sociotechnical assemblage' that results in the creation of facial recognition algorithms provides numerous pathways for quantified forms of bias to snowball, persist, and multiply. Bias is historically encoded in the development of cameras, where sensors and camera settings are typically tested on and optimized for lighter-skinned subjects (Roth, 2009). Here, poor dynamic range and illumination result in pictures that erase the contours and particularities of the faces of subjects with darker skin. […] Algorithms shape opportunities – in the case of facial recognition systems, the opportunity to be surveilled and tracked. In an age of	(ESPELAND; YUNG, 2019, p. 251)

data-driven policing, where big data analytics are seen as a solution to racially discriminatory practices (Davis et al., 2016)”	

Fonte: Elaborado pela autora.

4.3.4 Categoria 4 - Saúde

Durante a coleta e análise dos artigos, foi observada a ampla aplicação do reconhecimento facial na área da saúde, o que tornou necessária a criação da categoria Saúde. Essa tecnologia tem sido utilizada de diversas formas, como auxiliar no diagnóstico de síndromes, no controle de pandemias para a saúde pública e na melhoria da qualidade de vida de pessoas com deficiências. Por exemplo, a pesquisa realizada por Mazlan, Harun e Suliman (2017) destaca a viabilidade do uso do reconhecimento facial para indivíduos com deficiências nas mãos. Agências governamentais em todo o mundo utilizam sistemas biométricos para governar, monitorar e gerenciar os dados dos cidadãos. No entanto, cidadãos com problemas nas impressões digitais ou deficiências nos dedos enfrentam dificuldades, sendo necessário fornecer relatórios policiais, médicos e de comissão de juramentos para comprovar sua identidade, o que pode levar até três meses para ser concluído. A pesquisa sugere que a integração da biometria facial como parte de um sistema biométrico multimodal pode melhorar o processo de verificação, facilitando a identificação desses indivíduos.

A pesquisa de Setyati *et al.* (2021) compoem esta categoria pois traz analise sobre o reconhecimento facial aplicado às síndromes de Down e de Williams. As síndromes podem ser distinguidas pela estrutura do cromossomo 21 e características faciais específicas. Neste estudo foi utilizado redes neurais convolucionais (CNN) para reconhecimento facial, com duas arquiteturas diferentes. A primeira arquitetura alcançou uma precisão média de 91%, enquanto a segunda obteve 89%. A pesquisa demonstrou que o reconhecimento facial pode ser uma ferramenta precisa para identificar essas síndromes.

Raj e Tajammul (2022) aborda questões relacionadas à pandemia de Covid-19, especialmente no que diz respeito ao controle de vacinação e ao uso do reconhecimento facial. Instituições e empresas estão exigindo a comprovação de vacinação para acesso às suas dependências, mas verificar individualmente o status de vacinação demanda tempo e recursos. Para resolver esse problema, Raj e Tajammul (2022) propõem a implementação de um sistema automatizado baseado em reconhecimento facial. O sistema utiliza um aplicativo da web para coletar informações

sobre o status de imunização dos alunos e funcionários, que são armazenadas em um banco de dados.

Quadro 6 – Citações que exemplificam a Categoria 4: Saúde.

Citação	Autor
"The simple process of MyKad application would allow MyKad approval and collection to be ready within two hours. However, the same cannot be applied for citizens with problematic fingerprint or finger disabilities. Citizens with unreadable prints, or is a finger/hand amputee are required to provide police reports, medical reports, and documents from commissioner of oath to proof their identity. […] Multimodal biometrics system uses multiple biometrics characteristics such as facial data, fingerprint, iris and many more where these information are integrated for identification. Seeing that JPN AFIS has facial data which is useful but under-utilized, we wanted to demonstrate the viability of applying multimodal system in the context of facial recognition in verifying an individual."	(MAZLAN; HARUN; SULIMAN, 2017, p. 638)
"Cognitive problems, such as intellectual and developmental delays, learning disabilities, and speech disorders, are unique to Down syndrome. Down syndrome impairs the hippocampus, which is essential for memory and learning. People with Down Syndrome are more likely to have the following health problems: Thyroid disease, Leukemia, Obesity, Chronic Constipation, Sleep Apnea, Poor vision, Cataracts, Strabismus, Anemia, Congenital heart defects, and Hearing loss. Down syndrome and Williams syndrome can be diagnosed by detecting the face, or facial characteristics, such as picking up particular facial traits."	(SETYATI *et al.*, 2021, p. 139)
"With the help of Human Facial Recognition, our upcoming framework will identify the person and determine whether he or she has been vaccinated. If the individual has been vaccinated, the system will allow the individual and will also label the logging time in which the employee comes into to the office and for a student for their attendance (HMR). In most cases, this system featured an image of all of the employees/students who were involved in the HMR, regardless of whether they had been vaccinated or not. […]	(RAJ; TAJAMMUL, 2022, p. 350,356)

We successfully implemented a software system that will identify whether or not people have been vaccinated. Our paper demonstrates that it can help replace manual methods of identifying people with greater accuracy and efficiency. In this paper, we have some AWS features such as Aws rekognition, AWS S3 bucket Aws Lambda, Aws EC2 instance and Aws SES.”	

Fonte: Elaborado pela autora.

4.3.5 Categoria 5 - Software

A categoria denominada Software engloba artigos que abordam o reconhecimento facial e a ciência da informação em contextos relacionados ao desempenho do software. Um exemplo é o estudo de Dospinescu e Popa (2016), que se concentra nas melhorias de software para o reconhecimento facial. O estudo ressalta que o reconhecimento facial tem sido amplamente aplicado em diversas áreas, tais como segurança, combate ao crime e autenticação de usuários. Entretanto, a identificação precisa de indivíduos com base em fotografias e informações coletadas nas imagens ainda representa um desafio, em virtude da diversidade de características faciais humanas e das condições variáveis. Fatores como expressões faciais, iluminação, maquiagem e uso de óculos podem comprometer a precisão dos sistemas de reconhecimento facial. Além da segurança, o reconhecimento facial também tem impacto no setor de marketing, permitindo a formulação de estratégias mais eficazes. Em resumo, o reconhecimento facial é uma área em constante evolução, com potencial de aplicação em diversos setores, e espera-se que avanços futuros possibilitem sua utilização em tempo real e em condições menos restritivas.

No estudo de Pete *et al.* (2022), é apresentada uma solução inovadora para a verificação de identidade em plataformas digitais de serviços financeiros. A proposta envolve a utilização de APIs bancárias abertas para verificar os atributos de identidade em tempo real, compartilhando apenas o status de verificação, em vez dos dados completos. Isso traz benefícios significativos, como a confiabilidade dos dados, maior liberdade e anonimato para os usuários da internet, além de reduzir a dependência das grandes empresas de tecnologia. A implementação inclui um aplicativo da web que autentica o usuário por meio de senha e reconhecimento facial, verifica os dados nos bancos e compartilha apenas os atributos de identidade necessários com o site externo. O uso do reconhecimento facial como autenticação de dois fatores é discutido,

juntamente com melhorias e possíveis aplicações futuras. Em resumo, o objetivo do estudo é garantir a confiabilidade dos dados, a segurança e o anonimato na verificação de identidade online em aplicativos bancários.

O estudo realizado por Jafek *et al.* (2018) aborda o tema do reconhecimento facial e destaca os desafios envolvidos na detecção robusta de rostos em diversos ambientes. A pesquisa investigou seis fatores específicos que afetam o reconhecimento facial em imagens capturadas por máquinas, como brilho, contraste, medida de foco, uso de óculos, gênero e oclusão. Os resultados indicaram que a oclusão foi o fator que mais influenciou negativamente a detecção facial, enquanto o gênero e o uso de óculos tiveram um impacto mínimo. A otimização adequada desses fatores pode resultar em um aumento significativo na taxa de detecção de rostos. O estudo oferece recomendações para otimizar as imagens utilizadas no reconhecimento facial, visando melhorar a detecção e o reconhecimento de rostos em ambientes diversos. Essa otimização pode contribuir para a análise automatizada de grandes conjuntos de dados e aumentar a confiabilidade das conclusões obtidas a partir desses dados.

Quadro 7 – Citação que exemplifica a Categoria 5: Software.

