PROBLEMAS DERIVADOS DO USO DE RECONHECIMENTO FACIAL

Gustavo Businhani da Silvar[1], Bruno Da Silva Rodrigues[1]

[1]Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie
Caixa Postal 01302.907 – São Paulo – SP – Brasil

{gustavobusinhani@hotmail.com, bruno.rodrigues@mackenzie.br}

Abstract. *This article describes the problems arising from the use of facial recognition, whether through software or even human error. Today, the recognition facial faces somes difficulties that imply in the progress that this technology becomes good. This research discusses cases of false positives, which presente ambiguity in their results.*

Resumo. *Este artigo descreve os problemas derivados do uso de reconhecimento facial, seja por meio de softwares ou até mesmo por falhas humanas. Hoje, o reconhecimento facial passa por algumas dificuldades que implicam no progresso para que essa tecnologia se torne boa. Esta pesquisa discute casos de falsos positivos, que apresentam ambiguidades em seus resultados obtidos.*

1. Introdução

O reconhecimento facial, geralmente faz uso de métodos da área que utilizam tecnologia biométrica que reconhece automaticamente características faciais das pessoas. Normalmente, o que se chamam de reconhecimento facial é a abreviatura de reconhecimento e verificação de identidade com base em imagens ópticas das faces humanas. O reconhecimento faz o uso de uma câmera para coletar imagens ou fluxos de vídeo contendo rostos e em seguida, detecta e rastreia automaticamente os rostos presentes nas imagens e inicia operações algorítmicas em um aplicativo que possui base de dados com imagens de rosto detectadas. Para que isso ocorra tecnicamente, é necessário posicionar uma câmera para que seja detectado algum dado de algum rosto e depois incluir a coleta das imagens na aplicação. Simplificando, é usado para extrair características do rosto da foto, como a altura das sobrancelhas, os cantos da boca, orelhas, nariz [Gomes, 2018].

O uso de reconhecimento facial se faz cada vez mais presente em nossas vidas, aplicações como pagamentos online, desbloqueio de smartphones e controles de acesso se valem dessa tecnologia para agilizar o processo e facilitar o uso das aplicações. Por mais precisos e confiáveis que os algoritmos sejam, as rápidas e constantes transformações da tecnologia, trazem consigo novos paradigmas e desafios mais complexos que merecem a atenção tanto por dos usuários quanto para os desenvolvedores de aplicações.

Ao se fazer o uso da tecnologia por reconhecimento facial, devem ser levados em consideração alguns contrapontos que podem ser críticos a nível de processamento

das informações (imagens) obtidas como falta de iluminação no ambiente, câmeras posicionadas em ângulos não apropriados, expressões faciais realizadas durante a captura das imagens e baixas resoluções das câmeras. Esses fatores podem comprometer as informações que serão analisadas, impactando o resultado da aplicação e trazer consequências graves ao usuário.

As tecnologias que fazem o uso de reconhecimento facial, precisam apresentar métodos de desenvolvimento que evitem falhas dentro do seu contexto aplicacional. Por depender de fatores externos ao algoritmo de reconhecimento facial, por mais preciso que seu desenvolvimento tenha sido, a implementação pode retornar falhas durante seu uso.

Levando em consideração a importância da tecnologia de reconhecimento facial e a diversidade de aplicações criadas a partir do uso de algoritmos de reconhecimento facial, a proposta desse artigo é chamar a atenção da comunidade científica acerca dos problemas associados a popularização de aplicativos que se utilizam o reconhecimento facial, assim como a suas consequências aos usuários no âmbito criminal e em questões relacionadas a violação de liberdades civis e privacidade.

O artigo está estruturado nas subsequentes seções que consiste em:

- Fundamentação teórica – A tecnologia de reconhecimento facial, que diz respeito da área de visão computacional, utiliza a inteligência artificial, algoritmos e uma base de dados, para confirmar a identidade das pessoas;
- Metodologia – Se encontra a organização do projeto;
- Revisão referente aos problemas derivados do uso de reconhecimento facial – se encontra um breve detalhamento das notícias e artigos pesquisados para embasar uma discussão.
- Discussão – conclusões sobre os resultados das pesquisas referente aos problemas derivados do uso da tecnologia do reconhecimento facial.
- Conclusões.

2. Fundamentação Teórica

2.1. Reconhecimento Facial

O reconhecimento facial é uma técnica de biometria baseada em traços do rosto humano. Esse processo consiste em realizar pontos de medida do rosto, que fazem ligação algorítmica de traços e tamanhos, como por exemplo, fazer a medição exata entre o nariz e orelhas, tamanho do crânio, arcada dentária, entre outros detalhes, [Okabe, 2015].

