UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS

UNIDADE ACADÊMICA DE DIREITO

DAYANA DOS SANTOS LIMA

RELAÇÃO ENTRE O RECONHECIMENTO FACIAL E A SUA RESPONSABILIDADE JURÍDICA:

A LUZ DOS DIREITOS HUMANOS ESSA TECNOLOGIA PODE VIR A ENLEAR A DIGNIDADE HUMANA?

SOUSA

2023

DAYANA DOS SANTOS LIMA

RELAÇÃO ENTRE O RECONHECIMENTO FACIAL E A SUA RESPONSABILIDADE JURÍDICA:

A LUZ DOS DIREITOS HUMANOS ESSA TECNOLOGIA PODE VIR A ENLEAR A DIGNIDADE HUMANA?

Projeto de pesquisa apresentado a coordenação do Curso de Graduação em Direito da Universidade Federal de Campina Grande como requisito para conclusão do Curso de bacharelado em Direito.

Orientador: Dr. Guerrison Araujo Pereira De Andrade

SOUSA

2023

L732r Lima, Dayana dos Santos.

Relação entre o reconhecimento facial e a sua responsabilidade jurídica: a luz dos direitos humanos essa tecnologia pode vir a enlear a dignidade humana? / Dayana dos Santos Lima. – Sousa, 2023.

64 f. : il. color.

Monografia (Bacharelado em Direito) – Universidade Federal de Campina Grande, Centro de Ciências Jurídicas e Sociais, 2023.

"Orientação: Prof. Dr. Guerrison Araujo Pereira de Andrade".

Referências.

1. Processo Penal. 2. Dignidade Humana. 3. Reconhecimento Facial. 4. Constituição Federal. 5. Direito Processual Penal. 6. Direitos Humanos. I. Andrade, Guerrison Araujo Pereira de. II. Título.

CDU 343.1(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

DAYANA DOS SANTOS LIMA

RELAÇÃO ENTRE O RECONHECIMENTO FACIAL E A SUA RESPONSABILIDADE JURÍDICA:

A LUZ DOS DIREITOS HUMANOS ESSA TECNOLOGIA PODE VIR A ENLEAR A DIGNIDADE HUMANA?

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade Federal de Campina Grande (UFCG) – Campus Sousa/PB como requisito à obtenção do título de Bacharelado em Direito.

Orientador: Dr. Guerrison Araujo Pereira De Andrade

Data da aprovação: _____/_____/_____

Banca Examinadora:

_____

Prof. (a):

Universidade Federal de Campina Grande (UFCG)

_____

Prof. (a):

Universidade Federal de Campina Grande (UFCG)

_____

Prof. (a):

Universidade Federal de Campina Grande (UFCG)

SOUSA

2023

Agradecimentos

Tenho à minha disposição um espaço neste trabalho para elaborar algumas expressões de agradecimento a todos aqueles que me forneceram o ímpeto necessário para alcançar este patamar.

Em primeiro lugar, desejo externar minha gratidão a Deus, pois ele é a fonte do meu fortalecimento e bênçãos, sendo-lhe profundamente grato por todas as facetas da minha existência.

Manifesto também meus agradecimentos à minha família, que constitui o alicerce da minha jornada. São eles os pilares aos quais posso passear em qualquer instante, o meu refúgio seguro. A minha mãe, Luciene Bezerra dos santos, merece especial menção, pois sempre manteve em mim a diligência necessária. Meu pai, Darlan dos santos Lima, além de ser um eminente exemplo de honestidade, sempre me prestou apoio, infundindo-me coragem e motivação, mantendo uma crença contínua na minha pessoa. Igualmente, minhas primas Gilsilene Bezerra de Lima, e Quitéria Gezania dos santos, que foram ouvintes de toda a minha trajetória, e aos meus avós Vera lúcia dos Santos Lima, e Geraldo Almeida de Lima, cujas orações em meu nome e fé no meu sucesso sempre se fizeram presentes, bem como meu namorado, Lucas José Alves de França, que suportou incólume essa árdua etapa, incessantemente me incentivando e zelando por meu bem-estar.

Quero, também, estender minha gratidão as minhas amigas, Williane Pereira cruz e Maria Eduarda Alves Fernandes, que tiveram papel preponderante nesta trajetória, oferecendo auxílio nos momentos mais ansiosos. Almejo que essa amizade se perpetue através das décadas vindouras.

Por último, mas não menos importante, desejo expressar minha imensa gratidão ao meu orientador, Guerrison Araujo Pereira de Andrade, cujo trabalho e auxílio foram cruciais para concluir esta etapa. Rendo agradecimentos por todas as lições transmitidas.

RESUMO

Este trabalho teve como objetivo principal analisar a evolução do reconhecimento facial ao longo do tempo, considerando as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, e os riscos inerentes a essa tecnologia. O reconhecimento facial tem se destacado em diversas aplicações, porém, seu avanço suscita preocupações significativas relacionadas à privacidade e segurança dos dados pessoais. Nesse contexto, o estudo abordou tanto a evolução tecnológica quanto os aspectos legais e os riscos associados. A pesquisa teve início com uma revisão detalhada da evolução do reconhecimento facial, desde suas origens até as abordagens mais recentes baseadas em aprendizado de máquina. Foi destacada a crescente precisão e aplicabilidade da tecnologia em áreas como segurança, autenticação e interações cotidianas. Contudo, o foco principal recaiu sobre os impactos da LGPD no uso do reconhecimento facial. A LGPD, promulgada no Brasil em 2018, estabeleceu diretrizes rigorosas para a coleta, processamento e armazenamento de dados pessoais. O estudo explorou como essa legislação se aplica ao reconhecimento facial, abordando questões de consentimento, finalidade e direitos dos titulares dos dados. Foi investigado como as empresas e instituições se adaptaram para cumprir as exigências da LGPD ao implementar sistemas de reconhecimento facial. Ademais, o trabalho abordou os riscos associados à tecnologia de reconhecimento facial. Questões como viés algorítmico, coleta excessiva de dados e possíveis violações de privacidade foram discutidas em profundidade. A pesquisa também examinou casos de uso inadequado do reconhecimento facial que resultaram em repercussões negativas, tanto em termos de imagem quanto de consequências legais. Em resumo, este estudo apresentou a evolução do reconhecimento facial, considerando os parâmetros da LGPD e os riscos tecnológicos associados. Ao abordar as complexas interações entre tecnologia, regulamentação e ética, o trabalho destacou a necessidade de equilibrar os benefícios da inovação com a proteção dos direitos individuais. Como resultado, ofereceu uma visão abrangente das implicações do reconhecimento facial na sociedade contemporânea, promovendo uma reflexão crítica sobre seu uso responsável.

Palavras-chave: Dignidade humana; reconhecimento facial; Constituição Federal; dados pessoais; resultados vulneraveis

ABSTRACT

The main objective of this work was to analyze the evolution of facial recognition over time, considering the provisions of the General Law for the Protection of Personal Data (LGPD), Law nº 13.709/2018, and the risks inherent to this technology. Facial recognition has stood out in several applications, however, its advancement raises significant concerns related to the privacy and security of personal data. In this context, the study addressed both the technological evolution and the legal aspects and associated risks. The research kicked off with a detailed review of the evolution of facial recognition, from its origins to more recent machine learning-based approaches. The increasing accuracy and applicability of technology in areas such as security, authentication and everyday interactions was highlighted. However, the main focus was on the impacts of LGPD on the use of facial recognition. The LGPD, enacted in Brazil in 2018, established strict guidelines for the collection, processing and storage of personal data. The study explored how this legislation applies to facial recognition, addressing issues of consent, purpose and data subject rights. It was investigated how companies and institutions have adapted to comply with LGPD requirements by implementing facial recognition systems. In addition, the work addressed the risks associated with facial recognition technology. Issues such as algorithmic bias, excessive data collection, and potential privacy violations were discussed in depth. The research also examined cases of inappropriate use of facial recognition that resulted in negative repercussions, both in terms of image and legal consequences. In summary, this study presented the evolution of facial recognition, considering the LGPD parameters and the associated technological risks. By addressing the complex interactions between technology, regulation and ethics, the work highlighted the need to balance the benefits of innovation with the protection of individual rights. As a result, it offered a comprehensive view of the implications of facial recognition in contemporary society, promoting a critical reflection on its responsible use.

Keywords: Human dignity; facial recognition; Federal Constitution; personal data; vulnerable results..

Sumário

1 Introdução

Presentemente experienciamos uma era tecnológica que contribui substancialmente para a necessidade da sociedade, e um dos métodos advindos da tecnologia é o reconhecimento facial, que se expressa em um algoritmo que dispõe de imagens de pessoas, para que sejam manuseadas para identificação de possíveis crimes.

A relevância de compenetrar-se a esse tema é que ele possui uma grande relevância em nossa contemporaneidade pelo fato que acarreta responsabilidades estas que por copiosas vezes são inexploradas, consequentemente contribuindo para uma insegurança jurídica por parte dos cidadãos.

Ao questionarmos sobre os algoritmos presentes na prática forense transporta à tona a indagação sobre a veracidade, bem como a garantia de que são fatos neutros ou permeados de vieses pessoais que possam ferir a imparcialidade e cooperar para a consumação de injustiças, levando em conta, primordialmente, a conjuntura do racismo institucional e individual hodierno em nossa sociedade.

No que concerne singularmente ao tema da segurança pública, no tocante de serem utilizados vários métodos de identificação criminal no país, escolhemos como objeto do presente estudo a biometria de reconhecimento facial, diante da funcionalidade ao seu uso exponencial e à relevância de verificar a sua exatidão e neutralidade quando se trata de impor medidas arbitrarias e sancionatórias pelo Estado na execução do ius puniendi.

A pesquisa acudiu-se a perspectiva da disciplina legal da proteção de dados pessoais no Brasil, associada à análise de bibliografia, manuseou-se o método de direito comparativo, sobre o estudo de algoritmos, sua evolução e suas repercussões quanto a sua utilização. Destarte, vararemos a pesquisar a legislação em vigor que opera a matéria no ordenamento pátrio, com intuito de averiguar se exaure as hipóteses práticas e se existem ainda lapsos a serem retificados para asseverar a simultaneidade da tecnologia do reconhecimento

facial com direitos constitucionalmente garantidos, como o da dignidade da pessoa humana.

No que se refere a experiência do reconhecimento facial no Brasil chama especial atenção. Pois ao falarmos de vigilância pública e, consequentemente, em políticas criminais adotadas pelo Estado para uma maior incontestabilidade, é inverossímil deixar de mencionar sobre racismo e a seletividade do sistema penal no país. Vastamente amparado na busca por um determinado tipo criminoso e ainda com grande porção de preconceito racial exposta como marca dos tempos de escravidão, o sistema penal no Brasil atualmente aflige notadamente mais pessoas negras do que brancas.

Embora o tema seja bastante pertinente não possui legislação especifica para reger a respeito do reconhecimento facial, amparando-se somente na lei 13.709, conhecida pela lei da proteção de dados, informações das quais devem serem emitidas com a permissão dos cidadãos, conquanto, na realidade ocorre que imagens são muitas vezes são colhidas em câmeras de segurança, por exemplo, e estas são utilizadas para a identificação de pessoas a fim de resolução de possíveis praticas criminais.

Isto posto, a forma como são obtidos esses dados proporciona uma insegurança jurídica, visto que tais dados são realizados através de uma inteligência artificial, que de acordo com especialistas, apresentam imprecisões como indução ao erro, preconceito bem como pode levar a um constrangimento indesejado a pessoas inocentes.

2 Historicidade do reconhecimento facial

É inegável o quanto a tecnologia vem aduzindo profusos benefícios para a sociedade, proporcionando a interligação de pessoas em diferentes localidades, facilitando além da comunicação, a celeridade em resolução de problemas, e assim como em outras searas, no campo jurídico esse mecanismo apresenta vantagens eximias.

Uma das realizações advindas desse cosmo tecnológico, foi o reconhecimento facial, como o próprio nome elucidativo, trata-se de um instrumento instruído para reconhecer qualquer indivíduo, baseando-se em padrões capazes de identificar rostos humanos através da inteligência artificial.

Woodrow Bledsoe, juntamente com Helen Chan e Charles Bisson, da Panoramic Research, Palo Alto, California, perscrutou computadores de programação no sentido de discernir rostos humanos. Tais imagens foram fornecidas por uma agência de inteligência anônima, escassamente desse trabalho fora publicado.

Cedido um avultado banco de dados de imagens, referente a um livro de fotos de caneca e uma fotografia, entretanto, o problema era selecionar no banco de dados um pequeno mescla de registros dessa maneira um dos registros da imagem adequou-se à fotografia. O êxito do programa poderia ser apreciado em termos da razão da lista de conclusões para o número de registros no banco de dados.

Nesse ínterim, Bledsoe minudenciou o seguinte infortúnio:

> “Esse problema de reconhecimento é dificultado pela grande variabilidade na rotação e inclinação da cabeça, intensidade e ângulo de iluminação, expressão facial, envelhecimento etc. Algumas outras tentativas de reconhecimento facial por máquina permitiram pouca ou nenhuma variabilidade nessas quantidades. O método de correlação (ou correspondência de padrões) de dados ópticos não processados, que é frequentemente usado por alguns pesquisadores, certamente falhará nos casos em que a variabilidade é grande. Em particular, a

> correlação é muito baixa entre duas imagens da mesma pessoa com duas rotações diferentes da cabeça.” (Bledsoe,1966).

Nessa perspectiva, é possível interpretar que o método do reconhecimento facial, apresentava falhas das quais aspectos como uma mera inclinação de cabeça poderia intricar a identificação, e consequentemente tal artificio não apresentaria plena veracidade, de modo que essa garantia acarretaria de certa forma em uma incredibilidade do programa.

Em experimentos realizados no instituto de pesquisa de Stanford, Peter Hart cientista da computação e empresário americano, em experiências realizadas em um banco de dados com mais de 2000 fotografias, o computador superava consistentemente os seres humanos quando apresentada as mesmas tarefas de reconhecimento, para Peter Hart o projeto havia naquele momento funcionado.

indubitavelmente, os computadores possuem mais complexidade para caracterizar rostos do que triunfar a reconhecidos mestres no xadrez, a título de exemplo. Irrefutavelmente a ultrapassagem desses problemas ainda temporizaria inúmeros anos.

Em virtude dos aperfeiçoamentos na tecnologia da câmera, procedimentos de mapeamento, preparação de máquina e fugacidade de processamento, o reconhecimento facial logrou a sua emancipação. E passou a ser manuseado como meio de segurança pelo Estado.