Citação	Autor
"[…] But despite the amazing innovations and developments in which all take part, the extent of a person from a photograph by comparing it with other images previously saved in a database it is still problematic and a very complex topic. This is mainly due to the variety of human faces depending on the area and the different conditions in which they can be, such as camera performance, facial expressions, lighting, makeup, glasses and more. Most times, a very simple variation of these conditions affect the accuracy of the systems through which the facial recognition is performed, mainly when using highly populated databases. This is the main cause for facial recognition systems are not yet widely used. […] Face recognition systems used today works very well in limited circumstances, although they work well with frontal images and constant illumination. We can say that the majority of current face recognition algorithms fails in different conditions in which people need to use the idea of this technology. The next generation of facial	(DOSPINESCU; POPA, 2016, p. 20; 26)

recognition systems should recognize people in real time and in circumstances far less limited.	
“The app will ensure that you are above that age after accessing your birthdate in the bank database. The user will need to give prior access to the bank while utilizing the app services. To the problem of impersonation that exists, we propose to tackle it with two-factor authentication. Hackers can obtain codes and OTPs with access to users’ devices, so we use facial recognition to authenticate the user [3]. Every time the user needs our app to vouch for his identity to a third party using open banking APIs, we match his picture taken at the movement with the catalogue of that user’s picture present with the banks.”	Pete *et al.* (2022, p. 942)
“Our dataset contains a broad compilation of non-ideal factors for face detection. These results are important for a number of reasons. First, they help computer vision researchers understand which factors to consider when configuring cameras for noncooperative facial recognition. Second, they suggest how to optimize these factors for face detection and recognition. Third, they indicate the factors which should be taken into account when taking cooperative photos for use in facial databases. Fourth, they help guide which research areas (e.g., sunglasses removal, face reconstruction) researchers need to focus on in the near future. […] These results are promising, suggesting that even in noncooperative situations, camera location and internal parameters can be carefully chosen to allow for a high rate of face detection. Further work will be necessary to examine the effect of these factors on face recognition.”	Jafek *et al.* (2018, p. 1;11)

Fonte: Elaborado pela autora.

4.4 COMENTÁRIOS POR CATEGORIAS

A construção das categorias anteriormente desenvolvidas, baseou-se em artigos de períodicos científicos da área de biblioteconomia e ciência da informação (LIS) indexado em DOAJ; Dimensions, Lens e WOS e de acordo com a forma como foi abordado o reconhecimento facial nos estudos. Este desenvolvimento resultou em 5

categorias: **1-Vigilância e Privacidade; 2-Biblioteca e Arquivo; 3- Raça e Gênero; 4-Saúde; 5-Software**.

Na categoria 1 – Vigilância e Privacidade, aparecem artigos que abordam como tema central a coleta de informações e o uso dessas informações do reconhecimento facial com o objetivo de monitoramento e vigilância. Até que ponto que a vigilância contínua e por meio de câmeras de vídeo deixa de ser para segurança e pode se tornar uma ameaça aos dados pessoais, como as informações da face e do próprio corpo. Surge a preocupação da automatização das tecnologias de vigilância que alcançam um maior poder na sua capacidade de coletar, analisar, armazenar e compartilhar dados em grande escala. Isso resulta em um monitoramento em tempo real da localização dos cidadãos, tornando a vigilância onipresente. E são nesses pontos que os estudos da área de ciência da informação e os algoritmos de reconhecimento facial se intersectam. De acordo com a American Library Association (ALA), à medida que as tecnologias móveis são introduzidas em espaços públicos, surgem questionamentos. Assim como ocorreu quando as câmeras foram incorporadas aos telefones celulares, os drones também podem levantar preocupações semelhantes, especialmente à medida que se tornam mais avançados, autônomos, compactos e acessíveis. Eles têm o potencial de capturar imagens, documentar eventos e, se utilizados de maneira inadequada, invadir a privacidade de pessoas desprevenidas, como descrito em um texto que trata sobre regulamentação do uso. Percebemos uma diferença quando o autor comenta que na Suécia já ocorreram processos referentes ao uso de reconhecimento facial na sala de aula, como monitoramento de estudantes. Referente ao estudo de Mary et al., (2022) os autores relatam que a tecnologia tem como objetivo diminuir o trabalho humano e se tornar em algo mais eficiente. Dentro do sistema capitalista sabe-se que o objetivo real é gerar rendimentos, ou seja, menos funcionários, menos salários a serem pagos e maior margem de lucro.

Dentro dessa mesma categoria, outra pesquisa que se destaca por criticas levantadas a um estudo sobre reconhecimento facial, na qual foram treinados algoritmos para distinguir os rostos dos uigures, um grupo étnico predominantemente muçulmano na China, dos rostos de coreanos e tibetanos. O aspecto relevante aqui é que, para a realização da pesquisa, não foi solicitada a aprovação do conselho de ética para a coleta de informações, uma vez que um grupo étnico diferente seria estudado. Isso nos leva a um debate ético sobre pesquisas, coleta de informações e publicações, uma vez que esses assuntos são intrínsecos à área de ciência da informação devido ao seu envolvimento na publicação científica. Por fim, embora exista um uso frequente do

RF em aplicativos e ferramentas, há uma escassez de estudos abrangentes que avaliem sua eficácia. Portanto, os benefícios dessa abordagem ainda são considerados limitados.

No pesquisa de Bromberg, Charbonneau e Smith (2020) em que relatam o uso de câmeras corporais em uniformes policiais, apesar dos autores indicarem que o apoio público varia de acordo com a finalidade e contexto de uso, devemos lembrar que no Brasil de 2023 essa prática tem diminuído a letalidade no geral, e um número mais expressivo quando se fala de adolescentes de 15-19 anos e população negra, pois inibe as ações policiais ilegais o que pode levar a critica de setores conservadores.

> Após a adoção das câmeras corporais portáteis por alguns batalhões da Polícia Militar de São Paulo, o número de crianças e adolescentes mortos em intervenções de policiais militares em serviço caiu 66,3% em 2022, na comparação com 2019. A letalidade de negros caiu cerca de 64%, porém essa população continua sendo três vezes mais atingida em intervenções policiais (CRUZ, 2023).

É notoria a ligação entre Vigilância e Privacidade com a Ciência da Informação, mas o reconhecimento facial com relação a vigilância e privacidade pode ser melhor explorado, com poucos artigos que tenham abordado as teorias, técnicas e preocupações discutidas nesse contexto, tanto na área acadêmica quanto nas principais entidades relacionadas, dentro dos resultados encontrados nas bases pesquisadas nessa pesquisa. A Biblioteconomia e a Ciência da Informação são áreas de estudo que segundo a a ALA se baseiam em valores fundamentais que orientam sua prática. Dentre esses valores, a privacidade é um dos principais enfatizados no Manual de Política da ALA (American Library Association, 2017).

A privacidade é uma preocupação essencial para a ALA, pois reconhece a importância de proteger as informações pessoais, sigilo e a liberdade dos usuários de serviços de informação. Esse valor reflete a necessidade de garantir que as pessoas possam buscar, acessar e usar a informação sem medo de vigilância excessiva ou invasão de sua privacidade.

A Categoria 2 Biblioteca e Arquivo compreende artigos relacionados à área de Ciência da Informação que exploram o uso do reconhecimento facial na segurança do usuário e do acervo. Um exemplo é o caso em que o reconhecimento facial foi utilizado para identificar uma pessoa que danificou o acervo de uma biblioteca. Outros estudos enfatizam a importância da segurança em bibliotecas, equilibrando o acesso aos materiais com a proteção adequada das coleções, usuários e funcionários. Para solucionar problemas de acesso, como o uso de cartões falsos e roubados, eles

propõem substituí-los pelo reconhecimento facial.

Ambos estudos destacam o papel dos bibliotecários na preservação das coleções e na segurança das bibliotecas, mas com enfoques diferentes. Enquanto alguns autores enfatizam o papel dos profissionais bibliotecários, a importância de sua atuação e os desafios ao rastrear o histórico de empréstimos dos estudantes, propõem o uso do reconhecimento facial para aprimorar o controle de acesso à biblioteca e fornecer informações sobre multas e registros relacionados, com o objetivo de facilitar o acesso aos serviços da biblioteca. Outros destacam a disposição dos profissionais bibliotecários em adotar sistemas de reconhecimento facial para melhorar o controle de acesso, alguns até com o objetivo de "redução de custos", o que pode implicar no possível descarte deste profissional em atendimento presencial.

Em um dos estudos, surgiram dificuldades ao implementar a tecnologia de reconhecimento facial em bibliotecas, apesar de terem obtido êxito em sistemas de controle de presença estudantil. Além disso, outras pesquisas enfatizam as conexões com: ciência da informação, biblioteconomia e arquivologia no que diz respeito à gestão de coleções arquivadas e à criação de bases de dados. Ao abordar a gestão documental e os meios de comunicação, essas pesquisas destacaram os desafios enfrentados devido ao volume e à complexidade da informação audiovisual. Em ambos os casos, as tecnologias biométricas, como o reconhecimento facial, surgem como ferramentas promissoras para auxiliar na indexação de imagens e facilitar a busca e o acesso às informações.

