ISSN 2238-9121

TECNOLOGIAS DE RECONHECIMENTO FACIAL E ALGORITMOS DISCRIMINATÓRIOS: IMPLICAÇÕES E DESAFIOS NA PROTEÇÃO DE DADOS

TECHNOLOGIES AND DISCRIMINATORY ALGORITHMS: IMPLICATIONS AND CHALLENGES IN DATA PROTECTION

Camille Hilgemann Almança
Aline Martins Rospa

RESUMO

O artigo explora como a crescente adoção das TRF em diversas esferas, como segurança pública, monitoramento comercial e até mesmo nas interações cotidianas, trouxe à tona preocupações éticas e sociais profundas. Entre as principais questões abordadas, está a propensão dessas tecnologias a refletirem e reproduzirem preconceitos existentes na sociedade, gerando discriminação contra minorias raciais, grupos marginalizados e outros indivíduos vulneráveis. Em síntese, as TRFs têm um papel potencialmente transformador na sociedade, mas seu desenvolvimento e uso requerem uma vigilância constante para garantir que suas aplicações respeitem e promovam os direitos humanos. A busca por justiça e equidade nas TRF não é apenas um desafio técnico, mas uma questão essencial para o futuro das relações entre tecnologia e sociedade. O artigo parte do seguinte problema de pesquisa: como estabelecer mecanismos de proteção jurídica eficazes para mitigar os riscos de discriminação algorítmica nas Tecnologias de Reconhecimento Facial (TRFs), garantindo a proteção dos dados pessoais e a privacidade dos indivíduos? O objetivo geral é compreender como estabelecer mecanismos de proteção jurídica eficazes para mitigar os riscos de discriminação algorítmica nas Tecnologias de Reconhecimento Facial (TRFs), garantindo a proteção dos dados pessoais e a privacidade dos indivíduos. A pesquisa utilizará uma abordagem qualitativa. O método de procedimento será o monográfico. Serão utilizadas as técnicas de pesquisa documental e bibliográfica. Para garantir que as TRFs promovam a justiça e o respeito aos direitos humanos, é necessária uma regulamentação específica que previna discriminações algorítmicas, responsabilizando os envolvidos e garantindo um desenvolvimento inclusivo e ético.

Palavras-chave: discriminação algorítmica; privacidade; tecnologias de reconhecimento facial.

ABSTRACT

The article explores how the growing adoption of Facial Recognition Technologies (FRTs) in various areas, such as public security, commercial monitoring, and even in everyday interactions, has brought to light profound ethical and social concerns. Among the main issues addressed is the propensity of these technologies to reflect and reproduce existing societal biases, resulting in discrimination against racial minorities, marginalized groups, and other vulnerable individuals. In summary, Facial Recognition Technologies have a potentially transformative role in society, but their development and use require constant oversight to ensure that their applications respect and promote human rights. The pursuit of justice and equity in FRTs is not just a technical challenge but an essential issue for the future of the relationship between technology and society. The article stems from the following research problem: how can effective legal protection mechanisms be established to mitigate the risks of algorithmic discrimination in Facial Recognition Technologies (FRTs) while ensuring the protection of personal data and individuals' privacy? The general objective is to understand how to establish effective legal protection mechanisms to mitigate the risks of algorithmic discrimination in Facial Recognition Technologies, ensuring the protection of personal

data and individuals' privacy. The research will use a qualitative approach. The procedure method will be monographic. Documentary and bibliographic research techniques will be used. To ensure that Facial Recognition Technologies promote justice and respect for human rights, specific regulations are necessary to prevent algorithmic discrimination, holding accountable those involved and guaranteeing an inclusive and ethical development of these technologies.

Keywords: algorithmic discrimination; privacy; facial recognition technologies.

INTRODUÇÃO

Nos últimos anos, as tecnologias de reconhecimento facial (TRFs) têm experimentado um avanço considerável, consolidando-se como uma ferramenta cada vez mais comum em diversas áreas da sociedade. Esse crescimento pode ser explicado por diversos fatores, como os avanços em Inteligência Artificial (IA), a disponibilidade de grandes volumes de dados e a crescente necessidade de segurança e praticidade.