A preponderância dos sistemas opera a tecnologia de câmera 2D, na qual agrega uma imagem plana de um rosto e mapeia "pontos nodais, que são o tamanho e o formato dos olhos, nariz, maçãs do rosto, distância entre as extremidades da face e etc. O sistema infere a posição relativa dos pontos e converte os dados em um código numérico. Os algoritmos de reconhecimento pesquisam um banco de dados armazenado de rostos para auferir uma analogia correta.

A Tecnologia 2D executa-se em condições estáveis e com uma iluminação apta, o controle de passaporte emprega esse método. Todavia ela não é considerada idônea em ambientes negrumes, deste modo não obtém

resultados positivos quando os objetos se movimentam. Sendo exequível uma falsificação através de uma simples fotografia, por exemplo.

Em 2019 a Apple, empresa famigerada na qual projeta e vende produtos eletrônicos de consumo, software de computador e computadores pessoais, adere a modernização ao implementar a técnica do reconhecimento facial com o propósito de desbloquear os seus dispositivos, como o iPhone e o iPad Pro proporcionando mais segurança ao consumidor.

O meio de identificação facial, vem paulatinamente adentrando na sociedade contemporânea, sendo adotada por outros ordenamentos jurídicos para vigilância pública, no entanto, a sua aplicação apresentam inconsistências, tanto na questão da proteção dos dados, quanto no que tange a sua admissibilidade como prova.

Embora expresse um corpulento comprazimento que envolve o recurso, se faz necessário ponderar as suas limitações que transparecem o estágio em que se encontra, como bem mencionado em um relatório da Electronic Frontier Foundation (EFF):

> "...A adoção de tecnologias de reconhecimento facial como essas está ocorrendo sem supervisão significativa, sem testes de precisão adequados dos sistemas conforme eles são realmente usados em campo e sem a promulgação de proteções legais para evitar o uso indevido interno e externo. Isso levou ao desenvolvimento de sistemas não comprovados e imprecisos que afetarão os direitos constitucionais e afetarão desproporcionalmente as pessoas de cor." (LYNCH,2018)

As taxas de acerto dos sistemas caem notoriamente em função de diversos fatores como iluminação, fundo da imagem, posicionamento do indivíduo na imagem, bem como homogeneidade fenotípica, principalmente se essas imagens são colhidas através de seguimentos de vídeo, coadjuva para um

falso positivo, que corresponde de forma errônea o rosto analisado a outro ao qual ele não compatibiliza de fato.

Nesse sentido, observa-se que a evolução da era tecnológica, pode contribuir substancialmente para a agilidade na vivencia dos cidadãos, apesar disso é imprescindível uma cautela em lidar com ela, do contrário tem potencial de dilacerar o princípio da dignidade da pessoa humana.

2.1 Reconhecimento facial na utilização da segurança pública em outros ordenamentos jurídicos.

Ao indigitarmos as implicações sociais mais aflitivas da inteligência artificial, analisamos seu intuito quanto a vigilância generalizada em vários ordenamentos jurídicos ao redor do mundo, e nas implicações, para direitos e liberdades. Em sui generis, consideramos o uso crescente de reconhecimento facial e uma subclasse de reconhecimento facial, e avaliar as progressistas demandas por regulamento.

Diante a essa eventualidade, é consternador pensar que a nossa privacidade, dados, direitos, liberdade, garantias estão de certa forma sendo tocados, de modo que, até que ponto essa tecnologia pode adentrar em nosso cotidiano, bem como quais serão os desfechos oportunos para aquele que o fizerem de forma irresponsável.

Nesse sentido, de acordo com uma pesquisa realizada no Instituto AI Now, Universidade de Nova York, apresenta possíveis riscos desse utensilio de segurança sem a devida preocupação quanto aos impactos perante a sociedade.

> “o papel da IA na vigilância generalizada se expandiu imensamente nos EUA, na China e em muitos outros países em todo o mundo. Isso é visto no uso crescente de redes de sensores, rastreamento de mídia social, reconhecimento facial e reconhecimento de afeto. Essas expansões não apenas ameaçam a privacidade individual, mas também aceleram a automação da vigilância e, portanto, seu alcance e difusão. Isso apresenta novos perigos e amplia muitas preocupações de longa data.” (INTITUTO AI NOW, 2018)

É pertinente salientar que os governos estão expandindo rapidamente o uso de sistemas automatizados, para que haja uma celeridade maior em resoluções de dilemas, no que tange a criminalidade, assim como no objetivo de evitar que possíveis crimes venham a ocorrer, países como o EUA ampara-se nesse mecanismo também para evitar situações problemáticas como terrorismo, ou migrações indesejadas.

No entanto, os direitos civis ficam vulneráveis, agências governamentais estão adquirindo e implantando sistemas automatizados de decisão, (ADS), trata-se daquelas publicidades que surgem durante o uso em mecanismos de pesquisa, por exemplo. No entanto, muitos desses sistemas não foram testados e mal projetados para suas tarefas, resultando em violações ilegais e muitas vezes inconstitucionais dos direitos individuais.

Não obstante, quando eles cometem erros e tomam decisões erradas, a capacidade de questionar, contestar e retificar isso costuma ser fatigante ou inverossímil. Um número reduzido de agências está tentando fornecerem mecanismos de transparência, devido processo e outros direitos básicos, mas o sigilo comercial e leis semelhantes ameaçam impedir a auditoria e o teste adequado desses sistemas.

Com base nos esforços proativos da agência e em litígios estratégicos recentes, delineamos caminhos para a responsabilidade de publicidades que na maioria das vezes, indesejadas, apresentam insegurança aos usuários, pondo em risco a sua privacidade, e que desventuradamente seus dados são repassados sem a sua permissão.

Quando esse tipo de problema ocorre, eles são frequentemente difíceis reverte-los. Escassas ADS são arquitetadas ou implementadas de maneira que venha a permitir desembaraçadamente de modo que os indivíduos afetados contestem, mitiguem ou corrijam decisões adversas ou incorretas.

Outrossim, a discrição humana e a idoneidade de intervir ou revogar a determinação de um sistema geralmente são substancialmente limitadas ou

removidas dos gerentes de caso, assistentes sociais e outros treinados para entender o contexto e as nuances de uma determinada pessoa e situação.

Colaboradores da linha de frente tornam- se meros intermediários, comunicando decisões inflexíveis tomadas por sistemas automatizados, ou seja, impossibilitando alterações. Detectar tais problemas exige supervisão e monitoramento. Também requer acesso a dados que por inúmeras vezes não estão disponíveis para advogados e para o público, nem monitorados por agências governamentais.

Esses sistemas também não são normalmente construídos com escassa supervisão ou responsabilidade. Isso dificulta a descoberta de resultados automatizados problemáticos, especialmente porque tais erros e evidências de discriminação frequentemente se manifestam como danos coletivos, apenas reconhecíveis como um padrão em muitos casos individuais.

Segundo pesquisadores da ACLU e da Universidade da Califórnia (UC), testaram a ferramenta Rekognition da Amazon comparando as fotos de membros efetivos do Congresso dos Estados Unidos com um banco de dados contendo 25.000 fotos de pessoas que foram presas.

Os resultados mostraram níveis significativos de imprecisão: o Rekognition da Amazon identificou incorretamente 28 membros do Congresso como pessoas do banco de dados de prisões. Além disso, os falsos positivos ocorreram de forma desproporcional entre membros do Congresso não brancos, com uma taxa de erro de quase 40% em comparação com apenas 5% para membros brancos.

Baseados nesses dados supracitados podemos interpretar que a tecnologia de reconhecimento facial é, um meio inexato que pode vir a ferir a dignidade da pessoa humana, de modo que pelo fato de ser um sistema preconceituoso, logo, a suas atribuições irão muitas vezes de maneira errônea atribuir um resultado impreciso.

Os problemas técnicos endêmicos presentes nos sistemas de reconhecimento facial significam que falsos positivos continuarão a ser um

obstáculo comum no futuro. As tecnologias de reconhecimento facial funcionam adequadamente quando todas as fotografias são tiradas com uma boa iluminação semelhante e de uma perspectiva frontal como uma foto de identificação, por exemplo.

No entanto, quando as fotos contrastadas entre si contêm iluminação, sombras, planos de fundo, poses ou expressões distintas, as taxas de inexatidão podem ser significativas.

O reconhecimento facial também é extremamente desafiador ao tentar identificar alguém em uma imagem tirada em baixa resolução ou em um vídeo e tem um desempenho pior no geral à medida que o tamanho do conjunto de dados aumenta, em parte porque muitas pessoas em uma determinada população parecem semelhantes umas às outras.

Por fim, também é menos preciso com grandes discrepâncias de idade por exemplo, se as pessoas forem comparadas com uma foto tirada de si mesmas quando eram dez anos mais jovens, haverá também probabilidade de resultados dúbios.

2.2 Repercussão do mecanismo na liberdade civil

Ao analisarmos alguns dados já apresentados, podemos indagar, quais são os efeitos de uma frequente vigilância a partir da tecnologia de reconhecimento facial? Até que ponto estamos seguros? se esses dados recolhidos muitas vezes sem o nosso consentimento, pode vir a afetar ou não os direitos fundamentais como liberdade de expressão, igualdade, intimidade.

É inegável, que há uma expectativa de maior segurança, em domínio público e privado, e de acesso facilitado a produtos e serviços. entretanto, com a forte aplicação dessa tecnologia, passa-se a ser regularmente controlado, o que sem dúvidas traz diversos questionamentos em relação à proteção de direitos inalienáveis presentes na nossa Constituição federal.

Não são escassos os riscos gerados pelo reconhecimento facial, principalmente a partir do tratamento de dados sensíveis, sendo necessário

debater como deve ocorrer a utilização dessa ferramenta. A lacuna que é expressamente notada ao não termos uma legislação especifica, e a insegurança jurídica que se dá por ausência dessa normalização.

Os dados pessoais dos indivíduos trata-se de direitos individuais da qual o seu fornecimento só deveria ser oportunizado em uma relação mutua de consentimento entre o titular deste e o seu tomador. Assim explica Bioni (2020):

> "Há uma 'economia de vigilância' que tende a posicionar o cidadão como um mero expectador das suas informações. Esse é um diagnóstico necessário, sem o qual não se poderia avançar na investigação do papel do consentimento na proteção dos dados pessoais, especialmente, por rivalizar com tal condição de passividade atribuída ao cidadão quanto ao fluxo de suas informações pessoais." (Bioni, 2020)

Todavia, o usufruto desses dados propostos de reconhecimento facial impactaria claramente os direitos da Quarta Emenda e as atividades protegidas pela Primeira Emenda e restringiriam o seu texto. Se as agências de aplicação da lei adicionarem fotos de multidão, câmera de segurança em seus bancos de dados, qualquer um pode acabar em um banco de dados sem seu conhecimento, de modo que mesmo que não seja suspeito de um crime por estar no lugar errado na hora errada, ajustando-se a um estereótipo que alguns na sociedade consideram uma ameaça ou participando de atividades "suspeitas", como protesto político em espaços públicos repletos de câmeras.

Alguns usos propostos de reconhecimento facial impactariam claramente os direitos da Quarta Emenda, as atividades protegidas pela Primeira Emenda e restringiriam a fala. Se as agências de aplicação da lei adicionarem fotos de multidão, câmera de segurança e DMV em seus bancos de dados, qualquer um pode acabar em um banco de dados sem seu conhecimento - mesmo que não seja suspeito de um crime por estar no lugar errado na hora errada.

Em uma reportagem apresentada pelo site globo 2021, foi apresentado um individuo que passou por um reconhecimento fotográfico, e enquanto estava ajudando a um amigo a concertar o carro, foi abordado pela polícia, a sua foto

foi anexada em um banco de dados, não obstante, ele passou por esse constrangimento nove vezes, sendo inocente.

O mesmo ainda relata que tem medo de sair nas ruas e a qualquer momento ser preso, isso demonstra o quão atroz pode ser uso da ferramenta, sem a devida responsabilidade, quando a mesma sendo o único meio de prova para atribuir um crime a alguém.

No âmbito público, o reconhecimento facial tem sido manuseado hodiernamente para a segurança pública, controle de fronteiras, aspectos de prevenção de fraudes e roubos de identidade, proteção da saúde pública na área da educação e no transporte público.

Dado o histórico de uso inapropriado de dados coletados pelas autoridades policiais com base nas crenças religiosas, raça, etnia e tendências políticas das pessoas, inclusive durante o longo mandato do ex-diretor do FBI J. Edgar Hoover e durante os anos seguintes a 11 de setembro de 2001, os americanos se preocupam com a expansão dos bancos de dados de reconhecimento facial do governo.

Como outros programas de biometria que coletam, armazenam, compartilham e combinam dados confidenciais e exclusivos, a tecnologia de reconhecimento facial representa ameaças críticas à privacidade e às liberdades civis.

Nossa biometria é única para cada indivíduo, não podendo ser modificada e, muitas vezes, é facilmente acessível. O reconhecimento facial, no entanto, carrega consigo os riscos inerentes a outras biometrias a um novo nível porque é muito mais difícil impedir a coleta de uma imagem do seu rosto.

A possibilidade de que esse controle social com uso de tecnologia de vigilância, estabelecido para o domínio de possíveis atos criminais, pode vir a atravessar as fronteiras da prisão, e que ao invés de controlar a criminalidade estaria desencadeando um novo problema, como relata Jeremy Bentham:

> “particularmente importante naqueles casos em que o inspetor, além de ver que eles se conformam às regras em vigor, tem que lhes fornecer aquelas instruções transientes e incidentais que são necessárias no início de qualquer tipo de atividade. E penso que não é necessária muita argumentação para provar que a atividade de inspeção, como qualquer outra, será exercida a um grau maior de perfeição na medida em que menores forem os problemas causados por seu exercício.” (Jeremy bethan, 2019)

Nota-se que em copiosas vezes o reconhecimento facial apesar de ter um objetivo positivo, proporciona graves falhas, que podem desencadear problemas maiores do que mesmo aqueles que a priori foram escolhidos para os resolverem, visto que as massas de pessoas prejudicadas diante das falhas tecnológicas vêm apresentando números significativos.

Ao que podemos averiguar, todo esse processo de identificação, possui uma pré-conceituação de indivíduos, e a proteção de dados que se tratam de um direito fundamental, está sendo violado corriqueiramente, uma vez que, nós expomos nossos rostos ao público toda vez que saímos, e muitos de nós compartilhamos imagens de nossos rostos online quase sem restrições sobre quem pode ou não os acessar.

O reconhecimento facial, portanto, permite a captura e identificação de imagens ocultas, remotas e em massa. As fotos que pode acabar em um banco de dados pode incluir não apenas o rosto de uma pessoa, mas também como ela está vestida e possivelmente com quem ela está.