No entanto, é importante considerar os impactos éticos e legais relacionados ao uso do reconhecimento facial. A American Library Association (ALA) e a International Federation of Library Associations and Institutions (IFLA) destacam a necessidade de preservar os valores fundamentais das bibliotecas, como liberdade intelectual, privacidade, igualdade de acesso e diversidade. Portanto, ao avaliar a implementação do reconhecimento facial, é essencial considerar esses princípios, pois o monitoramento e controle dos usuários podem infringir essas recomendações.

Além disso, pesquisadores abordaram questões relacionadas à privacidade, aplicativos móveis e algoritmos, ressaltando a importância de políticas e regulamentações que considerem o viés nos conjuntos de aprendizado de máquina, os riscos de vigilância e as tomadas de decisões automatizadas, e incluem a necessidade da participaçãom das bibliotecas neste processo.

Apesar das facilidades de automatização proporcionadas pelo RF, é citado em mais de um artigo a redução do contato entre bibliotecários e usuários como uma

questão relevante. No contexto brasileiro, onde a profissão de bibliotecário é pouco valorizada, essa questão ganha destaque e preocupa que a possibilidade de a IA substituir completamente os bibliotecários. É necessário fortalecer a luta pela valorização dos bibliotecários como profissionais essenciais na democratização do acesso à informação, resistindo à substituição completa do trabalho humano pela inteligência artificial com a falácia de eficiência X redução de custos.

Se propoem o encontro de um equilíbrio entre a segurança proporcionada pelo reconhecimento facial e a interação pessoal entre bibliotecários e usuários. Embora o RF possa ser útil no controle de acesso e no aprimoramento dos serviços de biblioteca, é crucial avaliar cuidadosamente seus impactos sobre a privacidade e a liberdade intelectual. A IFLA (2019) defende o direito à privacidade pessoal e ao anonimato dos usuários da biblioteca, destacando a importância de evitar a revelação da identidade dos usuários e dos materiais que eles utilizam. A privacidade e a vigilância em massa são questões amplamente discutidas e ameaçadoras, e corremos o risco de perder a privacidade se o reconhecimento facial se tornar uma prática comum e parte de nossa cultura dominante (IFLA, 2019).

Esta categoria, como era de esperar, é a que melhor representa a CI mais tradicional em sua intersecção com o reconhecimento facial ao considerar as mudanças tecnológicas nas bibliotecas, é fundamental preservar os princípios éticos fundamentais da profissão bibliotecária, em busca de um equilíbrio adequado entre automação e interação humana. Importante também considerar as implicações sociais e éticas da substituição dos trabalhadores bibliotecários pela inteligência artificial com base no corte de gastos ou custo-beneficio. A proteção da privacidade, qualidade de atendimento e a garantia dos direitos dos usuários devem ser prioridades nesse processo.

Por fim, a busca por soluções tecnológicas deve ser acompanhada de uma reflexão profunda sobre seus impactos sociais, éticos e políticos, com o objetivo de construir uma sociedade mais justa e igualitária.

A Categoria 3 - Raça e Gênero reune questões relacionadas ao reconhecimento facial, viés racial, gênero e ética. A ciência da informação está envolvida nesse contexto ao analisar como as informações são coletadas, processadas e utilizadas, e como isso pode afetar as pessoas, especialmente em termos de discriminação racial e de gênero. Por exemplo, o uso de tecnologias de RF em exames educacionais pode resultar em discriminação contra minorias, prejudicando a representatividade e perpetuando o racismo estrutural.

No contexto do gênero e da vigilância no local de trabalho, a vigilância com reconhecimento facial pode ampliar as desigualdades sociais existentes, pois as mulheres são mais monitoradas, mas isso não as protege contra o assédio. E ainda existe o risco do uso das imagens de monitoramento serem utilizadas com outro objetivo como o mercado pornografico, sem o consentimento das mulheres.

Quanto ao RF na aplicação da lei, o uso dessa tecnologia pela polícia está associado a aumentos nas disparidades raciais nas prisões, devido à imprecisão na identificação de pessoas não brancas. Além disso, a existência de viés racial e discriminação em plataformas digitais, como o atendimento ao cliente no Twitter, destaca a necessidade de combater o preconceito racial e adotar abordagens específicas para promover a equidade social. Os estudos enfatizam as questões éticas relacionadas aos algoritmos de reconhecimento facial, podem introduzir vieses já existentes e moldar oportunidades e poder nas decisões e instituições sociais.

Todas essas pesquisas ressaltam a importância de combater o viés racial, promover a equidade de gênero, contra misoginia, e considerar os aspectos éticos ao aplicar o reconhecimento facial em qualquer área da sociedade. Políticas mais inclusivas, transparência no uso dos dados, treinamento adequado e supervisão são essenciais para garantir o uso justo, ético e responsável dessa tecnologia. IFLA nos lembra que, as consequências da implementação de tecnologias de RF ganharam destaque com os recentes protestos em Hong Kong, mostrando como nossos rostos podem se tornar uma arma de perseguição, opressão ou processo. Respondendo à pressão pública, algumas cidades começaram a proibir o uso de software de reconhecimento facial por agências estaduais; San Francisco, Somerville e Oakland são as primeiras cidades dos Estados Unidos com uma lei reguladora sobre esse assunto (IFLA, 2019).

Esses sistemas geralmente são treinados em um número diferente de rostos de grupos específicos de pessoas com características faciais semelhantes (principalmente pessoas brancas), o que pode levar à falha no reconhecimento de pessoas em um ambiente mais diversificado e, de maneira legal, isso pode levar a possíveis erros de identificação que vincula pessoas a crimes que não cometeram. Este assunto envolve questões de raça, identidade de gênero e orientação sexual, o que o torna mais ameaçador e prejudicial, existem vários exemplos de como essa tecnologia está desenvolvendo um racismo automatizado (IFLA, 2019). Assim como a IFLA, a ciência da informação tem um compromisso com a democracia, os direitos humanos em defesa dos valores humanísticos. Visto os relatos dos artigos, salientamos aqui um dos

muitos motivos da importância da luta feminista e antirracista na sociedade, que a luta cresça e fortaleça por um mundo em que sejamos “socialmente iguais, humanamente diferentes e totalmente livres” (Rosa Luxemburgo).

Na Categoria 4 – Saúde, Durante a coleta e análise dos artigos, foi observada uma quantidade considerável, embora menor, de artigos relacionados à área da saúde. O RF tem se mostrado uma ferramenta importante, auxilia no diagnóstico de síndromes, no controle de pandemias para a saúde pública e na melhoria da qualidade de vida de pessoas com deficiências.

Um exemplo relevante é uma pesquisa que enfatiza a viabilidade do uso do reconhecimento facial para indivíduos com deficiências nas mãos. Agências governamentais em todo o mundo utilizam sistemas biométricos para governar, monitorar e gerenciar os dados dos cidadãos. No entanto, cidadãos com problemas nas impressões digitais ou deficiências nos dedos enfrentam dificuldades ao fornecer relatórios policiais, médicos e de comissão de juramentos para comprovar sua identidade. A pesquisa sugere que a integração do reconhecimento facial como parte de um sistema biométrico multimodal pode melhorar o processo de verificação, facilitando a identificação desses indivíduos.

Outro estudo aborda a relevância da ciência da informação em relação à pandemia de Covid-19 e ao controle de vacinação. Com a necessidade de comprovação de vacinação para acesso a instituições e empresas, verificar individualmente o status de vacinação demanda tempo e recursos consideráveis. Para resolver esse problema, os autores propõem a implementação de um sistema automatizado baseado em reconhecimento facial. Esse sistema utiliza um aplicativo da web para coletar informações sobre o status de imunização dos alunos e funcionários, que são armazenadas em um banco de dados. A ciência da informação desempenha um papel crucial na concepção e operação desse sistema, permitindo um processo eficiente e seguro de verificação de vacinação.

Durante a pandemia de Covid-19, houve um aumento na adoção de tecnologias invasivas nos locais de trabalho, como rastreadores de atividade e produtividade para monitorar funcionários remotos, câmeras infravermelhas para verificar temperaturas e aplicativos para rastrear a saúde dos funcionários e possíveis exposições a vírus. Essas medidas levantaram preocupações sobre a privacidade e a precariedade dos trabalhadores com salários mais baixos. A resposta à pandemia também trouxe à tona exemplos de ativismo dos trabalhadores. Funcionários de diferentes setores fizeram protestos em busca de melhores salários, proteção e benefícios, uma vez que suas

funções foram consideradas essenciais durante a crise. Diversos profissionais exigiram melhores condições de trabalho e salários mais justos.