Um dos diferenciais do reconhecimento facial dos outros sistemas biométricos reside no fato desta tecnologia poder abranger várias disciplinas como processamento de imagem, reconhecimento facial de padrões, visão computacional e redes neurais. O reconhecimento facial tem aplicações principalmente nas áreas de biometria, controle acesso, aplicação da lei, sistemas de segurança e vigilância, [Saffi, 2019].

De certo modo, o reconhecimento facial é uma tecnologia que identifica os indivíduos por suas características faciais. Ele funciona comparando características

faciais selecionadas de uma determinada imagem com faces existentes em um banco de dados. Embora a precisão do sistema de reconhecimento facial, como a tecnologia biométrica, seja inferior a íris do olho e ao reconhecimento de impressões digitais, ainda é amplamente adotado por sua simplicidade, [Orvalho, 2019].

2.2. Inteligência Artificial

A inteligência artificial é um campo de conhecimento que utiliza modelos para suportar a tomada de decisões baseadas em fatos reais e dados experienciais, mesmo quando estes são incompletos [Sellitto, 2002].

De certo modo, resumidamente, é a possibilidade de uma máquina, por meio de algoritmos, possuir capacidade cognitiva semelhantes de um ser humano, [Silva e Mairink 2019]. Essa mesma tecnologia consegue sistematizar e automatizar tarefas intelectuais e, portanto, é potencialmente relevante para qualquer esfera da atividade intelectual humana, [Gomes, 2010].

Em uma das divisões da inteligência artificial, o aprendizado de máquina, pode ser considerado uma viabilização por esse mecanismo que permite que os computadores sejam capazes de reconhecer pessoas, tem a capacidade de executarem funções cognitivas, que são geralmente associadas à mente humana, tais como aprendizado e a solução de problemas. Em um sistema biométrico, pode ser dividido em três etapas, que são; captura, extração e comparação. Para isso, uma extração de características para reconhecimento facial é necessário o uso intenso do recurso de redes neurais, para que seja necessário atingir um nível de precisão adequado [SimpleID, 2021].

2.3. Big Data e Reconhecimento Facial

Hoje em dia, com o surgimento da *World Wide Web*, criou-se possibilidades de fazer um aumento de informações atingindo uma escala de pessoas muito maior que antigamente, como também fazer contatos por meio da internet com pessoas distantes fisicamente, de uma maneira mais simples as distâncias reais, [Markoff, 2006].

Conforme a identificação de padrões e tendências, os dispositivos eletrônicos possuem acesso aos dados do usuário para que essas informações sejam otimizadas e personalizadas. As redes sociais utilizam o *Data Mining* e fazem um tratamento nos dados que são obtidos para otimizar a experiência dos seus usuários, por isso os algoritmos são utilizados principalmente para esses casos, [França, et al., 2014].

Nesse contexto, pode-se considerar que os algoritmos são essenciais para criar diversas finalidades, que podem ser capazes de revisar ou compreender uma ação, por meio dos dados coletados, e assim entender as preferências e definir o perfil do usuário. O *Facebook*, por exemplo, utiliza a influência dos algoritmos quando os usuários fazem o uso das publicações e postagens de fotos de seus amigos. Entende-se com a explicação contida na página de “ajuda” do *Facebook*, que as interações feitas pelos usuários na Plataforma, são levadas em conta para que as operações algorítmicas tracem um conteúdo mais relevantes para os mesmos.

3. Metodologia da Pesquisa

A metodologia empregada nesta pesquisa, partiu de uma revisão da literatura específica acerca do tema. Este trabalho apresenta os resultados de uma pesquisa exploratória

realizada nas principais base de dados digitais como google scholar, SciELO, BDTD, com objetivo levantar informações sobre problemas relacionados ao uso de reconhecimento facial, construir hipóteses sobre os problemas e proporcionar familiaridade com o campo de estudo [Gil, 2002].

Com raciocínio similar, [Severino, 2016] afirma que a pesquisa exploratória busca apenas levantar informações sobre um determinado objeto, delimitando um campo de trabalho, sendo uma preparação para pesquisas mais aprofundadas.

A pesquisa foi desenvolvida a partir de consultas disponíveis de casos de falsos positivos e as referências foram apresentadas ao final deste texto. A hipótese aqui construída foi a de que o reconhecimento facial pode gerar falhas imprecisas, deixando a tecnologia vulnerável com resultados não confiáveis as pessoas, por exemplo, vazamento de dados, discriminação, que poderá ser confirmada ou não por estudos futuros e que poderão sugerir também formas mais seguras de utilizar o reconhecimento facial.

A análise dos dados obtidos será utilizada para a definição de padrões e inconsistências derivadas das complicações de captura, análise e definição de características que se somadas geram ambiguidades técnicas nos resultados finais das aplicações. Tal verificação, possibilitará a compreensão do tema e possíveis impactos nos usuários finais e na sociedade como um todo.