O acervo de fotografias facilmente identificáveis implica em maculação a direitos e valores de liberdade de expressão e liberdade de associação sob a primeira Emenda, singularmente porque fotografias de identificação facial de multidões ou protestos políticos podem ser capturadas em público, online e por meios públicos e semipúblicos sites de mídia social sem o conhecimento dos indivíduos.

Nesse sentido podemos indagar, como que algo que não o fora permitido, possui admissibilidade como prova, uma vez que é protegido por tratar de um direito fundamental pela Constituição Federal? Além de apresentar uma invasão de privacidade explicita, não há o que refutar quando se sentir lesado.

A morte de Freddie Gray, jovem negro da cidade de Baltimore, nos EUA, que sofreu uma lesão na coluna vertebral enquanto era levado por policiais para a delegacia. Ele entrou em coma e morreu dias depois, aos 25 anos. estava em sob custódia policial, o Departamento de Polícia de Baltimore exibiu fotos de mídia social em um banco de dados de reconhecimento facial para identificar os manifestantes e prendê-los.

O desfecho dessa trágica história, segundo o El País, no dia 1º de maio de 2015, foi anunciado que teriam entrado com acusações contra seis policiais por homicídio, uma vez que Gray "sofreu uma lesão crítica no pescoço como resultado de se seus pés e sem cinto de segurança dentro da van". Vale frisar que, a vítima já se encontrava imobilizada não apresentando risco de fuga nem mesmo de agressão aos policiais.

Três dos policiais que haviam sido acusados de homicídio culposo (homicídio sem a intenção de matar) e um enfrentou uma acusação adicional de homicídio de segundo grau, que é quando não há premeditação do crime, mas, o acusado age com indiferença mesmo sabendo que pode causar a morte de alguém.

Porém, todos os policiais foram libertados da prisão após pagarem fiança. Dois deles pagaram uma quantia de 250 mil dólares enquanto os outros quatro pagaram 350 mil. No ano de 2016, a Justiça decidiu por arquivar o caso.

Tal caso repercutiu negativamente, fazendo com que houvesse diversos protestos, exigindo-se, mas cautela dos policiais para pessoas negras, onde apresentavam na história vários casos de abusos de poder, e que resultavam em tragédias como essa supracitada.

A tecnologia de reconhecimento facial foi utilizada para perseguir e prender esses manifestantes de Baltimore que reagiram ao assassinato policial de Freddie Gray, com objetivo de inibir os protestos.

O Homeland Security, “Segurança Interna” vigiou manifestantes em 15 cidades usando vigilância por drones, enquanto câmeras do corpo policial, equipadas com tecnologia de reconhecimento facial, capturaram imagens dos mesmos. Sendo utilizado descontroladamente, ou seja, agora, a ferramenta passou a ser uma das ferramentas mais poderosas do policiamento.

Em 2013, um estudo envolvendo muçulmanos em Nova York e Nova Jersey constatou que a vigilância policial excessiva em comunidades muçulmanas teve um efeito significativamente de acobardar atividades protegidas pela Primeira Emenda.

De acordo com a diretora do programa dos EUA da Human Rights Watch. “Investigar comunidades com base somente na religião é profundamente prejudicial aos direitos humanos.” Especificamente, as pessoas estavam menos inclinadas a frequentar mesquitas que pensavam estar sob vigilância do governo para se envolver em práticas religiosas em público, ou mesmo para se vestir ou deixar o cabelo crescer de maneira que possa sujeitá-los à vigilância com base em sua religião.

Nessa investigação e perseguição a grupos religiosos a Associated Press também informou que a polícia da cidade de Nova Iorque monitorou estudantes universitários muçulmanos em todo o nordeste dos Estados Unidos, inclusive na Universidade de Syracuse, a Universidade de Yale e a Universidade da Pennsylvania, durante 2006 e 2007. Vários presidentes universitários criticaram as operações policiais da cidade de Nova Iorque publicamente.

> “As autoridades de Nova Iorque deveriam ter muito tempo que construir relações de confiança com minorias, ao invés de miná-las, é a melhor maneira de garantir a segurança da cidade. A investigação completa e transparente do programa de vigilância seria um passo significativo para restabelecer essa confiança”. (PARKER,2013).

Diante dessas violações a direitos e a liberdade religiosa as pessoas também eram menos propensas a se envolver com outras pessoas em sua comunidade que não conheciam por medo de que essa pessoa pudesse ser um informante do governo ou um radical. Resultando no afastamento social dessa população bem como a restrição de práticas religiosas.

Os pais desencorajavam seus filhos a participar de movimentos sociais, religiosos ou políticos muçulmanos. Os donos de empresas tomaram medidas conscientes para silenciar a discussão política desligando a Al-Jazeera em suas lojas, e os ativistas

autocensuraram seus comentários no Facebook. Tudo isso impactou de maneira desfavorável à vida desses indivíduos, de modo que, pessoas de cor poderiam ser vítimas dos riscos de falsos positivos discutidos acima provavelmente afetarão desproporcionalmente os afro-americanos e outras pessoas de cor.

Uma pesquisa incluindo pesquisa Vigilância governamental como essa pode ter por consequência impossibilitar no que tange à disposição dos americanos de se engajar em debates públicos e se associar com outros cujos valores, religião ou pontos de vista políticos podem ser considerados diferentes dos seus.

Há muito estudam a “espiral do silêncio” o significativo efeito inibidor sobre a disposição de um indivíduo de divulgar publicamente opiniões políticas quando acredita que suas opiniões diferem da maioria. Optando muitas vezes ora por ficar em silencio não expressando sua opinião sobre determinado assunto, ora indo pelo pensamento da maioria, evitando externar o seu real ponto de vista.

Em 2016, uma pesquisa sobre usuários do Facebook documentou o efeito silenciador sobre as opiniões divergentes dos participantes na sequência do conhecimento generalizado da vigilância do governo, os participantes eram muito menos propensos a expressar opiniões negativas sobre a vigilância do governo no Facebook quando percebiam que essas opiniões estavam fora da norma.

Tais situações estarrecedoras mostram os riscos reais para o discurso e as atividades protegidos pela Primeira Emenda na vigilância excessiva do governo especialmente quando esse discurso representa uma minoria, bem como quando há uma diferenciação de poderes, em uma relação do poder público em detrimento a um particular, quando houver uma concepção divergente, o desfavorecido, ou seja, a minoria estará sempre em um degrau abaixo.

Embora ainda não pareçamos estar no ponto em que o reconhecimento facial esteja sendo usado unicamente para monitorar o público, estamos em um estágio em que o governo está construindo os bancos de dados para tornar esse monitoramento possível. Devemos colocar verificações significativas no uso do reconhecimento facial pelo governo.

Devendo ser estabelecido até onde esse monitoramento digital poderá adentrar na vida dos cidadãos, em quais situações, a privacidade que está amparada na nossa Carta Magna deve efetivamente ser respeitada, fazendo a alusão a pratica do bom direito onde diz que o seu direito acaba quando começa o de outrem.

3 Os riscos inerentes à implementação da inteligência artificial e seus vieses

É incontestável que o progresso tecnológico tem trazido notáveis avanços para a sociedade, promovendo maior agilidade nas pesquisas, rapidez nas comunicações e uma sensação de ter o mundo literalmente ao alcance das mãos. O impacto transformador da tecnologia na sociedade tem sido fonte de benefícios significativos. No entanto, é importante reconhecer que, em contrapartida, a tecnologia não está isenta de falhas e preocupações que podem se afastar de sua finalidade central, que é facilitar a vida das pessoas.

A implementação da inteligência artificial tem sido reconhecida como uma ferramenta de natureza ambígua, que pode trazer tanto benefícios quanto desafios. Benjamin Cheatham discorre sobre uma série de aspectos que caracterizam as possíveis falhas inerentes à inteligência artificial.

Essas falhas abrangem questões relacionadas à disponibilidade e qualidade dos dados utilizados, as instabilidades tecnológicas que podem surgir no desenvolvimento e implementação de sistemas de IA, bem como as preocupações com a segurança e a vulnerabilidade às brechas no contexto da inteligência artificial. Por fim, surgem as questões críticas referentes à interação entre humanos e sistemas de IA, que envolvem desafios éticos, legais e sociais a serem abordados e mitigados. Ele ainda acrescenta:

> "... E essas são apenas as consequências não intencionais. Sem salvaguardas rigorosas, funcionários descontentes ou inimigos externos podem ser capazes de corromper os algoritmos ou utilizar um aplicativo de IA de forma maldosa. " (Cheatham,2019)

No que diz respeito ao reconhecimento facial, uma ferramenta amplamente fundamentada na tecnologia, é importante reconhecer que, embora tenha uma intenção benéfica em sua essência, sua implementação pode ser permeada por falhas significativas. Essas falhas podem representar uma ameaça não apenas à dignidade humana dos indivíduos, mas também ao próprio âmago moral dos que se tornam vítimas de uma tecnologia imprecisa. O reconhecimento facial, embora busque proporcionar benefícios, é suscetível a riscos que requerem uma avaliação cuidadosa e abordagens éticas para garantir

que seu uso não comprometa injustamente os direitos individuais e a integridade moral daqueles afetados por sua aplicação imprecisa.

Um dos principais elementos para a identificação é o arquivo de dados, há uma crescente dificuldade em incorporar, classificar, vincular e utilizar de forma adequada desses dados, devido ao aumento significativo de dados desestruturados provenientes de fontes como a internet, mídias sociais, dispositivos móveis, sensores e Internet das Coisas. Esse cenário resulta em uma maior propensão a armadilhas, como o uso incorreto ou a divulgação inversa de informações, prejudicando assim a integridade e a confiabilidade dos sistemas de reconhecimento facial.

Essa situação é frequentemente observada em relação a indivíduos pertencentes a comunidades negras, uma vez que suas características faciais apresentam similaridades que podem resultar em resultados imprecisos por parte da ferramenta de reconhecimento facial. Além disso, um exemplo adicional que merece destaque é o registro de imagens de pessoas que foram injustamente detidas, mesmo após terem comprovado sua inocência. Essa inclusão em bancos de dados de reconhecimento facial acarreta, de certa forma, uma sentença perpétua, afetando negativamente a liberdade e a justiça desses indivíduos.

No ano de 2022, o portal R7 divulgou um incidente de erro no sistema de reconhecimento facial, em que, com base em imagens de segurança, um indivíduo foi apreendido erroneamente. As autoridades, utilizando o sistema de reconhecimento facial, identificaram um cidadão como suspeito, mas um laudo posterior confirmou que o resultado obtido era impreciso. O responsável pelo crime em questão, ao contrário do indivíduo detido, possuía tatuagens como características distintivas. Esse incidente ilustra a falibilidade do sistema de reconhecimento facial, ressaltando a importância de avaliações cuidadosas e procedimentos de verificação para evitar resultados incorretos e injustos.

> "...Um laudo produzido por papiloscopistas da Polícia Civil do Distrito Federal apontou um morador do DF como autor de um crime que, ao que tudo indica, ele não teria cometido. Eduardo Wendel Pereira do Santos, de 23 anos, foi considerado suspeito de assaltar um ônibus em Brasília. Mas uma outra avaliação, feita por peritos criminais da PCDF,

> com análise de tatuagens, contrapõe a conclusão "com o máximo grau de plausibilidade". Esse foi o segundo possível erro recente do Instituto de Identificação que culminou com um suspeito inocente da acusação. “ (PORTAL R7, 2022).

Conforme anteriormente mencionado, esse incidente representa mais um exemplo de falha no sistema de reconhecimento facial ocorrido no Distrito Federal. No ano de 2021, José Domingos Leitão, um pedreiro de 52 anos, foi erroneamente preso pelas autoridades locais com base no reconhecimento facial, que o identificou como o autor de um crime ocorrido na capital. No entanto, verifica-se que ele é residente de Ilha Grande, no estado do Piauí, e estava presente na referida cidade no momento do delito em questão. Esse caso evidencia as consequências adversas que podem surgir devido a falhas no sistema de reconhecimento facial, destacando a importância de medidas de salvaguarda e verificações rigorosas para evitar equívocos e injustiças.

Outro aspecto essencial a ser considerado no contexto do reconhecimento facial é a existência de desestabilizações tecnológicas, tanto relacionadas aos processos quanto à própria tecnologia em todo o cenário operacional. Essas desestabilizações podem resultar em efeitos adversos no desempenho dos sistemas de inteligência artificial. Por exemplo, falhas na infraestrutura tecnológica, como interrupções no fornecimento de energia, problemas de conectividade ou erros de hardware, podem comprometer a capacidade dos sistemas de reconhecimento facial em realizar suas funções de maneira precisa e confiável.

Além disso, alterações ou atualizações inadequadas nos algoritmos ou nas configurações dos sistemas também podem causar instabilidades, afetando negativamente a eficácia e a acurácia dos resultados obtidos. É fundamental adotar medidas adequadas de monitoramento, manutenção e aprimoramento contínuo para minimizar as desestabilizações tecnológicas e garantir um desempenho consistente e confiável dos sistemas de reconhecimento facial.

Em um estudo realizado pela Universidade Federal de Campina Grande, o professor Eanes Pereira explica que nos sistemas de acesso biométrico, a face pode ser utilizada para permitir o acesso. No entanto, antes que a face possa ser reconhecida, é necessário detectá-la. A detecção facial, de forma geral,

consiste em determinar se existe uma face na imagem ou no vídeo, e em obter informações sobre a localização, largura e altura de um retângulo que englobe a face.

Esse retângulo é então recortado e processado nas etapas seguintes. No entanto, se houver um risco maior de falha na detecção facial em pessoas do gênero feminino em comparação com pessoas do gênero masculino, isso pode levar a situações em que uma pessoa do gênero feminino possa passar por constrangimentos desnecessários ou enfrentar dificuldades para ter sua face detectada corretamente.

> "Os resultados obtidos mostram que todos os cinco detectores de faces analisados apresentam alto risco de não detectar faces do gênero feminino e de pessoas entre 46 e 85 anos. Em situações em que a taxa de predição positiva é mais frequente para um determinado grupo (por exemplo, gênero masculino) do que qualquer outro, geralmente também será mais propenso a ter uma maior taxa de falso positivo. Além disso, os grupos de tons de pele escura são os apontados com maior risco de não serem detectadas faces para quatro dos cinco detectores de rosto avaliados. Dessa forma, o trabalho aponta a necessidade de investigar a existência de erros causados por viés ou injustiça, que podem estar presente em conjuntos de dados ou modelos de aprendizado de máquina." (Portal UFCG, 2021).

É evidente que indivíduos do gênero masculino afrodescendentes são os mais afetados pelos resultados incorretos do sistema de reconhecimento facial. Essas pessoas enfrentam uma taxa desproporcionalmente maior de falsos positivos, ou seja, são erroneamente identificadas como suspeitas ou culpadas. Essa disparidade decorre de diversos fatores, incluindo a qualidade e a representatividade dos dados utilizados no treinamento dos algoritmos de reconhecimento facial, bem como a ineficiência na capacidade de produzir resultados precisos para essa demografia específica.