As TRFs operam a partir da análise e identificação de características faciais individuais, utilizando sofisticados algoritmos de aprendizado de máquina. Esses algoritmos são treinados com grandes conjuntos de dados faciais, o que lhes permite identificar e distinguir rostos com alta precisão[1] Com isso, a tecnologia tem sido implementada em diferentes aplicações, que vão desde a segurança pública até estratégias de marketing direcionado.

No entanto, apesar dos benefícios oferecidos pelo reconhecimento facial, há um debate crescente sobre suas implicações éticas e legais. Pesquisadores como O'Neil, em 2016, destacam que esses sistemas podem reforçar preconceitos preexistentes, pois os algoritmos de aprendizado de máquina tendem a refletir os vieses contidos nos dados de treinamento. Além disso, apresentam maiores margens de erro para pessoas de determinadas etnias e gêneros, levantando preocupações sobre discriminação e equidade.

A tecnologia de reconhecimento facial compara imagens ou vídeos de indivíduos com um banco de dados previamente armazenado. O sistema mapeia e rastreia os traços faciais em padrões geométricos para identificar as características singulares de cada rosto. Atualmente, é difícil conceber atividades que não sejam monitoradas e classificadas, com os dados sendo utilizados de várias maneiras.

Dessa forma, o papel do Estado é fundamental na regulação e supervisão do uso das TRFs, assegurando que seu uso esteja alinhado com a legislação vigente e garantindo a

[1]GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. **Deep Learning**. Cambridge, Massachusetts: The MIT Press, 2016.

proteção dos direitos fundamentais, além de promover a devida transparência no uso dos dados coletados por essas tecnologias.

Assim sendo, esse estudo foi provocado pelo seguinte problema de pesquisa: como estabelecer mecanismos de proteção jurídica eficazes para mitigar os riscos de discriminação algorítmica nas Tecnologias de Reconhecimento Facial (TRFs), garantindo a proteção dos dados pessoais e a privacidade dos indivíduos? O objetivo geral é compreender como estabelecer mecanismos de proteção jurídica eficazes para mitigar os riscos de discriminação algorítmica nas Tecnologias de Reconhecimento Facial (TRFs), garantindo a proteção dos dados pessoais e a privacidade dos indivíduos.

Do ponto de vista operacional, segue 3 (três) objetivos específicos: i) analisar como funcionam as Tecnologias de Reconhecimento Facial (TRFs), bem como os avanços tecnológicos que impulsionaram seu desenvolvimento e nos riscos de discriminação algorítmica decorrentes de seu uso; ii) compreender os desafios atrelados as TRFs, principalmente no que tange a discriminação algorítmica e iii) investigar a necessidade de regulamentação das TRFs, destacando como a falta de supervisão pode resultar em discriminação e comprometer os direitos à privacidade e à proteção de dados.

A pesquisa utilizará uma abordagem qualitativa, explorando a utilização de tecnologias de reconhecimento facial (TRFs) no contexto contemporâneo, suas implicações éticas, legais e sociais. O método de procedimento será o monográfico, que tem como premissa o estudo de um caso em profundidade e pode ser considerado representativo de outros casos semelhantes. Serão utilizadas as técnicas de pesquisa documental e bibliográfica. A primeira dar-se-á através da análise de legislação, tratados e convenções. A segunda técnica de pesquisa será realizada através de uma revisão extensa da literatura existente sobre tecnologias de reconhecimento facial, incluindo artigos acadêmicos, relatórios técnicos e estudos de caso.

A justificativa desta pesquisa está na crescente utilização das Tecnologias de Reconhecimento Facial (TRFs) em diversas áreas da sociedade, desde a segurança pública até o uso em transações financeiras. No entanto, essa expansão também levanta preocupações significativas relacionadas à discriminação algorítmica e à proteção de dados pessoais, especialmente diante da falta de mecanismos jurídicos adequados para acompanhar a rápida evolução tecnológica. Nesse contexto, torna-se essencial analisar as legislações existentes, assim como propostas regulatórias em diferentes países, visando a implementação de padrões que garantam a proteção dos direitos dos indivíduos.