Por meio de uma análise estatística, desenvolvida a partir da base de informações e dados, será gerado uma série de indicadores de forma a estabelecer um quadro claro da situação atual e, informar de forma comparativa, a incidência de casos de falsos positivos.

Seguindo com a confecção e tabulação dos dados analíticos, é possível coletar algumas conclusões sobre a incidência de determinados casos e aplicações de métodos que tendem a demonstrar mais ambiguidades em suas varáveis. Por meio dos casos de estudo, podem ocorrer alguns indicadores, envolvendo gráficos, medias, desvio de padrão e outras medidas estatísticas, visando atuar de forma visual e didática no período de apresentação dos casos. A figura 1 apresenta um fluxograma de uma apresentação gráfica do desenvolvimento da pesquisa, [Coutinho, 2020].

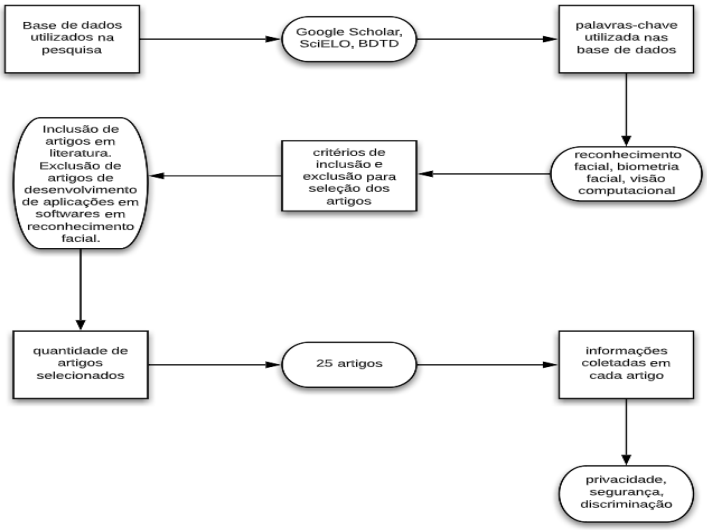

Figura 1. Fluxograma do desenvolvimento da pesquisa.

4. Revisão Referente aos Problemas Derivados do Uso de Reconhecimento Facial

Originalmente criada como uma tecnologia de biométrica alternativa ao uso da impressão digital, a utilização do reconhecimento facial, passou a ser usada para auxiliar em aplicações que vão desde desbloqueio de celular, até sistemas complexos usado por forças de segurança pública onde a integração de algoritmos de reconhecimento facial e Big Data são usados para combater e monitorar crimes.

Devido a relevância do tema e a diversidade de aplicações que fazem uso desta tecnologia, esta seção é dedicada aos casos de estudo sobre os problemas derivados que utilizam algumas aplicações do reconhecimento facial e tange focar os temas relacionados a privacidade, discriminação, segurança e crimes. Dentre os casos observados, destacam-se os seguintes:

4.1. Violações de Privacidade

A Escócia que está atuando junto com o Comitê Europeu de Proteção de Dados, decidiu avaliar o uso de reconhecimento facial em seu país e considera excluir o seu uso em escolas. A discusão foi motivado pelo caso principalmente em escolas da região de *North Ayrshire*, no qual a tecnologia era utilizada pelos estudantes na compra de merenda escolar, [Kundaliya, 2021].

As escolas contrataram o *software* da CRB Cunninghams, fazendo com que os estudantes tivessem uma agilidade e um pagamento da merenda sem contato com os alunos. A privacidade de uma criança é muito maior do que para os adultos, por isso as pessoas que defendem a privacidade, expressaram preocupações para esses alunos. Por conta disso, o *Information Commissioner's Office* (ICO), um orgão que se reporta diretamente ao Parlamento do Reino Unido, abriu uma investigação sobre as implementações da tecnologia de reconhecimento facial nas escolas.

Após uma série de perguntas da ICO, o conselho de *North Ayrshire* levou em consideração a privacidade das crianças, e que isso não seria benéfico caso houvesse algum vazamento de dados, por isso voltaram a usar o sistema de PIN, até que as investigações que foram abertas pelo *Information Commissioner's Office* (ICO) fossem concluídas, [Kundaliya, 2021].

O conselho de *North Ayrshire* disse que "embora estejamos confiantes de que o novo sistema de reconhecimento facial está operando conforme planejado, achamos prudente voltar ao sistema anterior de PIN (número de identificação pessoal) enquanto consideramos as consultas recebidas". [Kundaliya, 2021].