Como resultado, esses indivíduos são mais suscetíveis a enfrentar injustiças, discriminação e violações de seus direitos, o que reforça a necessidade urgente de abordar e mitigar esses viéses e falhas sistêmicas no desenvolvimento e na implementação de tecnologias de reconhecimento facial. É imprescindível ressaltar que a viabilidade de incursões por hackers não é

descartada quando o tema em questão é inteligência artificial, bem como a invasão de dados que podem ser inseridos no sistema de reconhecimento facial. Em outras palavras, os sistemas encontram-se vulneráveis a ataques cibernéticos e invasões.

Por ser uma ferramenta concebida por seres humanos, inevitavelmente está sujeita a falhas. Nos meandros do processo de análise de dados, equívocos na programação, negligências na gestão de dados e discrepâncias nos conjuntos de dados de treinamento podem acarretar comprometimento substancial da equidade, privacidade, segurança e conformidade regulatória. Na ausência de salvaguardas rigorosas, indivíduos insatisfeitos internos ou adversários externos podem potencialmente adulterar os algoritmos ou explorar de maneira maliciosa um aplicativo de inteligência artificial.

São obstáculos significativos que a inteligência artificial enfrenta no âmbito do reconhecimento facial, embora seja inquestionável que sua intenção inicial seja positiva. No entanto, a possibilidade de obter resultados imprecisos é considerável, e devido à natureza intrinsecamente discriminatória dessa ferramenta, ainda há uma necessidade substancial de aprimorar o sistema.

Ademais, embora os controles abrangentes em toda a organização sejam de vital importância, é raríssimo que sejam suficientes para mitigar todos os possíveis riscos. Geralmente, é necessário um nível adicional de rigor e adaptabilidade, haja vista que os controles necessários são influenciados por fatores como a complexidade intrínseca dos algoritmos, as exigências dos dados envolvidos, a natureza das interações entre seres humanos e máquinas (ou até mesmo entre máquinas), o potencial de exploração por parte de atores mal-intencionados e o grau de incorporação da inteligência artificial nos processos empresariais.

Medidas conceituais de controle, que podem ser iniadas com regulamentações de casos de uso, são ocasionalmente indispensáveis. Desse modo, é essencial implementar controles direcionados à análise e aos dados específicos, abrangendo requisitos de transparência, bem como mecanismos de feedback e monitoramento, como análises de desempenho para identificar possíveis degradações ou viés.

É de conhecimento geral que o reconhecimento facial carece de uma regulamentação específica, sendo atualmente abrangido pela Lei nº 13.709/2018, que trata da proteção de dados. Contudo, é importante ressaltar a existência do Projeto de Lei 2392/22, que visa proibir o uso de tecnologias de reconhecimento facial para fins de identificação nos setores público e privado, a menos que seja realizado um relatório prévio de impacto à privacidade das pessoas.

Portanto, ainda há uma ampla lacuna de conhecimento a ser preenchida acerca dos potenciais riscos do reconhecimento facial, os quais a sociedade enfrenta no contexto da inteligência artificial. Essa situação demanda um delicado equilíbrio entre inovação e risco, bem como a implementação de controles efetivos para gerenciar cenários imprevisíveis. É necessário fazer escolhas complexas envolvendo privacidade e segurança, a aplicação justa da lei e os direitos das vítimas, bem como a resolução de conflitos e a prevenção de discriminação.

3.1 Racismo advindos do reconhecimento facial.

O racismo é uma forma de discriminação e preconceito baseada na raça ou etnia de uma pessoa. Envolve a crença de que algumas raças são superiores a outras e, portanto, justifica a desigualdade de tratamento com base nessas características raciais. O racismo pode se manifestar de várias maneiras, desde atitudes e crenças individuais até estruturas e sistemas sociais que perpetuam a desigualdade racial.

O racismo pode ser explícito ou implícito. O racismo explícito é quando as pessoas expressam abertamente sentimentos de superioridade racial e promovem a discriminação com base na raça. Isso pode ocorrer por meio de insultos raciais, agressões físicas, segregação racial e outras formas de discriminação direta.

O racismo implícito é mais sutil e muitas vezes inconsciente. Refere-se a preconceitos e estereótipos arraigados que podem afetar as atitudes e comportamentos das pessoas, mesmo sem que elas estejam cientes disso. O racismo implícito pode se manifestar em formas de discriminação velada, como

a recusa de oportunidades de emprego com base na raça ou tratamento diferenciado em interações cotidianas.

Almeida conceitua racismo como uma forma de discriminação em razão de condições sejam elas culturais ou até mesmo no que se refere ao tom de pele de alguém, assim ele diz:

> "... é sistemática de discriminação que tem a raça como fundamento, e que se manifesta por meio de práticas conscientes ou inconscientes que culminam em desvantagens ou privilégios para indivíduos, a depender do grupo racial ao qual pertençam" (ALMEIDA, 2018,p. 25).

Ao fazermos um paralelo do que vem constantemente ocorrendo, é perceptível a forma discriminatória em que o reconhecimento facial exerce seu papel, o que era pra ser uma ferramenta com fins de proteger a sociedade, acaba que por copiosas vezes tomando proporções contrarias daquelas a fora determinada.

O chefe de polícia de Detroit, nos Estados Unidos, James Craig relatou no ano de 2020, que o reconhecimento facial não funciona em 96% das vezes, alegava-se ainda que além da morosidade do tempo para identificação de um indivíduo, apresentava resultados imprecisos de modo que confundia a equipe policial.

Essas ponderações ocorreram poucos dias após a ACLU (American Civil Liberties Union), uma organização não governamental dos Estados Unidos dedicada à defesa e preservação dos direitos dos cidadãos, apresentar uma queixa formal ao Conselho de Comissários de Polícia de Detroit, pedindo uma desculpa pública pela prisão de Robert Williams, um indivíduo negro detido em janeiro de 2020, após o mesmo ser erroneamente identificado pelo sistema de reconhecimento facial da polícia.

De acordo com a reclamação, o sistema de reconhecimento facial do Departamento de Polícia de Detroit identificou de modo equivocado Robert Williams como o autor por um roubo de relógios ocorrido um ano e meio antes. Williams foi preso em seu próprio quintal, na presença de sua esposa e filhos, e passou a noite detido em uma prisão local. No dia seguinte, ele foi interrogado,

momento em que o caso contra ele começou a desmoronar. A reclamação afirma que o investigador inicialmente parecia confuso e disse a Williams que o computador o identificara como o culpado, mas depois admitiu que "o computador deve ter se enganado". No entanto, as acusações contra Williams não foram retiradas de imediato.

Williams pautou que suas filhas não compreendiam aquela situação e, ao chegar em casa, elas estavam brincando de ser policiais e acusaram o pai de roubar coisas. A reclamação destaca que Williams teve que explicar o incidente ao seu empregador e à sua família, além de ter sofrido o estigma de ser preso em seu próprio quintal, na frente de sua família e onde os vizinhos também puderam testemunhar o ocorrido.

Tal caso narrado, podemos observar o quão atroz pode ser um reconhecimento facial impreciso, isso causou danos além de morais e poderia ter proporcionado danos materiais ao acusado inocentemente, de modo que ele poderia perder seu emprego por ter sido preso, além disso danos psíquicos a sua família, presenciando o seu esposo, e pai sendo levado de forma errônea. Robert Williams acrescenta:

> “Estudos federais mostraram que os sistemas de reconhecimento facial identificam erroneamente pessoas asiáticas e negras até 100 vezes mais do que pessoas brancas. Por que a aplicação da lei tem permissão para usar essa tecnologia quando obviamente não funciona? Fico com raiva quando ouço empresas, políticos e policiais falarem sobre como essa tecnologia não é perigosa ou defeituosa. O pior é que, antes de isso acontecer comigo, eu realmente acreditava neles. Eu pensei, o que há de tão terrível se eles não estão invadindo nossa privacidade e tudo o que estão fazendo é usar essa tecnologia para se aproximar de um grupo de suspeitos?”(ROBERT WILLIAMS, 2021).

É manifestamente evidente que essas deficiências do sistema de reconhecimento facial quando aplicado a indivíduos negros e asiáticos decorrem

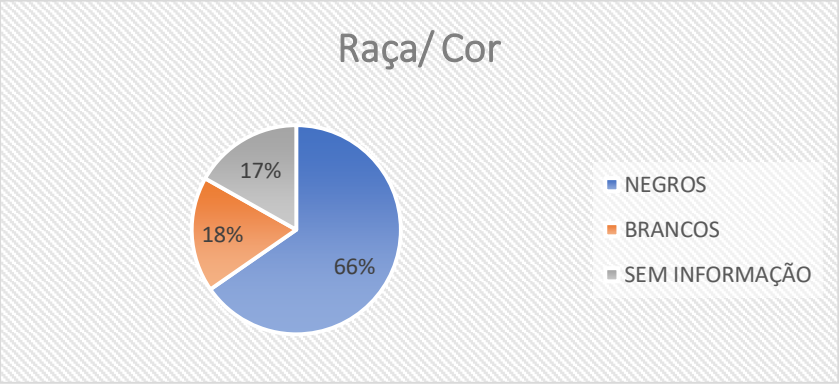
de suas características faciais similares, o que amplifica ainda mais a imprecisão dos resultados. Isso gera insegurança jurídica para aqueles encarregados da execução desse sistema e instila um sentimento de temor naqueles que são vítimas de uma inteligência artificial que erroneamente os penaliza.

De maneira análoga, no contexto brasileiro, é frequente relatos de indivíduos negros que têm enfrentado repetidamente essa mesma humilhação, sendo detidos de forma injusta, expostos ao escárnio perante vizinhos e familiares, e até mesmo obrigados a documentar diariamente sua localização por meio de fotografias, a fim de evitar futuras prisões arbitrárias.

Conforme apontado pelo portal G1, a parcela de indivíduos erroneamente encarcerados por meio do processo de reconhecimento fotográfico no Brasil compreende expressivos 83% de pessoas de ascendência negra. É uma lamentável constatação que essa realidade abarque, de maneira global, uma ampla escala de incidências.

Ao observarmos os dados constatados pelo relatório do ano de 2022, pelo CNJ, coordenado pelo ministro Rogério Schietti, é escancaradamente notória, a discriminação do reconhecimento facial para com os negros e pardos.

Gráfico 1 – Percentual de acusados por raça/cor e por sexo.



Fonte: Elaborado pelo GT com base no Levantamento de casos da imprensa (atividade I).

No que concerne ao gráfico apresentado, torna-se evidente a sobejante proporção de indivíduos afrodescendentes detectados pela tecnologia, o que reforça sobremaneira a concepção de que a mencionada ferramenta é exacerbadamente preconceituosa e propensa a equívocos.

O mencionado relatório também contempla uma explanação detalhada de processos por amostragem acerca de condenações ou prisões injustas, nas quais houve irregularidades no processo de identificação por parte do superior tribunal de justiça (STJ).

A amostra em questão abrangeu 28 processos, consistindo em uma análise qualitativa de casos julgados pelo STJ, nos quais ocorreram erros de reconhecimento. Nessa amostra, apenas em um dos processos analisados, a pessoa acusada era do gênero feminino. Em todos os demais processos, os acusados eram do gênero masculino, com 11 réus sendo classificados como negros (pretos e pardos), 9 como brancos e em 8 processos não foi obtida informação sobre raça/cor. Mais uma vez, torna-se manifesto o desafio em obter informações raciais dos envolvidos nos processos judiciais.

É sabido que a cor da pele assume um papel crucial nos processos de reconhecimento, uma vez que os erros cometidos evidenciam a reprodução do racismo estrutural, contido em nosso país considerando que a identificação por parte da vítima se torna suscetível à influência do estigma historicamente construído em relação à população negra.

Não obstante, é importante notabilizar que os "álbuns de suspeitos", que se trata de um conjunto de imagens que são utilizadas para identificação de indivíduos, frequentemente lidados em procedimentos de reconhecimento extrajudiciais consistem predominantemente de fotografias de indivíduos que possuem antecedentes criminais, o que se inclina a resultar na super-representação de pessoas negras nessas coleções, devido à seletividade racial existente no sistema de justiça criminal. Isso aumenta as chances de um reconhecimento positivo, embora não necessariamente preciso.

Outro item de visibilidade está relacionado ao titulado "efeito de reconhecimento inter-racial", vastamente documentado e debatido na literatura científica da Psicologia do Testemunho. Esse fenômeno refere-se ao fato de que, de modo geral, as pessoas enfrentam maior dificuldade em codificar características físicas de indivíduos pertencentes a grupos raciais distintos devido à sua menor familiaridade com tais grupos. Assim, há uma maior probabilidade de que uma pessoa branca reconheça erroneamente uma pessoa

negra ou indígena, por exemplo, em comparação com o reconhecimento de outra pessoa branca. Tendo em vista que as pessoas negras já são historicamente afetadas de maneira desproporcional pelas políticas de criminalização, as consequências negativas desse fenômeno recaem sobre elas com maior intensidade.

A combinação de todos esses fatores é evidenciada por meio de diversas pesquisas nacionais e internacionais que têm sido realizadas sobre o reconhecimento de pessoas, ressaltando o desafio de integrar a variável racial, de forma central, nas análises sobre o tema, bem como nas propostas direcionadas à redução da ocorrência de reconhecimentos errôneos e ao aumento do nível de credibilidade do sistema de justiça criminal.

Em 2016, estudiosos da Shanghai Jiao Tong University postularam que seu algoritmo era capaz de antecipar a criminalidade por meio da análise facial. No entanto, especialistas em engenharia de Stanford e do Google rebateram as alegações apresentadas no referido artigo, rotulando tal abordagem como uma nova forma de "fisionomia", uma pseudociência racial desacreditada que se popularizou entre os eugenistas, os quais inferem características de personalidade com base na conformação craniana de um indivíduo.

Ademais, o uso não regulamentado de sistemas de reconhecimento facial pode trazer riscos adicionais, incluindo formas mais sofisticadas de vigilância. Como a leitura labial automatizada, oferecendo a capacidade de observar e interpretar a fala à distância.

O reconhecimento facial pode estar subordinado a questões de viés e reconhecimento, incluindo o racismo. Isso ocorre devido a vários fatores, como a qualidade dos conjuntos de dados utilizados no treinamento dos algoritmos, as técnicas de reconhecimento facial de empregados, bem como as características específicas das faces das pessoas.