Um progresso importante a ser destacado é o dos artigos relacionadas ao reconhecimento facial para o diagnóstico de síndromes. Essas pesquisas são distintas das medições faciais baseadas em noções raciais e criminais utilizadas no passado. Em vez disso, elas contribuem para uma identificação mais precisa de síndromes, utilizando traços cientificamente comprovados. Assim, a ciência da informação desempenha um papel fundamental na compreensão, coleta de informações e aplicação do reconhecimento facial na área da saúde. Suas contribuições são evidentes na rapidez e melhoria do diagnóstico de síndromes, no controle de pandemias e no fornecimento de soluções eficientes para problemas relacionados à identificação e verificação biométrica. A ALA em 2020 relatou que durante a pandemia de Covid-19, houve um aumento na adoção de tecnologias invasivas nos locais de trabalho, como rastreadores de atividade e produtividade para monitorar funcionários remotos, câmeras infravermelhas para verificar temperaturas e aplicativos para rastrear a saúde dos funcionários e possíveis exposições a vírus.

Essas medidas levantaram preocupações sobre a privacidade e a precariedade dos trabalhadores com salários mais baixos. A resposta à pandemia também trouxe à tona exemplos de ativismo dos trabalhadores. Funcionários da Amazon, Whole Foods, Instacart e outros setores fizeram protestos em busca de melhores salários, proteção e benefícios, uma vez que suas funções foram consideradas essenciais durante a crise. Zeladores, babás, balconistas de mercearias, servidores e entregadores têm exigido melhores condições de trabalho e salários mais justos. À medida que os locais de trabalho começam a reabrir, as ações dos empregadores para proteger os trabalhadores, ou a falta delas, estão sendo examinadas. Uma pesquisa do Shift Project revelou que mesmo em grandes empresas faltavam proteções básicas de segurança para os trabalhadores, o processo de apoio aos trabalhadores era lento (ALA, 2020).

Uma observação a ser destacada aqui é o progresso das pesquisas relacionadas ao RF para o diagnóstico de síndromes. Essas pesquisas estão distantes das medições faciais que Lombroso (2020) utilizava, que eram baseadas em noções raciais e criminais. Em vez disso, elas contribuem para uma identificação mais precisa de síndromes que possuem traços cientificamente comprovados. Assim, a ciência da informação e os algoritmos aplicados a saúde impactam na coleta das informações e aplicação do RF na área da saúde. Suas contribuições são evidentes devido a

excelência e rapidez em um diagnóstico de síndromes assertivo, no controle de pandemias e no fornecimento de soluções eficientes para problemas relacionados à identificação e verificação biométrica para pessoas com deficiências físicas.

Para finalizar, a Categoria 5 – Software, no contexto dos artigos mencionados, a Ciência da Informação está relacionada ao reconhecimento facial, porém de uma forma de aplicação prática da área e não de desenvolvimento. Os estudos destacam os desafios e as melhorias relacionadas ao desempenho do software de reconhecimento facial, considerando fatores como expressões faciais, iluminação, maquiagem, uso de óculos e oclusão.

A CI e a categoria de software se encontram na atuação da CI na organização e recuperação de informações relevantes para o RF. Isso inclui a gestão de grandes quantidades de dados, a análise de características faciais humanas, a melhoria da precisão dos sistemas de reconhecimento e a otimização das imagens para detecção e reconhecimento de rostos em ambientes diversos.

> Para que um fato, evento ou instância da realidade possa ser computado, é necessário que este objeto seja convertido em um formato passível de ser reconhecido e processado pelos computadores. Nas palavras de Mayer-Schonberger e Cukier (2013), tudo deve ser dataficado, e esse processo de conversão difere substancialmente da simples digitalização uma vez que os diversos parâmetro do objeto devem estar estratificados e disponíveis para operações computacionais e análises algorítmicas (LOTT; CIANCONI, 2018, p.).

Os estudos mencionados apresentam soluções inovadoras que utilizam tecnologias como APIs bancárias abertas e reconhecimento facial como uma forma de autenticação de dois fatores, visando garantir a confiabilidade dos dados e a segurança dos usuários.

Além disso, a CI também é relevante na discussão sobre a confiabilidade dos dados, a segurança e o anonimato na verificação de identidade online em aplicativos bancários. A CI desempenha um papel importante na pesquisa e no desenvolvimento de técnicas, métodos e soluções para aprimorar o reconhecimento facial, superar desafios e explorar novas aplicações em setores como segurança, combate ao crime, autenticação de usuários, marketing e serviços financeiros.

No contexto atual, há uma ampla discussão no campo da Ciência da Informação em torno de temas relacionados, destacam-se: a Pós-Verdade, a Desinformação, o Big Data, a Infodemia, a Ciência de Dados, a Mineração de Dados, a Inteligência Artificial, os Algoritmos e o Reconhecimento Facial. Esses temas estão cada vez mais relevantes

e despertam o interesse dos pesquisadores, estabelecendo conexões com questões sensíveis à sociedade, como democracia, acesso à informação, racismo, misoginia, entre outros assuntos importantes.

Essas questões tornaram-se indispensáveis para os profissionais da informação que atuam na comunidade científica, em instituições ou em organizações não governamentais (ONGs). Além disso, governos e gestores públicos e privados também reconhecem a importância desses temas e buscam compreender suas implicações. A análise e compreensão dessas no âmbito da Ciência da Informação contribuem para a formação de políticas e práticas mais informadas e éticas, visando promover o acesso à informação, a transparência, a igualdade e a preservação dos direitos individuais e coletivos.

5 CONSIDERAÇÕES FINAIS

A Inteligência Artificial e a Internet introduziram uma nova era tecnológica em que algoritmos coletam e analisam vastas quantidades de dados, criando um "meio informacional" que pode impactar em nossas escolhas. Nas mídias sociais, as recomendações personalizadas restringem as opções dos usuários, contribuindo para a polarização e empobrecimento do debate público. O surgimento do capitalismo de vigilância tornou os dados pessoais, incluindos dados biométricos, que são valiosos para as corporações, que os utilizam com o objetivo de obter lucro e tomar decisões sobre as pessoas, o que Dantas (2022) explica da informação como mercadoria.

A presente pesquisa teve como objetivo verificar como a literatura acadêmica em ciência da informação apreende a existência de efeitos sociais consequentes da aplicação de reconhecimento facial. Para isto identificamos as comunicações cientificas sobre RF na CI no Brasil e no âmbito internacional, nas quatro maiores bases indexadoras, tivemos como resultado 37 artigos que relacionavam os assuntos de estudo. Os trabalhos selecionados foram descritos na parte de caracterização em seguida foram construidas cinco categorias: a categoria "Vigilância e Privacidade" aborda a coleta e o uso de informações por meio do reconhecimento facial para fins de vigilância, levantando preocupações sobre a privacidade dos indivíduos. Os estudos discutem o uso de diferentes formas de vigilância e suas implicações éticas, políticas e sociais. Eles enfatizam a necessidade de regulamentação adequada para proteger a privacidade e os direitos das pessoas.

Na categoria "Biblioteca e Arquivo", o reconhecimento facial é explorado como uma ferramenta de segurança e melhoria dos serviços oferecidos em bibliotecas e arquivos. Os estudos destacam casos de uso bem-sucedido do reconhecimento facial para identificar infratores, melhorar a autenticação de usuário e facilidade de atendimento, e não necessidade de intereção com o profissional bibliotecário com o objetivo de “corte de custos” da biblioteca. Ou seja, será que estamos falando de uma substituição deste profissional na biblioteca por uma IA? Iasi (2023) nos lembra que Aristóteles já zombava da ideia de que, se os aparelhos conseguissem mover-se por si próprios, não haveria necessidade de escravos. Obviamente, ele usava esse absurdo como justificativa para a escravidão, com o argumento que ela era necessária e inerente (IASI, 2023). No caso das bibliotecas a automatização sem incluir a necessidade de bibliotecários além de demonstrar a desvalorização, o monitoramento do usuário vai em contra ao que prega os manuais e recomendações da IFLA e ALA.

Essas entidades, estão de acordo com o código de ética do profissional bibliotecário ao afirmar que a introdução de um sistema de reconhecimento facial, que visa "cortar custos" ao eliminar a interação com os bibliotecários, vai contra esses princípios éticos e pode resultar em um ambiente menos inclusivo e acolhedor para os usuários. A falta de interação humana e o monitoramento constante podem comprometer a privacidade e a liberdade intelectual dos usuários, algo que as organizações bibliotecárias procuram proteger.