A *Defend Digital Me*, é uma organização que protege os direitos das crianças à privacidade e à vida familiar. Essa organização tem como missão obter dados seguros, justos e transparentes nas escolas da Inglaterra. A diretora dessa organização, Jen Persson, elogiou a decisão de algumas escolas como a *Great Academy Ashton*, ao fato de parar completamente o uso do *software* de reconhecimento facial. Segundo Jen Persson, [Kundaliya, 2021], "...dos Estados Unidos à Europa, as autoridades estão proibindo o reconhecimento facial, mas no Reino Unido estamos usando crianças como cobaias para as tecnologias mais invasivas de privacidade do mercado".

Nos Estados Unidos também não é diferente, o governo de Nova Iorque aprovou uma lei na qual proíbe o uso de qualquer tecnologia biométrica nas escolas do estado,

até julho de 2022. Estudos realizados pela revista *Office of Information Technology* e a revista *Education Department,* que mostraram o uso do reconhecimento facial pode trazer experiências negativas para as pessoas, [Keane, 2020].

De certa forma, as escolas tem o objetivo de proteger os alunos de criminosos sexuais, funcionários não autorizados ou até mesmo outras pessoas que se passam por alunos para causar alguma tragédia. Embora essa tecnologia ainda possa possuir muitas falhas na forma em que é aplicada, não se pode descarta-la, mas é necessário aguardar até que essas falhas sejam eliminadas [Breternitz, 2021].

A *Clearview AI* é uma empresa de software de reconhecimento facial que possui um banco de dados com mais 20 bilhões de imagens e coletas partir de imagens indexadas na Internet e disponiveis em redes sociais. Segundo Ton-That, "o Software funciona como o Google, mas em vez de colocar palavras, o usuário coloca uma foto de um rosto no campo de busca". Segundo o site a de noticias [BBC, 2021].

A *Clearview AI* permite que agências governamentais utilizem seu banco de dados de rostos para reconhecimento de indivíduos, e recentemente vendeu licensas de uso da aplicação para o governo da Ucrânia, para que identificasse as pessoas mortas vítimas pela guerra. [Clayon, 2022].

Recentemente, a agência *Office of the Australian Information Commissioner* (OAIC), pediu que *Clearview AI* parasse de armazenar fotos tiradas na Austrália e deletassem as fotos que já estavam em seu banco de dados. Apesar da *Clearview AI*, só coleta imagens que são divulgadas publicamente na Internet, a ação pode ser considerada de certo modo, uma invasão à privacidade, pois pode-se publicar fotos na Internet, mas estas fotos podem não ser salvas em algum banco de dados sem autorização [BBC, 2021].

No que se diz respeito às leis que defendem os direitos civis, estas deveriam ser mais rigorosas; por isso que nos dias atuais, países estão se juntando para criar legislações que protegem esses direitos civis.

4.2. Uso do reconhecimento facial em crimes digitais

No Brasil os criminosos estão se aproveitando do uso do reconhecimento facial para aplicarem golpes, principalmente em datas como dia das crianças, natal, páscoa, entre outras datas especiais, onde habitualmente as pessoas recebem presentes e gratificaçõe e ficam propensas a serem vítimas de fraudes.

A fraude é aplicada, onde os criminosos simulam uma entrega de um presente no qual a vítima supostamente ganhou em consequencia de alguma promoção ou concurso promovido por uma loja. Após a entrega do presente, o suposto entregador, que na verdade é o criminoso, tira fotos da vítima para a confirmação do recebimento do produto, além de pedir informações pessoais para serem preenchidas, como CPF e RG. A partir desses dados obtidos, os criminosos começam a pedir empréstimos em banco ou até mesmo compram veículos no nome da pessoa que foi a vítima do golpe.

Segundo a diretora do Procon-PR Claudia Silvano [Branco, 2021] “Eles estão se dando ao trabalho de comprar uma lembrança, entregar para as pessoas e conseguir as informações para aplicar o golpe. São verdadeiras quadrilhas, que cada vez mais estão especializadas". Ainda de acordo com Claudia Silvano, os criminosos usam as fotos que foram tiradas das vítimas e seus dados pessoais para burlar os sistemas de segurança de

reconhecimento facial de instituições bancárias, podendo realizar transações em nome de terceiros.

4.3. Discriminação de indivíduos em função de falhas no reconhecimento

Países como Estados Unidos, utilizam muitos *softwares* de reconhecimento facial nos quais são utilizados por policiais. Em 2019 um homem chamado Nijeer Parks de pele negra foi incriminado injustamente após um policial inserir a foto de um outro suspeito no *software* e o mesmo reconhecer uma pessoa que foi presa no passado e já estava inocentado após ter cumprido uma pena de seis anos de prisão, [Khan, 2020].

Após os policiais pegarem Parks, foi levado em uma cela da prisão no qual passou 10 dias, e se recusou um acordo com a justiça do Estado. O juiz exigiu evidências dos procuradores além da correspondência no sistema de reconhecimento facial. Sem ter uma prova concreta, eles retiraram as queixas contra Parks.