Ora, se os dados utilizados para treinar um sistema de reconhecimento facial não representarem a diversidade racial da população, isso pode levar a resultados imprecisos e discriminatórios. Ademais, as técnicas de reconhecimento facial podem ser mais propensas a falhas na identificação de

pessoas com tons de pele mais escuros, criadas em taxas de erro mais altas para esses grupos.

Esses imbróglios têm significado, pois podem levar a consequências negativas para as pessoas apoiadas. Por exemplo, indivíduos de determinadas raças podem ser falsamente identificados como suspeitos criminosos, levados a pensar injustas, detenções irreconhecíveis ou tratamento discriminatório.

É primordial conceituarmos racismo, em simplórias palavras podemos denominar o termo racismo como o modo de segregação, discriminação a outrem por sua raça.

Para combater o racismo no reconhecimento facial, é necessário abordar essas questões sistêmicas, isso inclui a diversidade e representatividade dos dados, é crucial garantir que os conjuntos de dados usados no treinamento dos algoritmos sejam representativos da diversidade racial da população. Isso envolve a coleta de dados de diferentes grupos raciais e étnicos, bem como a inclusão de pessoas com uma variedade de características reconhecidas.

Kade Crockford, diretor do Programa Technology for Liberty da ACLU de Massachusetts, bem menciona a respeito da tendenciosidade da tecnologia em incriminar pessoas negras, e o uso de fotos de um banco de dados manuseadas a fins de comparação com os indivíduos considerados suspeitos. Assim menciona:

> “Há um problema com os algoritmos e os dados de treinamento serem tendenciosos, mas esse não é o único problema com o viés nessa tecnologia. O outro problema é que a polícia está usando arquivos de fotos policiais como banco de dados de comparação, e as próprias fotos são tendenciosas devido ao grau em que o policiamento foi executado de maneira desproporcional ao longo da história e até o presente.” (KADE CROCKFORD, 2019)

Observamos um padrão alarmante de prisões desproporcionais de indivíduos negros e pardos em praticamente todas as categorias de delitos menores, incluindo casos como dirigir com a carteira suspensa ou vencida, posse de drogas, furtos, invasão de propriedade e conduta desordeira, práticas

que podem exercidas por qualquer pessoa independente de raça ou cor, mas que infelizmente são deduzidas a pessoas negras.

O viés nas detenções relacionadas à maconha é particularmente surpreendente, uma vez que a maioria das pessoas presas por delitos ligados ao uso dessa substância são negras ou pardas. Isso não ocorre porque os brancos não consomem maconha, mas sim porque raramente são presos por esse tipo de crime. Essa discrepância revela um viés evidente, e ao utilizar esses conjuntos de dados e fingir que se trata de uma tecnologia neutra, essa tendência é codificada e perpetuada.

O racismo tem efeitos prejudiciais nas vítimas, pois promove a marginalização, o estigma e a exclusão social. Também contribui para a perpetuação de desigualdades socioeconômicas e oportunidades limitadas para grupos raciais minoritários.

Combater o racismo requer esforços tanto individuais quanto coletivos. Isso inclui a conscientização sobre os preconceitos raciais e a promoção da igualdade racial, bem como a implementação de políticas e leis antidiscriminação. A educação, o diálogo intercultural e a valorização da diversidade são componentes fundamentais na luta contra o racismo e na construção de uma sociedade mais justa e inclusiva.

3.2 Psicologia Testemunhal: Aplicações na Identificação Pessoal e nos Depoimentos Forenses

O reconhecimento facial desempenha um papel significativo na psicologia forense, especialmente quando se trata da identificação de suspeitos em casos criminais. A psicologia fornece insights valiosos sobre os processos cognitivos e perceptuais envolvidos no reconhecimento facial, bem como os possíveis vieses e limitações associados a essa prática.

Estudos demonstram que a memória humana para rostos pode ser suscetível a erros e distorções, especialmente em situações de estresse ou eventos traumáticos. A psicologia forense investiga fatores que podem influenciar a precisão do reconhecimento facial, como o tempo de exposição ao

rosto, o grau de atenção do observador, a presença de pistas sugestivas e o uso de técnicas adequadas de entrevista.

Em termos psicológicos, a experiência de um assalto repleto de adrenalina, na qual a vítima é exposta, representa um fator que frequentemente dificulta a precisão do reconhecimento facial, impedindo uma identificação assertiva do indivíduo como sendo o perpetrador do crime. Isso se deve ao fato de que, inconscientemente, a vítima pode direcionar sua acusação para alguém que possua características físicas semelhantes, incorrendo inadvertidamente em um equívoco de identificação.

Nesse sentido, a psicóloga Dra. Lilian Stein conduziu uma análise abrangente sobre os progressos científicos na área da psicologia do testemunho, com ênfase nas aplicações voltadas ao reconhecimento pessoal. descrito no relatório nº 59 do projeto "Pensando o Direito", uma iniciativa promovida pela Secretaria de Assuntos Legislativos (SAL) do Ministério da Justiça e pelo Ipea, esses foi o resultado da pesquisa:

> “O grau de confiança que a pessoas tem sobre a precisão de sua memória nem sempre é um indicador confiável de sua fidedignidade. Mesmo vítimas ou testemunhas de crimes que, parecem confiar plenamente em suas lembranças sobre os fatos e pessoas envolvidas nestes crimes, não estão isentas de uma avaliação equivocada sobre a exatidão daquilo que testemunharam. Há mais de três décadas, os cientistas têm recomendado que “[...] o Judiciário não deve se valer da confiança da testemunha como um índice de precisão” (DEFFEMBACHER, 1980, p. 243).

Além disso, a psicologia forense também examina questões relacionadas à confiabilidade dos depoimentos de testemunhas oculares, considerando fatores como a influência de informações externas, a contaminação da memória e a sugestionabilidade.

Com base nesses conhecimentos, os profissionais da psicologia forense desempenham um papel importante na avaliação crítica de evidências de reconhecimento facial em casos de identificação de crime, ajudando a garantir uma abordagem rigorosa e cientificamente embasada na análise dessas evidências.

Com o intuito de aprofundar a discussão, o Instituto de Pesquisa Econômica Aplicada (IPEA) conduziu um estudo abrangente sobre as questões relacionadas ao reconhecimento pessoal. Um dos aspectos abordados neste estudo foi a constatação de que os desafios relativos à identificação precisam do suspeito surgem mesmo antes do início das investigações conduzidas pela polícia civil.

Essa problemática se manifesta quando os policiais militares precisam identificar rapidamente o autor do crime ou quando se baseiam exclusivamente no testemunho da própria vítima para buscar um suspeito.

> "Em função da própria natureza da atividade do policial militar, inexiste qualquer suporte/estrutura para a realização desses reconhecimentos, em regra realizados através da técnica do "show up" ... A possibilidade de "show-up", tanto para fotos quanto pessoas, é bastante presente, em todas as fases de apuração do fato criminoso. Este procedimento é citado na literatura científica como o mais sujeito a erros de identificação." (IPEA, 2015)

É inegável, que as normas que regem o testemunho partem do pressuposto de que os sentidos individuais capturam de maneira objetiva os eventos e que a memória os registra como imagens em um filme ou sons gravados. No entanto, é importante considerar que os canais sensoriais operam de forma seletiva devido à capacidade limitada do sistema perceptivo.

Diante de estímulos simultâneos, o sistema tende a focar naqueles aos quais está mais habituado (como observações diferentes entre guardas de trânsito e pedestres no mesmo contexto). Além disso, a percepção também é influenciada pelo estado emocional da pessoa, o que pode afetar a forma como os eventos são percebidos e lembrados.

Uma outra questão de suma importância a ser considerada em estudos posteriores diz respeito à necessidade de coleta de dados quantitativos sobre o número de indivíduos erroneamente condenados devido à utilização de provas dependentes da memória. Ao contrário dos Estados Unidos da América, onde o Projeto Innocence constatou uma taxa de 75% de erros judiciais diretamente

relacionados, por exemplo, a identificações equivocadas de pessoas, em nosso país não dispomos de informações nesse sentido que poderiam ser objetivamente relevantes para impulsionar reformas no âmbito da legislação processual penal.

Mesmo que o reconhecimento facial desempenhe um papel crucial na psicologia forense, especialmente na identificação de suspeitos em casos criminais. A psicologia oferece insights valiosos sobre os processos cognitivos e perceptuais subjacentes ao reconhecimento facial, bem como os possíveis vieses e limitações associados a essa prática.

A memória humana para rostos é suscetível a erros e distorções, especialmente em situações de estresse ou eventos traumáticos. A psicologia forense examina fatores que afetam a precisão do reconhecimento facial, como tempo de exposição, atenção do observador e técnicas de entrevista adequadas.

A influência do estado emocional da pessoa, como em situações de assalto com adrenalina, pode dificultar a identificação precisa, levando a equívocos de identificação. Os profissionais da psicologia forense desempenham um papel crucial na avaliação crítica de evidências de reconhecimento facial, garantindo uma análise rigorosa e embasada cientificamente. Estudos adicionais podem se concentrar na coleta de dados quantitativos sobre condenações errôneas devido a evidências dependentes da memória, a fim de impulsionar reformas na legislação processual penal.

Em última análise, compreender as nuances da percepção e memória humanas é vital para garantir abordagens justas e precisas na investigação e identificação de crimes.

4 Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), Lei nº 13.709/2018, consiste no arcabouço normativo brasileiro pelo qual se estabelece as diretrizes para o tratamento de informações pessoais e nelas se impõe modificações nos artigos 7º e 16 do Marco Civil da Internet.

Com a implementação da lei geral de proteção de dados, o Brasil ingressa no grupo de nações que possuem uma legislação específica para salvaguardar os dados pessoais e a privacidade de seus cidadãos. Outros marcos regulatórios semelhantes incluem o Regulamento Geral em relação a Proteção de Dados (GDPR) na União Europeia, que se tornou obrigatório em 25 de maio de 2018 e abrange todos os países membros da UE, e o California Consumer Privacy Act of 2018 (CCPA) nos Estados Unidos da América, que foi implementado por meio de uma iniciativa estadual na Califórnia e aprovado em 28 de junho de 2018 (AB 375).

A lei fundamenta-se em uma variedade de princípios, tais como o zelo pela privacidade, o direito de autodeterminação na esfera da informação, a liberdade de expressão, a circulação de informações e a manifestação de opiniões, a inviolabilidade da vida privada, da reputação e da imagem, o estímulo ao desenvolvimento econômico e tecnológico, a promoção da inovação, a preservação da livre iniciativa, da concorrência justa e da proteção dos direitos do consumidor, bem como a salvaguarda dos direitos humanos, da liberdade e da dignidade das pessoas. Conforme disposto em seu texto normativo:

> “Art. 5º Para os fins desta Lei, considera-se: [...] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (BRASIL, 2018)

Além desses princípios supracitados traz consigo um conjunto de conceitos jurídicos inovadores, como "informações pessoais" e "informações pessoais sensíveis". Ela estabelece os critérios para um tratamento adequado dessas

informações, define um conjunto de direitos para os indivíduos titulares desses dados, impõe obrigações específicas aos responsáveis pelo controle dessas informações e estabelece uma série de procedimentos e normas para garantir um tratamento apropriado e um compartilhamento responsável das informações pessoais com terceiros.

É de suma importância frisar que no texto da lei em seu artigo 5º inciso XII, dispõe explicitamente que deverá haver expressão voluntária, informada e inequívoca pela qual o titular concorda com o processamento de seus dados pessoais para um propósito específico, ou seja, há a necessidade do titular do direito, consentir ou não, sobre o uso de seus dados ou imagem.

A lei é aplicável a qualquer informação que se relacione a uma pessoa identificada ou que possa ser identificada, incluindo dados sobre a origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou organizações de natureza religiosa, filosófica ou política, informações relacionadas à saúde ou vida sexual, dados genéticos ou biométricos, desde que esses dados estejam vinculados a uma pessoa específica.

No contexto do reconhecimento facial, a LGPD também se aplica. O reconhecimento facial envolve o processamento de dados biométricos sensíveis, pois trata da identificação única e individual de uma pessoa com base em características faciais únicas.

De acordo com a LGPD, o tratamento de dados pessoais sensíveis, como os dados biométricos obtidos pelo reconhecimento facial, requer um cuidado especial e uma base legal específica. O consentimento do titular dos dados é uma das bases legais possíveis para o tratamento dessas informações, além de outras bases previstas na lei, como o cumprimento de obrigação legal ou regulatória, a execução de contrato, a proteção da vida ou da integridade física, entre outras.

Além disso, a LGPD impõe obrigações aos responsáveis pelo tratamento dos dados, como a adoção de medidas de segurança adequadas, o fornecimento de informações claras e transparentes aos titulares dos dados, a garantia do direito de acesso e correção dos dados, e a limitação do compartilhamento dessas informações apenas para as finalidades previamente estabelecidas.

Portanto, a LGPD desempenha um papel fundamental na regulamentação do uso do reconhecimento facial, visando proteger a privacidade e os direitos dos indivíduos em relação ao tratamento de seus dados biométricos sensíveis.

Nesse contexto, o processamento de qualquer informação pessoal em geral, incluindo dados biométricos em particular, deve ser entendido como uma sequência de procedimentos que devem estar em conformidade com a legislação brasileira, especialmente a LGPD, bem como com outras leis dispersas relacionadas à proteção de dados pessoais (MONTEIRO, 2017, p. 2-4; TEOFILO et al., 2019, p. 8), e também com regulamentos futuros que possam ser promulgados.

Nesta perspectiva, emerge uma preocupação pertinente acerca da privacidade individual, dado que as pessoas se encontram potencialmente sujeitas à vigilância constante, o que resulta na violação de suas esferas de privacidade. Lamentavelmente, esses indivíduos frequentemente desconhecem a quem recorrer para salvaguardar seus direitos infringidos.

Uma das principais críticas dirigidas ao reconhecimento facial reside na notória falta de segurança, pois tal tecnologia pode levar à prisão indevida de um indivíduo por um crime que não cometeu. Ademais, também se evidencia a preocupante possibilidade de vazamento de dados, o que pode desencadear potenciais casos de fraude, envolvendo informações que a pessoa sequer consentiu em serem utilizadas.

O deputado Guiga Peixoto, autor do projeto de lei 2392/22 que visa regular a questão do reconhecimento facial, discorre sobre as principais problemáticas relacionadas a essa tecnologia, como se segue:

> “A consequência do mau uso desses dados pode ser extremamente nociva para os cidadãos. Imagine-se a hipótese de uma pessoa ser presa por erros na identificação ou então o constrangimento de ter negado o acesso a determinado estabelecimento do qual é sócio. Outra possibilidade é o mau uso desses dados em razão de vazamentos ou mesmo do uso comercial dessas informações, alimentando a prática de fraudes, estelionatos, roubo de identidades ou falsidades ideológicas das mais variadas.” (Guiga Peixoto, 2022.)