Portanto, é essencial abordar essa questão com cautela, considerando os impactos sociais classistas e éticos envolvidos. A automação e o uso de tecnologias avançadas devem ser aplicados de forma a complementar e fortalecer o trabalho dos bibliotecários, em vez de substituí-los, garantindo que os valores fundamentais da igualdade de acesso à informação e do respeito à privacidade sejam preservados. E que as entidades da área sejam mais rigorosas nestas questões, promovam mais discussões relacionados ao RF nas bibliotecas e outros espaços de informação, pois apesar das recomendações pelo que foi verificado nas pesquisas a IA tem sido fortemente utilizada nas bibliotecas.

A categoria "Raça e Gênero" aborda as questões de viés racial e gênero relacionadas ao RF. Os estudos revelam preocupações com o viés embutido nos sistemas de reconhecimento facial, que resultam em disparidades raciais e de gênero. Também são discutidas as implicações éticas do uso do reconhecimento facial, e destacam a importância de políticas inclusivas e considerações éticas para promover a equidade. O resultado desta categoria demonstra que o uso de tecnologias de reconhecimento facial, em exames educacionais, pode resultar em discriminação contra pessoas negras e outros grupos minorizados. Isso afeta a representatividade e perpeta o racismo estrutural. Na aplicação da lei, há uma associação entre essa tecnologia e o aumento das disparidades raciais nas prisões, devido à imprecisão na identificação de pessoas não brancas. Davis (2022) diz que o surgimento do complexo industrial-prisional vem acompanhado de uma campanha ideológica para nos convencer de que a raça é um marcador de criminalidade, ou seja a figura de um criminoso sempre é um homem jovem e negro. E que além da população branca a própria população negra aprender a temer o homem negro (DAVIS, 2022, p. 32).

No contexto do gênero e da vigilância no local de trabalho, a vigilância com reconhecimento facial pode ampliar as desigualdades sociais existentes, pois as mulheres são mais monitoradas, embora isso não as proteja contra o assédio.

Os medos do monitoramento das câmeras são reflexos sociais das marcas do

patriarcado. Além disso, existe o risco de as imagens de monitoramento serem utilizadas para fins pornográficos sem o consentimento das mulheres. o que pode resultar em assédio moral e sexual, ao colocar trabalhadoras em situações humilhantes e constrangedoras. Estudos destacam questões éticas dos algoritmos de reconhecimento facial, que podem introduzir vieses e afetar as decisões e instituições sociais. É essencial combater o viés racial, promover a equidade de gênero e considerar os aspectos éticos ao aplicar essa tecnologia. Políticas inclusivas, transparência, treinamento adequado e supervisão são fundamentais para garantir um uso justo e responsável.

Na categoria "Saúde", o reconhecimento facial é aplicado no diagnóstico de síndromes, controle de pandemias e melhoria da qualidade de vida para pessas com deficiência. Os estudos demonstraram o uso viável do reconhecimento facial para pessoas com deficiências. Além disso o RF é uma ferramenta precisa para identificar síndromes específicas, também foi proposto como uma solução para o controle de vacinação durante a pandemia de Covid-19. A categoria "Software" agrupou estudos que abordaram melhorias e desafios relacionados ao reconhecimento facial em contextos de desempenho de software. Os resultados desta categoria destacaram a funcionalidade do RF e demonstraram, a necessidade de aprimorar a precisão do RF, especialmente em condições variáveis, e propuseram soluções inovadoras para a verificação de identidade em plataformas digitais.

De forma ampla essas categorias destacaram preocupações e avanços relacionados ao reconhecimento facial em diferentes contextos, como vigilância, segurança, ética, privacidade, serviços de informação (bibliotecas e arquivos), inclusão e desempenho do software. Os resultados dos artigos em geral ressaltam a necessidade de regulamentações adequadas, considerações éticas e uma abordagem baseada em direitos humanos para garantir o uso responsável e ético do reconhecimento facial.

Ainda com base nos resultados desta pesquisa, percebe-se que os pesquisadores têm, ainda que de forma inicial, um interesse na pesquisa de reconhecimento facial na área de ciência da informação. O objetivo principal da pesquisa foi fornecer à comunicação científica uma visão de como estão dispostas as pesquisas de reconhecimento facial na ciência da informação e servir como embasamento para a sociedade no uso dessa ferramenta. Dessa forma, o estudo busca ser uma fonte de informação que possa ser consultada e estudada ao buscar o papel da ciência da informação nos estudos de algoritmos de reconhecimento facial,

abrangendo diferentes aplicações e preocupações relacionadas aos profissionais da informação. Espera-se que esta pesquisa contribua para o protagonismo da área de ciência da informação no tema de algoritmos de reconhecimento facial.

Para pesquisas futuras, sugere-se ampliar o estudo e a publicação sobre reconhecimento facial e ciência da informação, uma vez que os artigos, e as entidades ALA e IFLA indicam a necessidade e a importância do bibliotecário e das bibliotecas no desenvolvimento de políticas para o reconhecimento facial. Portanto, tanto os pesquisadores quanto os usuários dos espaços e aplicativos que possuem reconhecimento facial precisam fazer uso dessa ferramenta de forma consciente das consequências, mesmo diante dos benefícios. Enquanto as políticas de uso de dados avançam na sociedade, é fundamental considerar os aspectos éticos e os direitos humanos para garantir o uso responsável e ético do reconhecimento facial.

REFERÊNCIAS

AMERICAN LIBRARY ASSOCIATION (ALA). **ALA Policy Manual**: Section B: positions and public policy statements. Chicago: ALA, 2017. Disponível em: https://www.ala.org/aboutala/governance/policymanual Acesso em: 01 de jul de 2023.

American Library Association (ALA). Facial Recognition. 2018. Disponível em:. http://www.ala.org/tools/future/trends/facialrecognition. Acesso em 10 de jul de 2023.

AMARAL, Fernando. **Introdução à Ciencia de Dados: mineração de dados e big data.** SL. Alta Books. 2016.

ARANALDE, Michel Maya**.** Reflexões sobre os sistemas categoriais de Aristóteles, Kant e Ranganathan. **Ciência da Informação**, v. 38, n. 1, 2009. Disponível em: http://revista.ibict.br/ciinf/article/view/1257/1435. Acesso em: 15 jun. 2021.

ASSANGE, Julian. **Quando o Google encontrou o Wikileaks.** São Paulo: Boitempo, 2015.

ASMITHA, Podapati; SUNITHA, Thella. Student Attendance using Face Recognition Technology. **2022 International Conference On Intelligent Controller And Computing For Smart Power (Iciccsp)**, [S.L.], p. 1-4, 21 jul. 2022. IEEE. Disponível em:. http://dx.doi.org/10.1109/iciccsp53532.2022.9862329 . Acesso em 25 de mai de 2023.

AVELINO, Rodolfo da Silva; CASSINO, João Francisco; SILVEIRA, Sérgio Amadeu da. Direitos Humanos, Inteligência Artificial e Privacidade. **Monções: revista de Relações Internacionais da UFGD**, Dourados, v.8, n.15, jan/jun 2019. Disponível em: https://ojs.ufgd.edu.br/index.php/moncoes/article/view/11546. Acesso em: 15 ago. 2021

BARBOSA, Mariana et al (org.). **Pós-verdade e fake news:** Reflexões sobre a guerra de narrativas. Rio de Janeiro: Cobogó, 2019.

BARKANE, Irena. Questioning the EU proposal for an Artificial Intelligence Act: the need for prohibitions and a stricter approach to biometric surveillance1. **Information Polity**, [S.L.], v. 27, n. 2, p. 147-162, 26 jul. 2022. Disponível em:. http://dx.doi.org/10.3233/ip-211524. Acesso em: 10 de jul de 2023.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Zahar, 2001.

BAUMAN, Zygmunt. **Vigilância Líquida.** Rio de Janeiro: Zahar, 2014.

BARDIN,Laurence. **Análise de conteúdo.** Lisboa, Portugal: Edição 70, 2010.

BANERJEE, Kyle; ANDERSON, Maija. Batch metadata assignment to archival photograph collections using facial recognition software. **The Code4Lib Journal.** [S.l.], p. 1-1. jul. 2013. Disponível em:. https://journal.code4lib.org/articles/8486 Acesso em: 09 de jul de 2023.

BEZERRA, Arthur Coelho. Vigilância e cultura algorítmica no novo regime global de mediação da informação. **Perspectivas em Ciência da Informação**, v. 22, n. 4, p. 68–

81, dez. 2017. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S141399362017000400068&lng=pt&tlng=pt. Acesso em: 01 set. 2019.