Isso mostra-se que, Parks por ter uma pele escura foi preso devido a erros em *software* de reconhecimento facial. Uma análise feita em 2019 mostra um claro viés nestes sistemas, com tendência muito maior a identificar incorretamente mulheres negras (1 falso positivo em 1 mil) do que brancas (1 em 10 mil), [Rigues, 2020].

A União das Liberdades Civis de Nova York (NYCLU), informou que, em um ambiente no qual possui grande escala de jovens, podem ser possíveis falhas de identificações nas quais podem ocorrer reações caóticas, como por exemplo: *bullying* e brincadeiras de mau gosto.

A grande empresa *Google* não deixa o público usar o *software* de reconhecimento facial, assim como é feito pelos *softwares Google Search*, *Google Maps*, *Google Earth*, entre outras. Esse *software* não é liberado para o público, pois ainda está sendo avaliado com objetivo de melhorar sua eficiência e confiabilidade, [Lee, 2018].

No reconhecimento facial, tem-se muitas preocupações consideráveis entre as pessoas que trabalham no Vale do Silício e os grupos de direitos civis sobre a aplicação dessa tecnologia. Embora o *Google* utilize o reconhecimento facial para ajudar os usuários a identificar amigos em fotos, a tecnologia não está aberta para uso público, pois o lado "humano" da Inteligência Artificial não possui a diversidade do qual precisa e os dados em si tem alguns preconceitos inerentes, [Lee, 2018].

Ainda por se tratar pela empres *Google* o aplicativo *Google Photos* associou um casal de negros erroneamente como gorilas. As fotos dos usuários que utilizam esse aplicativo podem ser organizadas automaticamente com base nos objetos que estão nas fotos, feito por meio do algoritmo,

O recurso de "*tags"* aprende à medida que recebe os dados, fazendo com que se refine seu método para categorizar os objetos. Porém a categorização não é a única etapa da fotografia que a empresa tem problemas. O *Google* tentou consertar o algoritmo, porém decidiu remover a *"tag*" gorila por completo, devido não encontrar o erro que pode ter causado, [Grush, 2015].

Alguns pesquisadores que fizeram um estudo entre cinco empresas, incluindo a *Amazon*, *IBM*, e *Microsoft*, relataram que a gigante *Amazon* teve um desempenho muito ruim por meio do seu software chamado *Rekognition* ao detectar mulheres com peles

mais escuras por exemplo. O estudo desses pesquisadores mostrou-se deficiente e que o software teve uma taxa de erro de 31% ao reconhecer o gênero das imagens de mulheres com peles mais escuras, [Raji et al., 2020].

O algoritmo do reconhecimento facial ainda tem muitas preocupações, devido a base de dados não possuir suficientemente imagens diversificadas para que esses algoritmos possam aprender a identificar pessoas com peles mais escuras. Nesse mesmo estudo, testaram uma foto da apresentadora de TV americana Oprah Winfrey, e com base nesse teste do *software* da *Amazon,* o resultado foi inesperado, pois mostrou-se que a apresentadora era na verdade um homem, um verdadeiro erro, no qual mostra que o algoritmo ainda possui uma taxa de erro muito maior que o esperado.

4.4. Problemas Derivados na Segurança

É provável que os policiais dos Estados Unidos da América, estejam alimentando esses *softwares* com dados falhos, incluindo esboços compostos e fotos de celebridades que compartilham características fisicas com suspeitos. E isso é indubitável que não podemos confiar até mesmo naqueles que fornecem segurança pública.

As fotos que tiramos no nosso dia a dia, para postar em redes sociais, pode ser alvo da privacidade, além disso o autoretrato digital passou a ser utilizado como uma forma de identidade digital. Recentemente foram vazados dados pessoais, incluindo biometrias, que fizeram mais de 220 milhões de brasileiros vítimas, e isso acende um alerta sobre a segurança dos cidadãos nos meios online, [Covolato, 2021].

No Reino Unido utiliza-se a tecnologia de reconhecimento facial de forma que pode ser considerada um pouco questionável, no qual não tem base legal e uma eficácia duvidosa. A Câmera dos Lordes no Reino Unido, abriu um inquérito questionando sua eficácia, [Kloving, 2021].

5. Discussão

Em visão computacional, podemos notar que a coleta, analise e síntese dos dados, são feitos por meio da própria alimentação fornecida para os bancos de dados fornecido pelos os humanos que alimentam com seus relatórios gerais. O fato é que o algoritmo necessita de um grande volume de dados para poder tomar suas próprias decisões. Estes são retirados de toda a população continuamente, o que pode gerar consequências futuras nas questões de direitos fundamentais e, por isso, precisam ser jurídica e eticamente regulados, [Barros, 2020].