Nesse parâmetro, entendemos que um dos princípios abordados na lei de proteção de dados, é exatamente a segurança e a privacidade dos dados das pessoas, ou seja, os indivíduos que são filmados, que permitem ser identificados através do reconhecimento facial, precisam sempre ser informados, para que seus dados serão utilizados e assegurar ainda que tais dados não sejam utilizados para outros fins.

Essa apreensão decorre da possibilidade de que as informações dos indivíduos sob monitoramento possam ser indevidamente apropriadas e empregadas por agentes inescrupulosos em atividades criminosas, tais como obtenção fraudulenta de empréstimos, acesso indevido a contas bancárias, entre outras.

Em determinadas circunstâncias, tais como as relacionadas à segurança pública, a empresa ou o governo possuem a responsabilidade de notificar sobre a coleta de dados por meio de placas, por exemplo, porém não necessitam, obrigatoriamente, solicitar a autorização individual de cada usuário. Assegurar a prevenção de fraudes, a proteção do titular dos dados, e procedimentos de identificação e autenticação são outros cenários que contemplam a exceção.

Diante das situações expostas, é evidente a urgência de uma legislação específica para garantir maior segurança dos dados coletados, bem como proteção à privacidade que, lamentavelmente, está comprometida. Além de assegurar a precisão dos resultados, é crucial evitar que as informações pessoais sejam indevidamente vazadas e utilizadas para fins não autorizados.

4.1 Proposta legislativa 2392/2022: regulamentação do emprego de tecnologias de reconhecimento facial.

Com o propósito de estabelecer regras para salvaguardar e regular o emprego do reconhecimento facial, o Deputado Guiga Peixoto (PSC/SP) concebeu um projeto de lei que trata sobre a utilização de tecnologias de reconhecimento facial tanto no âmbito público quanto no privado. Esse projeto tem como objetivo fixar diretrizes que visam garantir uma maior proteção dos

dados fornecidos por meio dessa tecnologia, bem como prevenir o uso desses dados para propósitos ilícitos.

Uma das principais críticas dirigidas ao reconhecimento facial reside no fato de ocorrer o uso inadequado de informações, bem como o compartilhamento desses dados por parte de empresas, muitas vezes sem a devida autorização do fornecedor, o que flagrantemente contraria as disposições contidas na Lei nº 13.709/2018. Essa legislação estabelece que é imprescindível obter o completo consentimento do indivíduo em relação à utilização de seus dados.

Nessa perspectiva, o projeto de lei estipula em seu artigo 2º que:

> "Art. 2º O tratamento de dados biométricos oriundos de tecnologias de reconhecimento facial deverá atender ao disposto na Lei Geral de Proteção de Dados (LGPD), Lei nº13.709, de 14 de agosto de 2018, e não poderão ser repassados a terceiros, salvo ao poder público para casos exclusivos de segurança pública, defesa nacional e atividades de investigação e repressão de infrações penais. Parágrafo único. É considerado nulo termo de consentimento para o tratamento dos dados de que trata esta Lei que admita o repasse desses dados a terceiros." (PL Nº 2392, 2022).

É perceptível que o emprego do reconhecimento facial tem experimentado um crescimento veloz tanto no âmbito público quanto no privado. Órgãos responsáveis pela segurança pública têm utilizado esse artefato para identificar indivíduos procurados em locais de aglomeração significativa. No setor privado, empresas o empregam para autenticar permissões de acesso ou para a conveniência dos usuários ao usufruírem de serviços. Setores como companhias aéreas, empresas de telefonia e redes de supermercados têm ampliado sua oferta de novos serviços, resultando em maior comodidade para seus usuários e redução de custos para as empresas e órgãos públicos.

Contudo, é importante ressaltar que o uso indiscriminado dessas tecnologias pode acarretar abusos sob a ótica dos consumidores e, ainda mais grave, sob a perspectiva dos cidadãos. Por exemplo, quando serviços de reconhecimento facial são disponibilizados sem a presença de funcionários para lidar com possíveis equívocos na identificação. Ademais, há a preocupante possibilidade de que tais dados sejam indevidamente utilizados devido à

comercialização desregrada ou ao vazamento das informações, o que poderia resultar em práticas como fraudes, estelionatos, roubo de identidades ou diversas formas de falsidade ideológica.

O uso inadequado do reconhecimento facial resulta em desafios adicionais, tais como a possibilidade de prisões injustas ou, ainda mais constrangedor, ser levado à delegacia por um crime que não foi cometido, o que, lamentavelmente, não é tão incomum como poderia parecer. Conforme uma pesquisa realizada pelo MIT Media Lab, alguns dos softwares comerciais alcançam até 99% de precisão na identificação de homens brancos, enquanto a taxa de erro na identificação de mulheres negras pode chegar a alarmantes 35%, uma proporção claramente inaceitável.

Esses dados revelam uma alarmante falta de segurança e, em vez de fornecer um serviço que garanta proteção à sociedade, o uso desse reconhecimento facial produz exatamente o oposto, gerando um clima de temor entre indivíduos afrodescendentes, que vivenciam o receio constante de serem abordados com base em resultados e erros provenientes dessa tecnologia.

No ano de 2018, foi iniciado um inquérito civil público pelo Ministério Público do Distrito Federal e Territórios (MPDFT), com o objetivo de analisar as medidas de utilização do reconhecimento facial. Nesse inquérito, foi constatado que dados provenientes de pessoas que declararam o imposto de renda e utilizaram a autenticação facial comumente empregada para desbloquear telas estavam sendo empregados para confirmar se o rosto exibido na identificação pertencia ou não ao indivíduo em questão.

> “O Banco de dados utilizado pela Certibio tem 70 milhões de cadastros. Isso porque ela usa as informações armazenadas pelo Serviço de Processamento de Dados (SERPRO), empresa pública responsável por alguns serviços de tecnologia da administração federal. Entre eles está o processamento da declaração do Imposto de Renda e a autenticação facial – basicamente, ela confirma se um rosto pertence a uma pessoa ou não. A base do SERPRO possui 70 milhões de registros biométricos e biográficos únicos, fornecidos pelo Departamento Nacional de Trânsito (DENATRAN) partir das informações das carteiras de motoristas.” (SERPRO, 2018).

Isso implica que as pessoas que forneceram esses dados consentiram que eles fossem utilizados apenas para confirmar sua identidade como titulares das carteiras de habilitação ou como declarantes de imposto de renda. O SERPRO possui uma base de dados contendo 70 milhões de registros biométricos e biográficos exclusivos, fornecidos pelo Departamento Nacional de Trânsito (DENATRAN) com base nas informações presentes nas carteiras de motoristas. Esses dados são empregados pela Certibio para realizar suas atividades relacionadas ao reconhecimento facial e à verificação de identidade.

Embora manifestemos uma notável apreensão quanto à salvaguarda da privacidade e dos direitos humanos fundamentais no contexto do uso indiscriminado e imprudente dessas tecnologias, é válido ressaltar que o Brasil dispõe atualmente de uma legislação moderna que aborda essa demanda a LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709, de 2018).

Na referida norma, fica determinado que a obtenção e o tratamento de informações biométricas (abrangendo também as derivadas de tecnologias de reconhecimento facial) De acordo com a legislação, a coleta e processamento de dados biométricos, incluindo aqueles provenientes de tecnologias de reconhecimento facial, são devidamente regulamentados e exigem a obtenção de consentimento que seja "livre, informado e inequívoco". Esse consentimento deve ser solicitado de maneira destacada de outros consentimentos e os dados biométricos só podem ser utilizados para finalidades específicas.

Apesar dessa proteção estabelecida, não há impedimento para que as instituições que utilizam esses dados incluam, em suas solicitações de consentimento, a possibilidade de comercialização dos dados biométricos. Tendo em vista que o usuário ou cidadão é a parte vulnerável nessa relação, é muito provável que ele se sinta pressionado a aceitar essas condições para ter acesso a determinados serviços exclusivos ou facilidades oferecidas.

Assim sendo, as pessoas aceitam inadvertidamente essa utilização de dados por desconhecerem, no que concerne aos seus direitos à privacidade e à utilização de suas informações, ao confiar que a empresa na qual estão utilizando o serviço não as empregará para outros propósitos.

Ademais, devido à necessidade dos serviços, elas aceitam automaticamente sem sequer ler o contrato, por exemplo. Essas práticas comuns no cotidiano da sociedade impedem que as pessoas tenham maior cautela com seus dados, resultando em uma vulnerabilidade de sua privacidade.

Assim sendo, diante dos obstáculos que o avanço tecnológico enfrenta e da flagrante insegurança que se apresenta, é imprescindível a criação de uma legislação específica para responsabilizar aqueles que fazem uso dos dados alheios sem a devida autorização. Além disso, é necessário exercer uma cautela aprimorada em relação ao emprego do reconhecimento facial, a fim de reduzir substancialmente os alarmantes registros de resultados equivocados e, assim, evitar que inocentes sejam injustamente punidos por um erro que pode afetar suas vidas de forma permanente.

4.2 Decisões atuais acerca do reconhecimento facial.

Considerando a explanação do pensamento acadêmico e da normativa legal relativa ao procedimento de identificação facial, procederemos à análise de algumas orientações jurisprudenciais pertinentes a esta matéria em tela, destacando os alicerces argumentativos subjacentes bem como as ramificações resultantes oriundas do emprego deste instrumento tecnológico.

Em uma das circunstâncias examinadas, em meio a um incidente de assalto, sujeitos portando indumentárias denominadas "toucas ninja", que deixam somente os olhos expostos, empreendem uma tentativa de subtrair a carga de um caminhão. Um dos operadores do veículo, após minuciosamente revisar as imagens relativas a outro episódio de subtração, alega não nutrir quaisquer hesitações acerca da identificação de um dos infratores: com base nas características dos olhos visíveis e na escolha de trajar vestimentas sociais, alega ser a mesma pessoa em ambos os cenários delituosos.

A certeza se intensifica quando ele é exposto a uma gravação contendo a voz do indivíduo suspeito. Em tribunal, ele reforça sua convicção ao afirmar que, ao examinar as fotografias apresentadas pelas autoridades policiais, identificou uma tatuagem que o assaltante supostamente ostentaria em seu antebraço - apesar de tal detalhe não ter sido mencionado no decorrer do

inquérito e do fato de que o sujeito retratado nas imagens do outro roubo estava com seus membros superiores cobertos. O suspeito, assim identificado, é condenado a uma pena superior a cinco anos pelo delito de tentativa de subtração.

> (STJ - HC: 680416 ES 2021/0220565-0, Relator: Ministro REYNALDO SOARES DA FONSECA, Data de Publicação: DJ 16/09/2021)

No veredicto do HC 680.416, proferido em setembro de 2021, o ministro Reynaldo Soares da Fonseca caracterizou o processo de identificação como "susceptível de questionamento" e, em virtude da ausência de outras evidências capazes de sustentar a condenação, inocentou o réu, medida corroborada pelo próprio Ministério Público Federal.

A referida determinação constitui uma entre as quase noventa deliberações já emanadas pelo Superior Tribunal de Justiça desde o momento em que a Sexta Turma, mediante uma reestruturação da jurisprudência prevalecente, estabeleceu a concepção de que o desrespeito ao preceito delineado no Artigo 226 do Código de Processo Penal invalida a identificação prévia do acusado perpetrada pelas autoridades policiais, sendo tal circunstância incapaz de fundamentar a condenação do indivíduo, ainda que corroborada em etapa posterior do procedimento judiciário.

Em um outro cenário amplamente destacado nos meios de comunicação, o empreendedor comparece ao estabelecimento no início do dia e constata a ocorrência de um ato de subtração. Por meio da análise meticulosa das imagens registradas pelas câmeras de vigilância, constata-se que o perpetrador do delito envergava uma camiseta do clube esportivo Barcelona, ostentando o numeral 10 em suas costas. Notificadas, as forças policiais desencadeiam rondas investigativas e detêm um indivíduo trajando a mencionada indumentária associada à equipe espanhola, exibindo, ainda, o mesmo numeral que o jogador renomado Lionel Messi portava naquele mês de janeiro de 2021.

> (STJ - HC: 686317 SC 2021/0255611-2, Relator: Ministro JESUÍNO RISSATO (DESEMBARGADOR CONVOCADO DO TJDFT), Data de Publicação: DJ 13/08/2021)

No HC 686.317, o desembargador convocado Jesuíno Rissato acompanhou o parecer do Ministério Público Federal e declarou a absolvição do réu, destacando que a decisão condenatória "ou se baseou em reconhecimento de uma camiseta ou se fundou em reconhecimento indireto de imagens de vídeo (não periciadas e sobre fatos por ninguém presenciados)".

O equivocado reconhecimento de indivíduos suspeitos tem subsistido como uma das primordiais instigadoras de equívocos no âmbito judiciário, culminando na detenção injusta de inocentes. Esse panorama engendrou a instauração, nos Estados Unidos, no ano de 1992, da Iniciativa pela Inocência (Innocence Project), uma organização instituída por juristas peritos na solicitação de compensações estatais em razão da condenação indevida de indivíduos desprovidos de culpa.

A inquietação que se instaura reside na eventualidade de uma detenção injusta, na qual o indivíduo que sofreu o agravo pode, naturalmente, intentar uma demanda visando reparação por prejuízos morais e, em algumas circunstâncias, até mesmo por danos de natureza material. No entanto, o processo indenizatório em questão se estende por muitos anos até alcançar uma resolução, e mesmo quando se consuma a determinação, esta não atenua os danos infligidos à vítima, o que culmina na subsistência de um senso de incerteza jurídica e perpetuação de agravos psicológicos.

A Organização Não Governamental Iniciativa pela Inocência Brasil empreendeu uma investigação de cunho analítico, corroborando a ocorrência de proporções notavelmente elevadas no tocante às detenções equivocadas de indivíduos, as quais derivam do emprego do procedimento de identificação facial. Aproximadamente 75% das condenações injustas se originam de equívocos perpetrados por vítimas e testemunhas no momento da identificação dos suspeitos. Ademais, em 38% dos cenários nos quais se verificou tal engano, múltiplas testemunhas oculares erroneamente assinalaram o mesmo indivíduo inocente.

Um outro substancial entrave que deriva do emprego do reconhecimento facial é a utilização desse método para fins ilícitos, ocasionando uma série de pronunciamentos judiciais que visam reparar prejuízos de ordem moral,

decorrentes do uso inadequado em transações de empréstimos nas quais o titular não deu autorização expressa. Adicionalmente, desencadeia-se também prejuízos materiais, resultantes da circunstância em que as vítimas veem seus nomes inseridos de maneira indevida em registros negativos, justamente em virtude da formalização de empréstimos não consentidos.