BEZERRA, Arthur Coelho; SCHNEIDER, Marco; PIMENTA, Ricardo M.; SALDANHA, Gustavo Silva. **IKritika:** Estudos críticos em informação. Rio de Janeiro: Garamond, 2019.

BEZERRA, Josenildo Soares; MAGNO, MadjaElayne da Silva Penha. Vigilância negra: O dispositivo de reconhecimento facial e a disciplinaridade dos corpos. **Novos Olhares**, v.9, n. 2, jul-dez 2020. Disponível em: https://www.revistas.usp.br/novosolhares/article/view/165698. Acesso em 15 ago. 2021.

BRADLEY, Fiona. Representation of Libraries in Artificial Intelligence Regulations and Implications for Ethics and Practice. **Journal Of The Australian Library And Information Association**, [S.L.], v. 71, n. 3, p. 189-200, 3 jul. 2022. Disponível em:. http://dx.doi.org/10.1080/24750158.2022.2101911. Acesso em: 10 de julho de 2023.

BREY, Philip. Ethical aspects of facial recognition systems in public places. **Journal Of Information, Communication And Ethics In Society**, [S.L.], v. 2, n. 2, p. 97-109, 31 maio 2004. Emerald. http://dx.doi.org/10.1108/14779960480000246.

BROWN-SYED, Christopher; OWENS, Brian M.. Roundup. **Library & Archival Security**, [S.L.], v. 24, n. 2, p. 119-128, jul. 2011. Informa UK Limited. http://dx.doi.org/10.1080/01960075.2011.606092.

BROMBERG, Daniel E.; CHARBONNEAU, Étienne; SMITH, Andrew. Public support for facial recognition via police body-worn cameras: findings from a list experiment. **Government Information Quarterly**, [S.L.], v. 37, n. 1, p. 101415, jan. 2020. Elsevier BV. Disponível em:. http://dx.doi.org/10.1016/j.giq.2019.101415 . Acesso em: 10 de jul de 2023.

BOTEZ, Andra Manuela; REPANOVICI, Angela. The importance of security for people and collections in libraries. **Revista Română de Biblioteconomie Şi Ştiinńa Informării**: Romanian Journal of Library and Information Science, [S.l.], v. 13, n. 1, p. 11-20, 2017. Disponível em:. https://www.researchgate.net/publication/319237827_The_importance_of_security_for_people_and_collections_in_libraries#:~:text=The%20security%20of%20collections%20and,if%20not%20impossible%2C%20to%20replace. Acesso em: 09 de jul de 2023.

BULLOCK, Joseph; LUENGO-OROZ, Miguel. Automated Speech Generation from UN General Assembly Statements: Mapping Risks in AI Generated Texts. **International Conference on Machine Learning AI for Social Good Workshop**, Long Beach, United States, 2019. Disponível em: https://arxiv.org/abs/1906.01946v1 Acesso em: 18 jun. 2023.

BURGESS, Ben *et al*. Watching the watchers: bias and vulnerability in remote proctoring software. **Arxiv**, [S.L.], v. 1, n. 1, p. 1-19, 06 maio 2022. Disponível em:. http://dx.doi.org/10.48550/ARXIV.2205.03009. Acesso em: 10 de jul de 2023.

CALDERA-SERRANO, Jorge; ZAPICO-ALONSO, Felipe. Identificación facial biométrica. **El Profesional de La Información**, [S.L.], v. 18, n. 4, p. 427, 8 ago. 2009.

Ediciones Profesionales de la Informacion SL. Disponível em: http://dx.doi.org/10.3145/epi.2009.jul.11.Acesso em 3 de jun de 2023.

CASTELLS, Manuel. **Fim de Milênio - A era da informação: economia, sociedade e cultura**. Vol. 3: Paz e terra. São Paulo, 2012. p. 412.

CRUZ, Elaine Patricia. Mortes de adolescentes por PMs caem com uso de câmera corporal em SP. **Agênciabrasil.** São Paulo, p. 1-1. 16 maio 2023.

CONCEIÇÃO, Valdir Silva; NUNES, Ednar Maria; ROCHA, Angela Machado. O reconhecimento facial como uma das vertentes da inteligência artificial (IA): um estudo de prospecção tecnológica. **Cadernos de Prospecção** – Salvador, v. 13, n. 3, p. 745-758, junho, 2020. Disponível em:https://periodicos.ufba.br/index.php/nit/article/view/32818 Acesso em 02 nov de 2020.

CONSOLE, Claudio; MIRANDA, Catarina Runa; AUGUSTO, Gustavo; FRISOLI, Antonio; ORVALHO, Verónica. Real-time Emotion Recognition: Novel Method for geometrical facial features extraction. **Proceedings of the 9th International Conference on Computer Vision Theory and Applications,**p. 378-385, 2014. Disponivel em: https://www.scitepress.org/Papers/2014/47389/pdf/index.html Acesso em 8 nov. 2021.

CONTIN, Alexandre Celioto; SIQUEIRA, Oniye Nashara; BARUFI, Renato Britto; LEHFELD, Lucas de Souza. As visões da Pandemia: drones, reconhecimento facial, vigilância e a mitigação da privacidade. **Revista Húmus**, v. 11, p. 551-569, 2021. Disponível em:http://www.periodicoseletronicos.ufma.br/index.php/revistahumus/article/view/15257 Acesso em 22 mai. 2021.

COSSETI, Melissa Cruz. O que é inteligência artificial? 2018. Disponível em:. https://bit.ly/2xH7seo . Acesso em: 27 jun. 2020.

DAVIS, Angela. **O sentido de liberdade: e outros diálogos difíceis**. Editora Boitempo. São Paulo, 2022. p.158.

DREXLER. Jorge; EREZ, Noga. **¡Oh, Algoritmo!**. Álbum: Tinta y Tiempo. Sony Music Entertainment España, S.L., 2022.

DOSPINESCU, Octavian; POPA, Iulian. Face Detection and Face Recognition in Android Mobile Applications. **Informatica Economica**, [S.L.], v. 20, n. 1/2016, p. 20-28, 30 mar. 2016. Bucharest University of Economic Studies. Disponível em:. http://dx.doi.org/10.12948/issn14531305/20.1.2016.02. Acesso em 09 de jul de 2023.

DYLAN, Bob; LEVY, Jacques. **Hurricane**. Columbia, 1975. Disponível em: https://www.youtube.com/watch?v=bpZvg_FjL3Q Acesso em: 10 jul. 2023.

EL EFECTO. **Trovoada**. Rio de Janeiro, 2018. Disponível em: https://www.youtube.com/watch?v=fWKII3AjFXg Acesso em: 09 jul. 2023.

EMPOLI, Giuliano da. **Os engenheiros do caos.** Editora Vestígio. São Paulo, 2020. P. 190.

ENEMAN, Marie *et al*. The sensitive nature of facial recognition: tensions between the swedish police and regulatory authorities1. **Information Polity**, [S.L.], v. 27, n. 2, p. 219-232, 26 jul. 2022. IOS Press. Disponível em:. http://dx.doi.org/10.3233/ip-211538. Acesso em: 10 de jul de 2023.

ESPELAND, Wendy; YUNG, Vincent. Ethical dimensions of quantification. **Social Science Information**, [S.L.], v. 58, n. 2, p. 238-260, 23 maio 2019. SAGE Publications. Disponível em:. http://dx.doi.org/10.1177/0539018419851045. Acesso em: 10 de jul de 2023.

ENTLER, Ronaldo. A fisionomia genérica do crime. **ZUM Revista de fotografia**. 2021. Disponível em: https://revistazum.com.br/colunistas/a-fisionomia-generica-do-crime/. Acesso em: 1 fev 2023.

EVANS, Dave. A Internet das Coisas Como a próxima evolução da Internet está mudando tudo. **Cisco Internet Business Solutions Group (IBSG)**. Abril de 2011. Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf Acesso em: 18 jun. 2023.

FIGLIUZZI, Renan Silva. **Inteligência artificial:** um novo paradigma tecnológico?2018. 47f. Monografia (Bacharel em Economia) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018. Disponível em: https://bit.ly/2W7pQq3 . Acesso em: 20 mai. 2021.

FREITAS, Marcos Cezar de. Economia e educação: a contribuição de Álvaro Vieira Pinto para o estudo histórico da tecnologia. **Revista Brasileira de Educação**, v. 11 n. 31 jan./abr. 2006. Disponível em: https://www.scielo.br/j/rbedu/a/hZP6xKjjyFPjFTMkskKpXbc/?format=pdf&lang=pt Acesso em: 19 jun. 2023.