Após inúmeras pesquisas realizadas para elaboração deste trabalho, pode-se notar que há uma estatística com base nos artigos estudados até o momento sobre os diferentes problemas relacionados ao uso/falhas do reconhecimento facial. Além disso, podemos notar que existem várias preocupações ao utilizar esse tipo de tecnologia, por exemplo, como a nossa privacidade, discriminação, entre outras.

A União Europeia está criando uma legislação que visa a proibição do uso da tecnologia do reconhecimento facial em locais públicos, essa legislação propõe também uma suspensão do uso dessa tecnologia para fins de policiamento, porém, essa legislação mostra que o uso da tecnologia de reconhecimento facial seria apenas para crimes hediondos como sequestro e terrorismos, [Ropeck, 2021].

Joy Buolamwini, a personagem do documentário The Coded Bias, pesquisadora do MIT, realizou uma das primeiras pesquisas que tratam de vieses em sistemas de reconhecimento facial, [Buolamwini e Gebru, 2018]. A pesquisa realizada no documentário de Buolamwini, mostrou-se que, no geral, homens e pessoas brancas foram identificados melhores do que outros grupos. Uma visão interseccional da pesquisa revela que todos os classificadores avaliados tiveram um pior desempenho ao classificar mulheres negras, [Ruback, Avila e Cantero, 2021].

A figura 2 mostra um exemplo de dados, apontados por Buolamwini e Gebru, utilizados em *softwares* de reconhecimento facial. Pode-se observar a distribuição desbalanceada por gênero e tipo de pele nos dois conjuntos de dados, Adience e IJB-A. Nos dados da Adience, enquanto homens de pele clara representam 41,6% do total, as mulheres negras representam 7,4%. Já nos dados do IJB-A, a diferença é ainda maior: homens de pele clara representam 59,4% do total e mulheres negras representam somente 4,4% do total, [Ruback, Avila, Cantero, 2021].

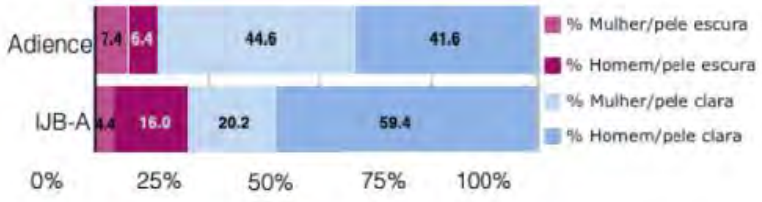

Figura 2. Exemplos de dados de representação fazendo a comparação de mulheres/homens com pele escura, [Buolamwini e Gebru 2018].

No Reino Unido, foram fornecidos relatórios para o Comitê de Justiça sobre a utilização das ferramentas algorítmicas, e foi questionado a eficácia de como o uso do reconhecimento facial quando implantado no Departamento de Polícia de Londres. A diretora Silkie Carlo, do grupo de campanha de liberdade civis *Big Brother Watch*, verificou que em cinco anos a polícia no Reino Unido, teve uma eficácia de 11 resultados positivos dentre os 500,000 rostos escaneados no banco de dados usando o reconhecimento facial. Isso mostra que geraram uma enorme quantidade de falsos positivos, ou seja, a atual taxa deles na totalidade das implantações é de 93% de falsos positivos, uma desigualdade surreal, [Skelton, 2021].

Os cidadãos que inserem os seus dados pessoais estão em uma posição mais vulnerável quando falamos dos serviços públicos disponibilizados online, como por exemplo, CNH Digital, RG Digital, entre outros. Se tratando no Brasil, o Estado é o responsável pela emissão da identidade digital do cidadão, pela custódia da sua assinatura eletrônica, pelas bases em que os dados do usuário são reunidos e confirmados e, ainda, pela prestação do serviço, sendo a quem essa identidade digital e a assinatura eletrônica serão opostas. Ou seja, caso seja vítima de algum golpe, o cidadão terá ainda mais dificuldade em comprovar que não foi o autor de solicitação feita em seu nome, [Covolato, 2021].

Segundo a professora Karen Yeung de Direito, Ética e Informática na Universidade de Birmingham, foi dito por ela que as bases de dados nesses experimentos de reconhecimento facial, não são muito estáveis. Em termos jurídicos, a

polícia do Reino Unido usa essa tecnologia para justificar suas implantações no sistema, [Skelton, 2021].

6. Conclusão

Neste trabalho, apresentamos um estudo que tem, por objetivo, exibir o quão a tecnologia de reconhecimento facial ainda está defasada ao ponto de se notar que os algoritmos ainda não estão aptos para uma sociedade igualitária. O uso de reconhecimento facial pode ser usado como um dos meios de prova para crimes, por exemplo, porém não pode ser único método utilizado.