Dada a complexidade do tema, esta pesquisa demanda uma abordagem

interdisciplinar, que combine aspectos tecnológicos, jurídicos e éticos na aplicação das TRFs. Ao entender esses fatores, é possível contribuir para a formulação de mecanismos de proteção jurídica mais robustos, além de fornecer subsídios para futuras regulamentações estatais que promovam transparência e responsabilidade no uso dessas tecnologias.

Dado o atual crescimento das tecnologias de reconhecimento facial (TRFs), este tema torna-se relevante e merece debate aprofundado, especialmente no que diz respeito às suas implicações éticas, sociais e jurídicas. Essas tecnologias, exigidas em segurança pública, serviços financeiros e no cotidiano, trazem benefícios potenciais, mas também riscos, como a discriminação algorítmica e transparente de privacidade. Discutir esses desafios em eventos acadêmicos promove uma reflexão necessária para o desenvolvimento de diretrizes e regulamentações que assegurem o uso ético e respeitoso dos TRFs na sociedade, demonstrando assim a o motivo pelo qual deve ser debatido no evento.

1 A APLICAÇÃO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL E SEU FUNCIONAMENTO

Nas últimas décadas, o uso de tecnologias de reconhecimento facial (TRFs) aumentou significativamente, isso ocorreu, em parte, pelos grandes avanços desenvolvidos na seara da inteligência artificial (IA). A tecnologia de reconhecimento facial utiliza algoritmos para comparar a imagem ou vídeo de uma pessoa com um banco de dados previamente armazenado. Em síntese, esse sistema rastreia e mapeia os padrões de uma face humana para identificar suas características únicas. Essa capacidade de identificar indivíduos com base em suas características faciais únicas tem revolucionado diversos setores, desde a segurança pública até o marketing.

O aumento do uso é inquestionável, o que se pode perquirir é como essas tecnologias estão sendo utilizadas. A ética dessas tecnologias depende de diversos fatores, incluindo a qualidade dos algoritmos, o treinamento dos modelos de reconhecimento e a análise das questões de privacidade. A implementação de sistemas de reconhecimento facial levanta importantes questões éticas, como a privacidade individual, a possibilidade de vigilância em massa e o potencial para discriminação algorítmica.

As tecnologias de reconhecimento facial são amplamente utilizadas nas mais diversas áreas, desde a segurança pública, autorização de transações financeiras, controle de acesso em aeroportos e áreas de alta segurança, desbloqueio de smartphones e notebooks, monitoramento de pacientes em hospitais, dentre tantas outras. Em segurança

pública, por exemplo, o reconhecimento facial tem sido utilizado para identificar criminosos em multidões, auxiliar em investigações e prevenir crimes.

Essa tecnologia, que compara um rosto escaneado ou um material em vídeo com uma base de dados, promete um grande ganho em termos de eficiência e celeridade. O reconhecimento facial é uma ferramenta que utiliza padrões biométricos para distinguir uma pessoa com mais agilidade e precisão, assim como outras formas de identificação biométrica como as impressões digitais ou leitura da íris, o reconhecimento facial considera características únicas de um indivíduo para confirmar que ele é quem diz ser. Além da segurança, o reconhecimento facial também tem sido utilizado em eventos esportivos para controlar o acesso de torcedores e identificar possíveis ameaças.

Além de sua aplicação em segurança, o reconhecimento facial também tem sido explorado em diversos outros setores, como o marketing, onde é utilizado para personalizar a experiência do cliente, e no varejo, para otimizar processos de pagamento e fornecer recomendações personalizadas. No setor de varejo, por exemplo, o reconhecimento facial pode ser utilizado para criar experiências de compra mais personalizadas, como sugerir produtos com base no histórico de compras do cliente.

Os pontos nodais no rosto de uma pessoa são as variáveis que tornam cada ser humano único, como espaço entre os olhos, espessura dos lábios, cicatrizes, marcas de expressão, comprimento do nariz, dentre outras características. Assim, é criado um mapa facial permitindo que as tecnologias de reconhecimento façam a validação e identificação daquele indivíduo. A criação desse mapa facial é um processo complexo que envolve a análise de uma grande quantidade de dados e a aplicação de algoritmos de aprendizado de máquina.