Geledes. **A ðNICA SEMELHANÇA.** [S.l.]: Portal Geledes, 2021. Disponível em: https://www.geledes.org.br/a-unica-semelhanca. Acesso em: 30 nov. 2021.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007.

GONZÁLEZ DE GÓMEZ, M. N. Novos cenários políticos para a informação. **Ciência da informação**, Brasília, v. 31, n. 1, p. 27-40, jan/abr 2002. Disponível em: http://revista.ibict.br/ciinf/article/view/975 . Acesso em: 03/09/2019

GONZÁLEZ DE GÓMEZ, M. N. O caráter seletivo das ações de informação. Informare, Rio de Janeiro, v. 5, n. 2, p. 7-31, 1999. **Perspectivas em Ciência da Informação**, v.22, n.4, p.68-81, out./dez. 2017. Disponível em:http://www.brapci.inf.br/_repositorio/2010/03/pdf_6d5abbf137_0008552.pdf Acesso em: 07/09/2019

GONZÁLEZ DE GÓMEZ, Maria Nélida. Novos cenários políticos para a informação. **Ciência da informação**, Brasília, v. 31, n. 1, p. 27-40, jan/abr 2002. Disponível em: http://revista.ibict.br/ciinf/article/view/975 . Acesso em: 03 set.2020.

GROS, Collin; STRAUB, Jeremy. A Dataset for Comparing Mirrored and Non-Mirrored

Male Bust Images for Facial Recognition. **Data**, [S.L.], v. 4, n. 1, p. 26, 8 fev. 2019. MDPI AG. Disponível em:. http://dx.doi.org/10.3390/data4010026 . Acesso em: 10 de jul de 2023.

GUNARATHNE, Priyanga *et al*. Racial Bias in Customer Service: evidence from twitter. **Information Systems Research**, [S.L.], v. 33, n. 1, p. 43-54, mar. 2022. Disponível em:. http://dx.doi.org/10.1287/isre.2021.1058. Acesso em: 10 de jul de 2023.

HAHN, Jim. Mobile augmented reality applications for library services. **New Library World**, [S.L.], v. 113, n. 9/10, p. 429-438, 29 set. 2012. Emerald. http://dx.doi.org/10.1108/03074801211273902.

HAN, Byung-Chul. **Sociedade da transparência.** Petrópolis/RJ. Vozes, 2017.

HAVELKA, Stefanie. Typologies of Mobile Privacy Behavior and Attitude: A Case Study Comparing German and American Library and Information Science Students. **The Serials Librarian**, 2021. 81:1, 42-58, Disponível em: https://doi.org/10.1080/0361526X.2021.1875961 Acesso em: 07 jul. 2023.

IASI, Mauro Luis. IAgora: inteligência artificial e alienação. **Blog da Boitempo**. 12/05/2023. Disponível em: https://blogdaboitempo.com.br/2023/05/12/iagora-inteligencia-artificial-e-alienacao/ Acesso em: 19 jun. 2023.

ISASI-ANDRIEU, A., LOPEZ-CARRERA, A.,RUIZ- IBANEZ. Gazela: social networks digital advisor for teenagers. **Profesional de la Informacion**, Vol. 21, No. 5, Sept.-Oct. 2012. Disponível em: https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/epi.2012.sep.11 . Acesso em 9 de jun de 2023.

IFLA. Riding the Waves or Caught in the Tide? Navigating the Evolving Information Environment. **Insights from the IFLA Trend Report**, 2013, para. 5.

IFLA. Facial Recognition, Libraries, And Intellectual Freedom. 2019. Disponível em: https://blogs.ifla.org/faife/2019/08/19/facial-recognition-libraries-and-intellectual-freedom/ **. Acesso em: 10 de jul de 2023.**

JAFEK, Benjamin; HENDERSHOTT, John; EICHOLTZ, Matthew; SANTOS-VILLALOBOS, Hector J.; JOHNSON, Christi; BOLME, David. Factor analysis in automated face detection: gender, occlusion, eyewear, brightness, contrast, and focus measure. **Disruptive Technologies In Information Sciences**, [S.L.], p. 1-13, 9 maio 2018. SPIE. Disponível em:. http://dx.doi.org/10.1117/12.2311281. Acesso em 10 de jul de 2023.

JOHNSON, Thaddeus L. *et al*. Facial recognition systems in policing and racial disparities in arrests. **Government Information Quarterly**, [S.L.], v. 39, n. 4, p. 101753, out. 2022. Elsevier BV. Disponível em: http://dx.doi.org/10.1016/j.giq.2022.101753. Acesso em: 09 jul. 2023.

KIRILLOVA, Elena Anatolyevna *et al*. Digital Right Protection Principles under Digitalization. **Webology**, [S.L.], v. 18, n. 04, p. 910-930, 30 set. 2021. NeuroQuantology Journal. Disponível em:.

http://dx.doi.org/10.14704/web/v18si04/web18173. Acesso em: 10 de jul de 2023.

KOCH, Márcio. **Visão Computacional para Reconhecimento de Faces aplicado na Identificação e Autenticação de Usuários na Web**. 2012. 139f. Trabalho de Conclusão do Curso (Bacharel em Ciência da Computação) – Universidade Regional de Blumenau, Blumenau, 2012. Disponível em: mailto:http:/bit.ly/2A3U8l7. Acesso em: 14 jan. 2021.

LARNIER, Jaron. **Dez argumentos para você deletar agora suas redes sociais**. Rio de Janeiro: Editora Intrínseca, 2018.

Lima, G. Ângela B. de O. (2010). MODELOS DE CATEGORIZAÇÃO: Apresentando o modelo clássico e o modelo de protótipos. **Perspectivas Em Ciência Da Informação**, 15(2), 108–122. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/23637 Acesso em: 04 de mai de 2023.

LIU, Yu-Li; YAN, Wenjia; HU, Bo. Resistance to facial recognition payment in China: the influence of privacy-related factors. **Telecommunications Policy**, [S.L.], v. 45, n. 5, p. 102155, jun. 2021. Elsevier BV. Disponível em:. http://dx.doi.org/10.1016/j.telpol.2021.102155. Acesso em: 10 de jul de 2023.

LOMBROSO, Cesare. **O Homem Delinquente**, Editora Edijur, 2020.

LOTT, Yuri Monnerat; CIANCONI, Regina de Barros. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da ciência da informação no brasil. **Perspectivas em Ciência da Informação**, [S.L.], v. 23, n. 4, p. 117-132, dez. 2018. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/1981-5344/3313.

MARY, I. Mettildha *et al*. Detecting Hostellers Using Face Recognition. **2022 International Conference On Data Science, Agents & Artificial Intelligence (Icdsaai)**, [S.L.], p. 1-5, 8 dez. 2022. IEEE. http://dx.doi.org/10.1109/icdsaai55433.2022.10028786.

MARDIANA; MUHAMMAD, Meizano Ardhi; MULYANI, Yessi. Library Attendance System using YOLOv5 Faces Recognition. **2021 International Conference On Converging Technology In Electrical And Information Engineering (Icctеie)**, [S.L.], p. 68-72, 27 out. 2021. IEEE. Disponível em: http://dx.doi.org/10.1109/icctеie54047.2021.9650628. Acesso em: 10 de jul de 2023.

MARX, Karl. **O capital**: Livro 1.2.ed. São Paulo. Boitempo, 2011.

MAZLAN, Faddly; HARUN, Afdallyna; SULIMAN, Saiful Izwan. Facial Recognition in Multimodal Biometrics System for Finger Disabled Applicants. **Indonesian Journal Of Electrical Engineering And Computer Science**, [S.L.], v. 6, n. 3, p. 638, 1 jun. 2017. Institute of Advanced Engineering and Science. Disponível em:. http://dx.doi.org/10.11591/ijeecs.v6.i3.pp638-645. Acesso em 09 de jul de 2023.

MORAES, Roque. Análise de conteúdo. Revista Educação, Porto Alegre, v. 22, n. 37, p. 7-32, 1999.

MOROZOV, Evgeny. **Big Tech: a ascensão dos dados e a morte da política.** São

Paulo. Ubu Editora, 2018.

O'NEIL, Cathy. **Armas de Destrucción Matemática:** cómo el big data aumenta la desigualdad y amenaza la democracia. Madrid, Capitán Swing Libros, 2017, 269p.

ONU. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 03 mar. 2021.

ORVALHO, Verónica. Reconhecimento Facial. **Revista Ciencia elementar**, v. 7, n. 4, 2019. Disponível em: https://rce.casadasciencias.org/rceapp/art/2019/073/ . Acesso em: 31 out. 2021.