O presente estudo indica que ainda serão necessários muitos esforços no desenvolvimento tecnológico de aplicações que usam o reconhecimento facial de maneira a obter uma ferramenta precisa, bem como garantir a privacidade dos usuários.

No que se diz respeito aos artigos referente aos direitos civis, às leis que os defendem, deveriam ser mais rigorosas; por isso que nos dias atuais, países estão se juntando para criar legislações que protegem esses direitos civis.

A população precisa se atentar ao andar nessas tecnologias de reconhecimento facial e tentar compreender que não há uma solução para os problemas sociais que são enfrentados no dia a dia. Essa tecnologia não vem para acabar com qualquer tipo de prática indevida dentro da sociedade ou criminalidade. Se essa tecnologia não for bem enraizada, pode gerar conflitos e violações na sociedade, prejudicando a população e violando os seus direitos.

Conclui-se que com os dados coletados referente a notícias e a artigos, a maioria de fato é relacionado a discriminação, então, pode-se observar que os algoritmos não possuem preconceito, mas sim, as pessoas que alimentam a base de dados do mesmo. Em relação a trabalho futuros, existem alguns pontos como, por exemplo, realizar pesquisas sobre a evolução da tecnologia de reconhecimento facial vem sendo aperfeiçoada cada vez mais com maior segurança e eficácia.

Referencias

Barros, Isabela Maria Pereira Paes; Silva, Isabela Inês Bernardino de Souza. (2020) “UTILIZAÇÃO DO RECONHECIMENTO FACIAL ELETRÔNICO POR EMPRESAS PARA IDENTIFICAÇÃO DE SUSPEITOS: SEGURANÇA OU VIOLAÇÃO DO ESTADO DEMOCRÁTICO DE DIREITO?”, https://periodicos.ufrn.br/transgressoes/article/view/19909/12958. Acesso em: 26 abr. 2022.

BBC News. (2021) “Database firm Clearview AI told to remove fotos taken in Australia”, https://www.bbc.com/news/technology-59149236. Acesso em: 13 dez. 2021.

Branco, Dácio C. (2021) “Golpe do presente rouba foto da vítima para fraudar reconhecimento facial”, https://canaltech.com.br/seguranca/golpe-do-presente-rouba-foto-da-vitima-para-fraudar-reconhecimento-facial-200660/. Acesso em: 15 dez. 2021.

Breternitz, Vivaldo José. (2021) “Reconhecimento facial é proibido em escolas de Nova Iorque”, https://revistaeducacao.com.br/2021/01/11/reconhecimento-facial-escolas/. Acesso em: 25 mai. 2021.

Buolamwini, Joy. e Gebru, Timnit. (2018) “Gender shades: Intersecctional accuracy disparities in commercial gender classification. Conference on Fairness, Accountability and Transparency”, Sorelle A. Friedler e Christo Wilson., p. 77-91.

Clayton, James. (2022) “Como reconhecimento facial é usado para identificar mortos na Ucrânia”, https://www.bbc.com/portuguese/internacional-61104864. Acesso em: 25 abr. 2022.

Coutinho, Thiago. (2020) “Quer aprender a fazer um fluxograma? Aqui vão 4 dicas para você!”, https://www.voitto.com.br/blog/artigo/fluxograma. Acesso em: 04 jun. 2020.

Covolato, Thaís. (2021) “Novo tipo de golpe que “rouba” o seu rosto: podemos confiar no reconhecimento facial como forma de identidade digital?”, https://tiinside.com.br/09/06/2021/novo-tipo-de-golpe-que-rouba-o-seu-rosto-podemos-confiar-no-reconhecimento-facial-como-forma-de-identidade-digital/. Acesso em: 13 mai. 2022.

Época Negócios. (2020) “Sistema de I.A falha em identificar pessoas não brancas e universidade desiste de usar reconhecimento facial”, https://epocanegocios.globo.com/Tecnologia/noticia/2020/02/racismo-em-i-leva-universidade-desistir-de-reconhecimento-facial-no-campus.html. Acesso em: 06 jun. 2021.

França, Tiago Cruz; Faria, Fabricio Firmino; Rangel, Fabio Medeiros; Farias, Claudio Miceli; Oliveira, Jonice. (2014) “Big Social Data: Princípios sobre Coleta, Tratamento e Análise de Dados Sociais”, https://www.inf.ufpr.br/sbbd-sbsc2014/sbbd/proceedings/artigos/pdfs/127.pdf. Acesso em: 13 mai. 2022.

Gil, Antônio Carlos (2002), Como Elaborar Projetos de Pesquisa, São Paulo: Atlas, 4ª edição.