Nesse contexto, foi proferida uma determinação relativa a um empréstimo realizado através do uso do reconhecimento facial, onde se reconheceu que a parte que apresentou a ação realmente detém o direito a receber compensação e reparação pelo prejuízo. Isso decorre do fato de que a contratação do empréstimo não havia sido autorizada pela parte autora.

> "Tribunal de Justiça do Estado da Bahia PODER JUDICIÁRIO TERCEIRA TURMA RECURSAL - PROJUDI PADRE CASIMIRO QUIROGA, LT. RIO DAS PEDRAS, QD 01, SALVADOR - BA ssa-turmasrecursais@tjba.jus.br - Tel.: 71 3372-7460 PROCESSO Nº 0001997-20.2021.8.05.0211. RECORRENTE: MARINEI VIRGEM CARNEIRO LIMA. RECORRIDA: BANCO PAN S A. RELATOR: Juiz Marcelo Silva Britto. EMENTA RECURSO INOMINADO. CONDIÇÕES DE ADMISSIBILIDADE PREENCHIDAS. CONTRATO DE EMPRÉSTIMO BANCÁRIO NÃO SOLICITADO PELA PARTE AUTORA. DISPONIBILIZAÇÃO DO VALOR EM CONTA BANCÁRIA DE TITULARIDADE DA CONSUMIDORA QUE COMUNICOU O FATO AO BANCO E DEPOSITOU O VALOR EM JUÍZO. CONTRATO DE EMPRÉSTIMO CONSIGNADO JUNTADO AOS AUTOS (EVENTO 21), COM ASSINATURA VIRTUAL. RECONHECIMENTO FACIAL QUE NÃO PREENCHE OS REQUISITOS DA INSTRUÇÃO NORMATIVA DO INSS 28/2008. FOTOGRAFIA QUE NÃO SE ENQUADRA NO CONCEITO DE AUTORRETRATO (SELFIE), PORTANTO, ILEGÍTIMA PARA COMPROVAR A VERACIDADE DA CONTRATAÇÃO, POR INVIABILIZAR A PROVA DE VIDA E SEMELHANÇA COM O DOCUMENTO DE IDENTIDADE. DOCUMENTO DE IDENTIDADE JUNTADO PELA RÉ QUE INDICA SE TRATAR DO MESMO APRESENTADO PELA AUTORA (EVENTO 01), ATRAVÉS DE SCANNER. HIPERVULNERABILIDADE DA CONSUMIDORA. ELEMENTOS SUFICIENTES QUE DENOTAM A IRREGULARIDADE DA CONTRATAÇÃO. SUPOSTA CONTRATAÇÃO REALIZADA ATRAVÉS DO ORIGINADOR (FONTES PROMOTORA EIR). CONTRATOS BANCÁRIOS QUE GARANTEM O RECEBIMENTO DE COMISSÃO PELOS

CORRESPONDENTES BANCÁRIOS. INDÍCIO DE FRAUDE. SENTENÇA QUE JULGOU IMPROCEDENTES OS PEDIDOS. REFORMA PARCIAL DA SENTENÇA PARA DECLARAR A INEXISTÊNCIA DE RELAÇÃO JURÍDICA FIRMADA ENTRE AS PARTES, A RESTITUIÇÃO EM DOBRO DO VALOR COMPROVADAMENTE DESCONTADO, A DEVOLUÇÃO DO VALOR DEPOSITADO E CONDENAR A RÉ AO PAGAMENTO DE INDENIZAÇÃO POR DANOS MORAIS NO VALOR DE R$ 5.000,00 (CINCO MIL REAIS), COM BASE NOS PRINCÍPIOS DA PROPORCIONALIDADE E RAZOABILIDADE. RECURSO CONHECIDO E PARCIALMENTE PROVIDO. ACÓRDÃO Vistos, relatados e discutidos os autos acima indicados. Realizado o julgamento, a Terceira Turma Recursal do Tribunal de Justiça do Estado da Bahia, decidiu, por unanimidade, CONHECER E DAR PROVIMENTO PARCIAL AO RECURSO, para reformar a sentença impugnada, nos termos do voto do relator, adiante lavrado, que passa a integrar este acórdão. Sala das Sessões, data certificada pelo sistema. Marcelo Silva Britto Juiz Presidente/Relator PROCESSO Nº 0001997-20.2021.8.05.0211. RECORRENTE: MARINEI VIRGEM CARNEIRO LIMA. RECORRIDA: BANCO PAN S A. RELATOR: Juiz Marcelo Silva Britto. VOTO Dispensado o relatório e com fundamentação concisa, nos termos do art. 46 da Lei nº. 9.099/95. Presentes os pressupostos extrínsecos e intrínsecos de sua admissibilidade, conheço dos recursos. No mérito, depois de minucioso exame dos autos, estou persuadido de que a irresignação manifestada pela autora recorrente merece parcial acolhimento. Constata-se dos autos a hipossuficiência da parte autora e a verossimilhança das suas alegações, devendo o caso ser analisado à luz da inversão do ônus da prova, conforme disposto no art. 6º, VIII, do Código de Defesa do Consumidor. Aduz a parte autora que foi surpreendida com um depósito em sua conta corrente no valor de R$13.758,12 (treze mil setecentos e cinquenta e oito reais e doze centavos), referente a uma contratação de empréstimo bancário consignado que não reconhece. Narra, ainda, que efetuou o depósito judicial do valor indevidamente creditado em sua conta bancária. Requer o cancelamento do contrato, a suspensão dos descontos e o pagamento de indenização por danos morais. A parte acionada, por outro lado, sustenta a legalidade da contratação, afirmando que a mesma ocorreu de modo virtual, juntando no evento 21 dos autos o contrato supostamente firmado entre as partes, com reconhecimento

facial, acompanhado do documento de identidade da Autora. Pugna pela improcedência total da ação. A ilustre magistrada a quo julgou improcedentes os pedidos. Com efeito, analisando detidamente os autos, verifica-se que os documentos apresentados pela parte acionada na fase instrutória (evento 21), não são aptos a comprovar que a parte autora efetivamente celebrou o contrato que ensejou os descontos impugnados na exordial, posto que, tratando-se de empréstimo via conta digital, com validação de assinatura eletrônica através de reconhecimento facial, caberia a parte ré se certificar dos cuidados inerentes ao tipo de contratação, conforme previsto na Instrução Normativa do INSS 28/2008. Nesse contexto, constata-se que o contrato colacionado pela Ré contém fotografia pessoal da Autora em ambiente, posicionamento e imagem absolutamente contrária aos critérios necessários para certificação da biometria facial, que utiliza o autorretrato (selfie) para comparação com imagens do banco de dados, fazendo uma prova de vida, levando em consideração o contexto da foto e o seu fundo. Assim, o contrato de empréstimo consignado que foi juntado aos autos no evento 21, com assinatura virtual, apresenta reconhecimento facial que não preenche os requisitos da instrução normativa do INSS 28/2008, pois não se enquadra no conceito de autorretrato (selfie), portanto, documento ilegítimo para comprovar a veracidade da contratação, por inviabilizar a prova de vida e semelhança com o documento de identidade. Ademais, por se tratar de alegação autoral que recai sobre fato negativo, no sentido de que não houve a contratação de empréstimo, desloca-se para o fornecedor de serviços bancários o ônus de comprovar a regularidade da cobrança, sobretudo pelo fato de que o contrato juntado informa que a contratação teria sido realizada através de correspondente bancário, o que gera repasse de comissão por cada contratação realizada. A plataforma eletrônica em que se deu a operação financeira contestada, diante da singularidade e complexidade do ambiente virtual (manifestação de vontade por meio de biometria facial), mormente para consumidores que têm uma vulnerabilidade informacional, leva a crer, em princípio, que não houve por parte da autora um consentimento informado. Ao contrário, todos esses fatos, na verdade, evidenciam que a parte autora foi vítima de uma fraude corriqueira nos dias atuais Nesse contexto, diante de alegação de ausência de vínculo jurídico com a Ré, cabia à instituição financeira comprovar a referida contratação, ônus que não se desincumbiu. Tal fato, por si só, é suficiente para justificar o pleito

indenizatório, posto que, em se tratando de indenização decorrente de má prestação do serviço, a prova do dano moral se satisfaz com a demonstração da sua existência, independentemente da prova objetiva do abalo na honra e na reputação, facilmente presumíveis. A jurisprudência mais atual tem reconhecido que todo dano moral causado por conduta ilícita é indenizável como direito subjetivo da própria pessoa ofendida. Também é assente que a moral, absorvida como dado ético pelo direito, que não pode se dissociar dessa postura, impõe sejam as ofensas causadas por alguém a outrem devidamente reparada pelo autor da ofensa. No caso, enquadra-se perfeitamente a referência feita a Savatier pelo insigne Caio Mário da Silva Pereira, que diz: O fundamento da reparabilidade pelo dano moral está em que, a par do patrimônio em sentido técnico, o indivíduo é titular de direitos integrantes de sua personalidade, não podendo conformar-se a ordem jurídica em que sejam impunemente atingidos. Colocando a questão em termos de maior amplitude, Savatier oferece uma definição de dano moral como ¿qualquer sofrimento humano que não é causado por uma perda pecuniária¿, e abrange todo atentado à reputação da vítima, à sua autoridade legítima, ao seu pudor, à sua segurança e tranquilidade, ao seu amor próprio estético, à integridade de sua inteligência, a suas afeições etc. (Traité de La Resposabilité Civile, vol. II, nº 525 .). Na fixação do quantum referente à indenização por dano moral, não se encontrando no sistema normativo brasileiro método prático e objetivo, o juiz deve considerar as condições pessoais do ofendido; o seu ramo de atividade; perspectivas de avanço e desenvolvimento na atividade que exercia, ou em outra que pudesse vir a exercer; o grau de suportabilidade do encargo pelo ofensor e outros requisitos, caso a caso. Requisitos que há de valorar com critério de justiça, com predomínio do bom senso, da razoabilidade e da exequibilidade do encargo a ser suportado pelo devedor. Com base nessas premissas, considerando-se a circunstância de que a indenização deve ter, sim, caráter punitivo, penalizando a conduta imprópria, desleixada e negligente, como a adotada pela Ré, desestimulando a prática de novos atos ilícitos, é de se entender que a indenização deve ser estipulada em R$ 5.000,00 (cinco mil reais), segundo os critérios de razoabilidade, atento às peculiaridades do caso concreto e de modo a evitar que a reparação se constitua enriquecimento indevido da pessoa prejudicada, mas também considerando o grau de culpa e porte econômico da empresa causadora do dano, que deve ser desestimulada a repetir o ato ilícito. Por essa razão, ao meu sentir, o

> decisum merece parcial reforma. Em vista de tais razões, com a devida vênia, voto no sentido de CONHECER E DAR PROVIMENTO PARCIAL AO RECURSO, para reformar a sentença impugnada e declarar a nulidade do contrato de que trata os autos, condenada à Ré a devolução, em dobro, do valor referente ao que foi descontado indevidamente no benefício da autora, mediante a devolução do valor creditados na conta corrente da consumidora, bem como condenar a Ré ao pagamento do valor de R$ 5.000,00 (cinco mil reais), a título de indenização pelos danos morais causados à parte recorrente, com juros legais a partir da citação, nos termos do art. 405 do Código Civil, e correção monetária a partir desta data (Súmula 362 do STJ). Sem condenação ao pagamento das custas processuais e dos honorários advocatícios, consoante o disposto no art. 55 da Lei nº 9.099/95. Sala das Sessões, data certificada pelo sistema. Marcelo Silva Britto Juiz Relator."
>
> (TJ-BA - RI: 00019972020218050211, Relator: MARCELO SILVA BRITTO, TERCEIRA TURMA RECURSAL, Data de Publicação: 04/05/2022)

Nesta jurisprudência do Tribunal de Justiça do Estado da Bahia, trata-se de um caso envolvendo um recurso judicial no qual a parte recorrente, Marinei Virgem Carneiro Lima, contesta a validade de um contrato de empréstimo bancário consignado realizado pelo Banco Pan S.A.

A recorrente alega que não solicitou o empréstimo, porém, o valor foi depositado em sua conta bancária, o que ela comunicou ao banco e posteriormente depositou o valor em juízo.

O contrato de empréstimo apresentado pelo banco contém uma assinatura virtual e reconhecimento facial que não cumprem os requisitos estabelecidos pela Instrução Normativa do INSS 28/2008, não se encaixando no conceito de autorretrato (selfie), tornando-o ilegítimo para comprovar a veracidade da contratação.

A recorrente alega vulnerabilidade do consumidor diante da complexidade da operação e solicita a anulação do contrato, suspensão dos descontos e indenização por danos morais.

A Turma Recursal do Tribunal de Justiça da Bahia decidiu que o contrato apresentado pelo banco não prova a validade da contratação devido às irregularidades no reconhecimento facial.

Considerou também que o ônus de comprovar a regularidade da cobrança recai sobre o banco, especialmente por se tratar de contrato supostamente intermediado por correspondente bancário com possibilidade de comissão.

Diante das evidências de fraude e vulnerabilidade da recorrente, a decisão reformou parcialmente a sentença anterior, declarando a inexistência de relação jurídica entre as partes, determinando a restituição em dobro do valor descontado, devolução do valor depositado e condenação do banco a pagar uma indenização por danos morais no valor de R$ 5.000,00.

O voto do relator destacou que o dano moral é indenizável em casos de conduta ilícita e que a reparação deve ter caráter punitivo e preventivo, desestimulando práticas semelhantes. A decisão também considerou critérios de razoabilidade e proporcionalidade na fixação do valor da indenização.

A jurisprudência trata de um caso em que a recorrente alega fraude em um contrato de empréstimo consignado, cuja validade é contestada devido a problemas no reconhecimento facial e na prova de autenticidade.

O tribunal decidiu a favor da recorrente, declarando a inexistência do contrato, determinando a restituição do valor e concedendo uma indenização por danos morais.

Frente às deliberações acerca deste assunto, torna-se notório que as ameaças associadas ao emprego do reconhecimento facial se acentuam quando aplicado de maneira negligente, ou na ausência de outros mecanismos suplementares para garantir de maneira definitiva a identidade do indivíduo em questão, isto é, para confirmar inequivocamente que o sujeito que busca adquirir um empréstimo é efetivamente a pessoa em questão.

O que suscita apreensão reside no aspecto de que indivíduos idosos que ostentem analfabetismo, semialfabetizo, ou um reduzido entendimento acerca de assuntos financeiros, possam se encontrar vulneráveis a essa circunstância,

tornando-se alvos da criminalidade, e em grande medida ignorantes acerca da viabilidade de assertivamente demandar seus direitos.