PARKS, Connie L.; MONSON, Keith L.. Recognizability of computer-generated facial approximations in an automated facial recognition context for potential use in unidentified persons data repositories: optimally and operationally modeled conditions. **Forensic Science International**, [S.L.], v. 291, p. 272-278, out. 2018. Elsevier BV. Disponível em: http://dx.doi.org/10.1016/j.forsciint.2018.07.024. Acesso em: 10 de jul de 2023.

PETE, Amogh *et al*. A novel approach for verifying selective user identity attributes online using open banking APIs. **Journal Of Information And Optimization Sciences**, [S.L.], v. 43, n. 5, p. 941-948, 4 jul. 2022. Disponível em:. http://dx.doi.org/10.1080/02522667.2022.2091098 . Acesso em: 10 de jul de 2023.

PINTO, Álvaro Vieira. **O conceito de tecnologia.** Rio de Janeiro. Contraponto, 2003.

RAO, Vegnish Rao Paramesura; PUWAKPITIYAGE, Chamode Anjana Hewawasam; SHAFIQ, Dalia Abdulkareem; ISLAM, Farhana; HANDAYANI, Dini Oktarina Dwi; YACOOB, Hamwira; MANTORO, Teddy. Design and Development of Facial Recognitionbased Library Management System (FRLMS). **2018 International Conference On Computing, Engineering, And Design (Icced)**, [S.L.], p. 119-124, set. 2018.Disponível em:. IEEE. http://dx.doi.org/10.1109/icced.2018.00032. Acesso em 10 de jul de 2023.

RAJ, Ankesh; TAJAMMUL, Mohd. Cloud-Based System for Identifying Vaccinated Individual. **International Journal For Research In Applied Science And Engineering Technology**, [S.L.], v. 10, n. 4, p. 350-357, 30 abr. 2022. Disponível em: http://dx.doi.org/10.22214/ijraset.2022.41237. Acesso em: 10 de jul de 2023.

ROZSA, Vitor; DUTRA, Moisés Lima; PINTO, Adilson Luiz; MURIEL-TORRADO, Enrique. O paradigma tecnológico da internet das coisas e sua relação com a ciência da informação. **Informação & Sociedade**: Estudos, v. 27, n. 3, 2017. Disponível em: https://brapci.inf.br/index.php/res/v/90985 acesso em: 26 ago. 2021.

RUEDIGER, M. A. *et al*. **Robôs, Redes Sociais e Política no Brasil**: Análise de interferências de perfis automatizados nas eleições de 2014. PolicyPaper. Rio de Janeiro: FGV DAPP, 2018.

SETYATI, Endang *et al*. CNN based Face Recognition System for Patients with Down and William Syndrome. **Knowledge Engineering And Data Science**, [S.L.], v. 4, n. 2, p. 138, 19 dez. 2021. State University of Malang (UM). Disponível em:.

http://dx.doi.org/10.17977/um018v4i22021p138-144. Acesso em: 10 de jul de 2023.

SHARON, Tamar; KOOPS, Bert-Jaap. The ethics of inattention: revitalising civil inattention as a privacy-protecting mechanism in public spaces. **Ethics And Information Technology**, [S.L.], v. 23, n. 3, p. 331-343, 16 jan. 2021. Springer Science and Business Media LLC. Disponível em:. http://dx.doi.org/10.1007/s10676-020-09575-7 . Acesso em: 10 de jul de 2023.

SCLAROOF, S; BETKE, M; KOLLIOS,G; ALON, J; ATHITSON,V; RUI LI; MAGEE, J; TAI-PENG TIAN. Tracking, analysis, and recognition of human gestures in video. **Eighth International Conference on Document Analysis and Recognition (ICDAR'05)**, Seoul, South Korea, 2005, v 2, pp. 806-810. Disponível em: https://ieeexplore.ieee.org/document/1575656/authors#authors Acesso em: 15 mar 2023.

SEVERINO, Antonio Joaquim. **Metodologia do Trabalho Científico**. São Paulo: Cortez, 2007.

SHORE, Alexis. Talking about facial recognition technology: how framing and context influence privacy concerns and support for prohibitive policy. **Telematics And Informatics**, [S.L.], v. 70, p. 101815, maio 2022. Elsevier BV. Disponível em: http://dx.doi.org/10.1016/j.tele.2022.101815. Acesso em: 10 de jul de 2023.

STARK, Luke; STANHAUS Amanda; ANTHONY, Denise L.. “I Don't Want Someone to Watch Me While I'm Working”: Gendered Views of Facial Recognition Technology in Workplace Surveillance. **Journal Association for Information Science and Technology**. 2020. 71: 1074–1088. Disponível em: https://doi.org/10.1002/asi.24342 Acesso em: 09 jul. 2023.

SONG, Il-Yeol; ZHU Yongjun. Big data and data science: what should we teach? **Expert Systems**, 33: p. 364-373, 2016. Disponível em: https://doi.org/10.1111/exsy.12130 Acesso em: 18 jun. 2023.

UN GLOBAL PULSE. **Home**. 2023. Disponível em: https://www.unglobalpulse.org/ Acesso em: 18 jun. 2023.

UPALA, Maulik; WONG, Wk. IoT Solution for Smart Library Using Facial Recognition. **Iop Conference Series**: Materials Science and Engineering, [S.L.], v. 495, p. 012030, 7 jun. 2019. IOP Publishing. Disponível em: http://dx.doi.org/10.1088/1757-899x/495/1/012030. Acesso em: 10 de jul de 2023.

VALENCIA, Adrián Sotelo. **Subimperialismo e dependência na América Latina**: o pensamento de Ruy Mauro Marini. São Paulo: Expressão Popular, 2019.

VALENTE, Jonas. Tecnologias de reconhecimento facial são usadas em 37 cidades no país. **Agência Brasil**, São Paulo, 19 set. 2019. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais. Acesso em: 07 ago. 2021.

VENTURINI, Jamila; GARAY, Vladimir. **Reconhecimento facial na América Latina: tendências na implementação de uma tecnologia perversa**. Alsur, 2021.

VIRILIO, Paul. **Guerra e Cinema.** 1ª Ed. São Paulo. Editora Pagina Aberta, 1993.

VAN NOORDEN, Richard. The ethical questions that haunt facial-recognition research. **Nature**, [S.L.], v. 587, n. 7834, p. 354-358, 18 nov. 2020. Springer Science and Business Media LLC. Disponível em:. http://dx.doi.org/10.1038/d41586-020-03187-3. Acesso em: 10 de jul de 2023.

XIE, L., MENG, H., LIU, ZQ. A Cantonese Speech-Driven Talking Face Using Translingual Audio-to-Visual Conversion. **Chinese Spoken Language Processing. Lecture Notes in Computer Science**. Springer, Berlin, Heidelberg, 2006, V 4274. Disponível em: https://doi.org/10.1007/11939993_64 Acesso em: 10 mar 2023.

WANG, Geng; ZHANG, Chaolin. Legal Regulation of Government Applications of Facial Recognition Technology: a comparison of two approaches. **Us-China Law Review**, [S.L.], v. 19, n. 6, p. 259-266, 28 jun. 2022. Disponível em:. http://dx.doi.org/10.17265/1548-6605/2022.06.002. Acesso em: 10 de jul de 2023.

WELCHEN. Vandoir. **Uso de inteligência artificial em apoio a decisão clínica:** o caso do Hospital do Câncer Mãe de Deus com a ferramenta cognitiva Watson Oncology. 2019. 218f. Dissertação (Mestrado em Administração) – Universidade de Caxias do Sul, Caxias do Sul, 2019. Disponível em: https://it.ly/2SDHcJ0. Acesso em: 02 abr. 2021.

WU, T; CHELLAPPA, R. Age Invariant Face Verification with Relative Craniofacial Growth Model. **Computer Vision – ECCV 2012. ECCV 2012.** Lecture Notes in Computer Science. 2012, vol 7577. Springer, Berlin, Heidelberg. Disponivel em: https://doi.org/10.1007/978-3-642-33783-3_5 Acesso em: 01 mar 2023.

ZAIDAN, Paula. Proteção de dados impacta no uso de reconhecimento facial. 2019. Disponível em: http://www.securityreport.com.br/destaques/protecao-de-dados-impacta-nouso-de-reconhecimento-facial/#.XtD7Z2hKjlU. Acesso em: 24 jun. 2020.

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal of Information Technology,** v.30, p.75–89, 2015. Disponível em: https://journals.sagepub.com/doi/pdf/10.1057/jit.2015.5 . Acesso em: 15 ago. 2021.

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