Gomes, Helton Simões. (2018) “Como funciona o reconhecimento facial? Entenda a tecnologia que lê o rosto”, https://www.uol.com.br/tilt/noticias/redacao/2018/10/11/entenda-a-tecnologia-por-tras-do-reconhecimento-facial.htm. Acesso em: 25 nov. 2021.

Gomes, Dennis dos Santos. (2010) “Inteligência Artificial: Conceitos e Aplicações”, www.professores.uff.br/screspo/wp-content/uploads/sites/127/2017/09/ia_intro.pdf. Acesso em: 10 mai. 2022.

Kenae, Sean. (2020) “New York temporarily bans facial recognition in schools”, https://www.cnet.com/news/best-internet-providers-in-new-york-city/. Acesso em: 21 jun. 2021.

Kleinman, Zoe. (2019) “Amazon: Facial recognition bias claims are ‘misleading’”, https://www.bbc.com/news/technology-47117299. Acesso em: 17 abr. 2021.

Kundaliya, Dev. (2021) “Schools suspend use of facial recognition after backlash”, https://www.computing.co.uk/news/4039273/schools-suspend-facial-recognition-backlash. Acesso em: 27 nov. 2021.

Lee, Dave. (2018) “Google executive warns of face ID bias”, https://www.bbc.com/news/technology-44977366. Acesso em: 23 abr. 2021

Markoff, John. (2006) “Entrepreneurs see a web guided by common sense”, Tradução: Fabiano Caruso. https://www.mail-archive.com/bib_virtual@ibict.br/msg01199.html. Acesso em: 14 abr. 2021.

Okabe, Rogério Kazuhiro. (2015) “RECONHECIMENTO FACIAL EM IMAGENS CAPTURADAS POR CÂMERAS DIGITAIS DE REDE”, https://revistas.unoeste.br/index.php/ce/article/view/1307. Acesso em: 15 mai. 2022.

Orvalho, Verónica. (2019) “Reconhecimento Facial”, https://rce.casadasciencias.org/rceapp/art/2019/073/. Acesso em: 08 mai. 2022.

Rigues, Rafael. (2020) “Reconhecimento facial falha e homem inocente passa 10 dias na cadeia”, https://olhardigital.com.br/2020/12/30/noticias/reconhecimento-facial-falha-e-homem-inocente-passa-10-dias-na-cadeia. Acesso em: 10 mai. 2022.

Ropeck, Lucas. (2021) “União Europeia quer proibir polícia de usar reconhecimento facial”, https://olhardigital.com.br/2020/12/30/noticias/reconhecimento-facial-falha-e-homem-inocente-passa-10-dias-na-cadeia. Acesso em: 07 fev. 2022.

Ruback, Livia; Avila, Sandra; Cantero, Lucia. (2021) “Vieses no Aprendizado de Máquina e suas Implicações Sociais: Um Estudo de Caso no Reconhecimento Facial”, https://sol.sbc.org.br/index.php/wics/article/view/15967. Acesso em: 09 mai. 2022.

Saffi, Jean C. Corrêa. (2019) “APRENDIZAGEM E RECONHECIMENTO DE FACES ATRAVÉS DE COMPUTER VISION E MACHINE LEARNING, APLICADO A AMBIENTES DE ACESSO RESTRITO”, https://www.imed.edu.br/Uploads/JEAN%20CARLOS%20MAFFI.pdf. Acesso em: 09 mai. 2022.

Sellitto, Miguel Afonso. (2002) “INTELIGÊNCIA ARTIFICIAL: UMA APLICAÇÃO EM UMA INDÚSTRIA DE PROCESSO CONTÍNUO”, https://doi.org/10.1590/S0104-530X2002000300010. Acesso em: 10 mai. 2022.

Severino, Antônio Joaquim (2016), Metodologia do Trabalho Científico, São Paulo: Cortez, 24ª edição.

Silva, Jennifer A. S.;Mairink, Carlos H. P. (2019) “Inteligência artificial: aliada ou inimiga”, http://famigvirtual.com.br/famig-libertas/index.php/libertas/article/view/247. Acesso em: 27 abr. 2022.

SimpleID. (2021) “Como funciona o reconhecimento facial”, https://simpleid.ai/como-funciona-o-reconhecimento-facial/. Acesso em: 13 mai. 2022.

Skelton, Sebastian Klovig. (2021) “Ban UK police use of facial-recognition, House of Lords told”, https://www.computerweekly.com/news/252508053/Ban-UK-police-use-of-facial-recognition-House-of-Lords-told. Acesso em: 28 out. 2021.

Wiggers, Kyle. (2020) “NIST benchmarks show facial recognition technology still struggles to identify Black faces”, https://venturebeat.com/2020/09/09/nist-benchmarks-show-facial-recognition-technology-still-struggles-to-identify-black-faces. Acesso em: 14 set. 2021.