Cumpre ressaltar que a identificação por meio de sistemas de vigilância por câmeras carece de uma certeza inabalável, uma vez que, frequentemente, a vítima é impulsionada por um ímpeto de justiça, e as similaridades fenotípicas podem comprometer o desfecho em pauta, podendo contribuir de forma substancial para a prisão injustificada de um inocente.

Frente ao delineado, é imperativo que se efetue uma aplicação da tecnologia de modo proveitoso, para a solução de controvérsias, entretanto, simultaneamente, deve-se observar os procedimentos legais, e não se restringir unicamente a tal meio probatório, uma vez que a justiça não pode ser administrada à custa da confusão de indivíduos íntegros, afetando diretamente a dignidade destes.

5 Considerações finais

A confluência da era digital com o avanço tecnológico tem engendrado uma paisagem complexa e desafiadora, onde a transformação social e a otimização dos processos se entrelaçam com dilemas éticos e jurídicos prementes. Nesse cenário multifacetado, emerge o tema do reconhecimento facial, uma tecnologia emblemática que tanto promete inovação e conveniência quanto suscita profundas preocupações relativas à privacidade, aos direitos individuais e à própria dignidade da pessoa humana.

É inegável que o reconhecimento facial tem assumido um papel protagonista nas narrativas tecnológicas contemporâneas, delineando um horizonte que transcende o imaginário e materializa-se em sistemas cada vez mais sofisticados e ubíquos.

A busca pela eficiência em processos de identificação e aprimoramento da segurança têm pautado a disseminação dessa tecnologia em diversas esferas da vida cotidiana, do acesso a dispositivos móveis à vigilância em espaços públicos e privados. Contudo, em meio ao entusiasmo suscitado por tais avanços, emergem dilemas profundos que clamam por análises reflexivas e medidas de regulamentação.

A ausência de uma legislação específica para o reconhecimento facial torna-se um vácuo jurídico preocupante que permite, em muitos casos, que essa tecnologia seja empregada sem critérios claros, salvaguardas adequadas e supervisão regulatória.

Tal omissão normativa gera um ambiente propício para abusos e violações, uma vez que as fronteiras entre a proteção da segurança pública e a preservação das liberdades individuais podem ser facilmente comprometidas.

Urge, portanto, a necessidade premente de uma legislação específica que estabeleça diretrizes claras para o desenvolvimento, implementação e uso do reconhecimento facial, com ênfase na proteção dos direitos humanos e da privacidade.

A temática transcende a esfera técnica e adentra o terreno filosófico e ético. A dignidade da pessoa humana, pedra angular dos direitos fundamentais, ressoa nesse contexto com urgência e relevância.

A coleta massiva e não consentida de dados biométricos, muitas vezes obtidos sem o conhecimento e a autorização das pessoas, mina a autonomia e o controle sobre informações pessoais, comprometendo a própria noção de autodeterminação informacional.

A transformação de rostos em informações processáveis e categorizáveis pode se converter em uma afronta à individualidade, transformando seres humanos em meros conjuntos de dados suscetíveis a manipulações e usos indevidos.

O risco de discriminação e viés algorítmico adentra também esse panorama complexo. O reconhecimento facial, se não cuidadosamente projetado e treinado, pode perpetuar e amplificar desigualdades sociais e raciais já enraizadas, expondo a fragilidade de algoritmos que, ao replicar preconceitos e estereótipos, tornam-se instrumentos de injustiça.

A interseção entre tecnologia e justiça social, assim, demanda uma abordagem crítica e atenta, visando a equidade e a equanimidade em todas as fases da implementação dessas tecnologias.

A preservação da dignidade humana requer, portanto, a conciliação entre os imperativos tecnológicos e as garantias fundamentais. A reflexão sobre os limites do reconhecimento facial, bem como a articulação de salvaguardas e parâmetros regulatórios, não se trata de um mero exercício acadêmico, mas de um imperativo de nossa época.

É indispensável o desenvolvimento de normas que garantam a proporcionalidade entre os benefícios da tecnologia e os riscos inerentes à sua utilização, protegendo os indivíduos de serem reduzidos a entidades rastreáveis e controláveis por algoritmos.

Em um mundo que almeja a inovação e a conectividade, não podemos negligenciar o compromisso inalienável com a dignidade e os direitos de cada ser humano.

A necessidade de uma legislação específica para o reconhecimento facial não é apenas um anseio jurídico, mas um chamado ético para assegurar que a tecnologia seja moldada por princípios de justiça, responsabilidade e respeito à individualidade. Ao ancorar-se nesses pilares, poderemos enfrentar os desafios inerentes a essa tecnologia, garantindo que o futuro seja uma construção coletiva de prosperidade, liberdade e dignidade para todos.

Em suma, o estudo dos erros inerentes ao sistema de reconhecimento facial deixa claro que a adoção indiscriminada dessa tecnologia representa um desafio significativo, suscetível de comprometer a própria dignidade da pessoa humana. Os equívocos frequentes e as consequências adversas que podem advir desses erros evidenciam a urgência de abordar essa questão de maneira mais ampla e sensata.

A análise detalhada dos casos em que indivíduos inocentes foram afetados erroneamente ressalta a importância de se estabelecer uma legislação específica que regule rigorosamente o uso do reconhecimento facial. A falta de parâmetros legais claros pode levar não apenas a injustiças, mas também a uma deterioração da confiança nas instituições e na própria tecnologia.

Diante desse cenário, é indispensável buscar um equilíbrio entre a inovação tecnológica e a proteção dos direitos fundamentais de cada indivíduo. A implementação responsável do reconhecimento facial requer a adoção de salvaguardas éticas e legais robustas, que garantam a preservação da dignidade, da privacidade e dos direitos de todos os cidadãos.

É, portanto, uma obrigação da sociedade e dos legisladores colaborar para criar uma base legal que assegure que a tecnologia seja utilizada de maneira justa e equitativa, minimizando os riscos de violações dos direitos humanos.

Em última análise, ao encarar os desafios e limitações do reconhecimento facial, resta claro que o desenvolvimento de uma legislação específica é não apenas uma necessidade premente, mas também um passo crucial para promover a convivência harmoniosa entre a tecnologia e a dignidade da pessoa humana na era digital.

6 Referências bibliográficas

GOMES, Helton Simões. Bancos e lojas pagam até R$ 4,70 por acesso a dados do seu rosto. UOL, 06 ago. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/08/06/bancos-e-lojas-pagam-ate-r-47-para-acessar-dado-do-rosto-de-brasileiros.htm. Acesso em: 27 de julho de 2023

PEIXOTO, Guiga . Projeto de lei: PL 2392/2022. câmara dos deputados, 2022. Disponível em: https://www.camara.leg.br/propostas-legislativas/2334803 . Acesso em: 15 jul. 2023.

PEREIRA, Débora. O USO DE CÂMERAS DE RECONHECIMENTO FACIAL EM CONTEXTO DE PÓS DEMOCRACIA–UMA FERRAMENTA CONTRA O INIMIGO NO DIREITO PENAL?. Disponível em: http://www.adpeb.com.br/v18/wp/wp-content/uploads/2021/02/O-USO-DE-C%C3%82MERAS-DE-RECONHECIMENTO-FACIAL-EM-CONTEXTO-DE-P%C3%93S-DEMOCRACIA-%E2%80%93-UMA-FERRAMENTA-CONTRA-O-INIMIGO-NO-DIREITO-PENAL.pdf

DA ROSA, Alex; DE ARAÚJO PESSOA, Sara; DA SILVA LIMA, Fernanda. Neutralidade tecnológica: reconhecimento facial e racismo. Revista V! RUS, v. 1, n. 21, 2020. Disponível em: http://vnomads.eastus.cloudapp.azure.com/ojs/index.php/virus/article/view/61/64

DE AZEVEDO, Maurício Goez; DE FARIA, Rubens Alexandre. RETRATO FALADO–A EVOLUÇÃO DO MÉTODO INDICIÁRIO PARA RECONHECIMENTO FACIAL. 2014. Disponível em: https://www.canal6.com.br/cbeb/2014/artigos/cbeb2014_submission_757.pdf Acesso em 02 de março de 2023

BAHIA. Tribunal de Justiça do Estado da Bahia. Recurso inominado. Contrato de empréstimo bancário não solicitado pela autora. Marinei Virgem Carneiro Lima. Relator: Marcelo Silva Britto. Bahia. 2022 Disponível

em: https://www.jusbrasil.com.br/jurisprudencia/tj-ba/1489261552 . Acesso em: 20 de agosto de 2023.

STJ: 90 decisões mostram fragilidade do reconhecimento de pessoas. Migalhas. 2022.Disponivel em: https://www.migalhas.com.br/quentes/359391/stj-90-decisoes-mostram-fragilidade-do-reconhecimento-de-pessoas Acesso em: 26/06/23.

BRASIL. Superior Tribunal de Justiça. Súmula nº 333. Cabe mandado de segurança contra ato praticado em licitação promovida por sociedade de economia mista ou empresa pública. Brasília, DF: Superior Tribunal de Justiça, [2007]. Disponível em: <http://www.stj.jus.br/SCON/sumanot/toc.jsp?b=TEMAp=true=0TIT333TEMA0> . Acesso em: 19 ago. 2011.

RODRIGUES, Gustavo. Reconhecimento Facial na Segurança Pública: Controvérsias, riscos e regulamentação. IRIS, 2019. Disponível em: https://irisbh.com.br/reconhecimento-facial-na-seguranca-publica-controversias-riscos-e-regulamentacao/ Acesso em: 15 de março de 2023.

LYNCH, Jennifer. Face Off: Law enforcement Use of Face Recognition Technology. EFF, 2018. Disponível em: https://www.eff.org/wp/law-enforcement-use-face-recognition Acesso em: 15 de março de 2023.

HILL, Kashimir. The Secretive Company That Might End Privacy as We Know It. NYtimes.2021. Disponível em: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html acesso em 10 de março 2023.

DALSENTER, Thamis. Reconhecimento Facial: laissez-faire, regular ou banir?. Migalhas, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial--laissez-faire--regular-ou-banir Acesso em: 26 de junho de 2023.

CAMERON, Dell. Polícia de Detroit admite que reconhecimento facial não funciona em 96% das vezes. Migalhas, 2020. Disponível em:

https://gizmodo.uol.com.br/policia-detroit-reconhecimento-facial-nao-funciona-96-por-cento-das-vezes/ acesso em 26/06/2023

Woodrow Bledsoe Originates Automated Facial Recognition. History of Information. Disponível em: https://www.historyofinformation.com/detail.php?entryid=2495 acesso em 02 de março de 2023.

Reconhecimento facial: como a tecnologia se expandiu. Thales group, 2023. Disponível em: https://www.thalesgroup.com/pt-pt/countries/americas/thales-brazil/dis/governo/inspire-se/reconhecimento-facial/surgimento-da-tecnologia#:~:text=O%20reconhecimento%20facial%20j%C3%A1%20tem,programa%C3%A7%C3%A3o%22%20podiam%20reconhecer%20rostos%20humanos. Acesso em 02 de março de 2023.

Exclusivo: 83% dos presos injustamente por reconhecimento fotográfico no Brasil são negros. G1 Globo, 2021. Disponível em: https://g1.globo.com/fantastico/noticia/2021/02/21/exclusivo-83percent-dos-presos-injustamente-por-reconhecimento-fotografico-no-brasil-sao-negros.ghtml Acesso em: 05 de maio de 2023.

APPLE. Sobre a tecnologia avançada do Face ID. 14 de novembro de 2018. Disponível em: https://support.apple.com/pt-br/HT208108. Acesso em 16 jun. 2019.

GOMES, Giovanna. A BRUTAL MORTE DE FREDDIE GRAY POR POLICIAIS NOS EUA. Aventuras na história, 2021. Disponível em: https://aventurasnahistoria.uol.com.br/noticias/reportagem/a-brutal-morte-de-freddie-gray-por-policiais-nos-eua.phtml?utm_source=site&utm_medium=txt&utm_campaign=copypaste 26 de março 2023.

DEVICH-CYRIL, Malkia. A LUTA DECISIVA CONTRA O RECONHECIMENTO FACIAL. Instituto Buzios, 2020. Disponível em: https://www.institutobuzios.org.br/a-luta-decisiva-contra-o-reconhecimento-facial/ 26 de março de 2023.

BRANDOM, Russell. How should we regulate facial recognition?. The verge, 2018. Disponível em: https://www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules Acesso em: 23 de março de 2023.

http://pensando.mj.gov.br/wp-content/uploads/2016/02/PoD_59_Lilian_web-1.pdf 28/06/2023

BAHIA. Tribunal de Justiça do Estado da Bahia. Recurso inominado. Contrato de empréstimo bancário não solicitado pela autora. Marinei Virgem Carneiro Lima. Relator: Marcelo Silva Britto. Bahia. 2022 Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-ba/1489261552 . Acesso em: 20 de agosto de 2023.

BRASIL, Tribunal de Justiça do Estado de Santa Catarina, Habeas Corpus - 686317 SC 2021/0255611-2. Santa Catarina. Habeas (STJ - HC: XXXXX SC XXXXX/XXXXX-2, Relator: Ministro JESUÍNO RISSATO (DESEMBARGADOR CONVOCADO DO TJDFT), Data de Publicação: DJ 13/08/2021) recorrente: Anderson Augustinho Barbosa Silva. Recorrido: Tribunal de Justiça do Estado de Santa Catarina. Relator: Desembargador Jesuino Rissato. 2021. Disponível em: < https://www.jusbrasil.com.br/jurisprudencia/stj/1263047678 > acesso em: 16 de julho 2023.

Brewer, N., & Wells, GL (2011). Identificação de testemunha ocular. Current Directions in Psychological Science , 20 (1), 24–27. https://doi.org/10.1177/0963721410389169

RAMIRO, André. Psicopolíticas: vigilância e segregação no reconhecimento facial. IP REC. Disponível em : https://ip.rec.br/blog/psicopoliticas-vigilancia-e-segregacao-no-reconhecimento-facial/. Acesso em: 27 de março de 2023.

BRASIL, Tribunal de Justiça do Estado da Bahia. Recurso Inominado 0001997-20.2021.8.05.0211 Bahia. Contrato de empréstimo bancário não solicitado pela parte autora disponibilização do valor em conta bancária de titularidade da consumidora que comunicou o fato ao banco e depositou o valor em juízo. contrato de empréstimo consignado juntado aos autos (evento 21), com assinatura virtual. reconhecimento facial[...] Recorrente: Marinei Virgem Carreiro Lima. Recorrida: Banco Pan. Relator: Juiz Marcelo Silva Brito. 2021. Disponível

em:< https://www.jusbrasil.com.br/jurisprudencia/tj-ba/1489261552 > acesso em 19 de julho de 2023.