É importante destacar que a precisão do reconhecimento facial pode variar dependendo de fatores como a qualidade da imagem, a iluminação e a pose do indivíduo. Além disso, a tecnologia ainda apresenta desafios em relação à identificação de pessoas com características faciais similares, como gêmeos idênticos, ou em situações com variações na expressão facial, como o uso de óculos ou máscaras. A precisão do reconhecimento facial também pode ser afetada por fatores ambientais, como a presença de sombras ou reflexos.

Algumas discussões podem surgir com a utilização dessa tecnologia, como taxas de erro mais altas para certos grupos demográficos, falta de privacidade dos cidadãos, risco de vazamento ou roubo dos dados e a violação de alguns direitos humanos, isso porque o sistema de reconhecimento facial não pede permissão para fazer a varredura de

informações. Outro lado controverso desta ferramenta é a coleta massiva de dados pessoais que, posteriormente, alimentam os algoritmos, ajudando a definir padrões de comportamento e consumo na sociedade contemporânea. A coleta massiva de dados biométricos levanta preocupações sobre a privacidade e a segurança das informações, além de questões relacionadas à discriminação e ao viés algorítmico.

Algoritmos podem ser definidos como rotinas logicamente encadeadas. Também podem ser compreendidos como o conjunto de instruções introduzidas em uma máquina para resolver um problema bem definido[2], por isso quando há a captura de imagens ou vídeos para a formação do banco de dados que servirão para as TRFS é muito importante que se saiba como, de fato, esses algoritmos estão programados para funcionar. A transparência na programação dos algoritmos é fundamental para garantir a imparcialidade e a equidade do sistema de reconhecimento facial. A transparência algorítmica é essencial para garantir que os sistemas de reconhecimento facial não sejam utilizados para discriminar grupos específicos da população.

2 ANÁLISE DOS DESAFIOS ASSOCIADOS AO USO DE TRFS: A DISCRIMINAÇÃO ALGORÍTMICA.

As TRFs atuais funcionam a partir de alguns passos específicos. Inicialmente, imagens são capturadas por instituições públicas ou privadas (como forças policiais, departamentos de trânsito, agências de identificação civil, empresas privadas de segurança, bancos etc.). Em seguida, essas imagens são convertidas em códigos alfanuméricos, que passam então a integrar as bases com as quais serão feitas as análises. Na fase operacional, uma nova imagem é capturada e comparada com o arquivo para verificação de identidade. O resultado do sistema algorítmico não é uma resposta definitiva (sim ou não), mas um cálculo de probabilidade que atesta qual a chance da nova imagem ser da pessoa cujo dado biométrico estava no arquivo[3].

[2]SILVEIRA, Sergio Amadeu. **Governos dos algoritmos**. Revista de Políticas Públicas, São Luís, v. 21, n. 1, 2017. Poder Político e Gestão Pública: questões e debates contemporâneos. Disponível em: https://periodicoseletronicos.ufma.br/index.php/rppublica/article/view/6123/4492. Acesso em: 15 jul. 2024.
[3]DUARTE, Daniel Edler; CEIA, Eleonora Mesquita. **Tecnologia, segurança e direitos**: os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (PDF). Disponível em: https://nev.prp.usp.br/publicacao/tecnologia-seguranca-e-

Dessa forma, o reconhecimento facial pode significar uma violação inerente ao tratamento de dados biométricos. Segundo o art. 5º, II da Lei Geral de Proteção de Dados Pessoais[4], esses dados são considerados sensíveis, ou seja, dados que, quando tratados de forma inadequada ou irregular, podem causar ou intensificar contextos discriminatórios para os titulares, podendo resultar em danos à personalidade.

A LGPD traz a categoria de dados sensíveis como forma de garantir uma maior proteção no contexto de tratamento de dados que podem ser manejados de forma potencialmente discriminatória e lesiva. O art. 5º, II, da LGPD define como sensíveis os dados pessoais sobre raça, etnia, religião, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, e dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

A coleta e o uso de dados biométricos para reconhecimento facial podem perpetuar e amplificar vieses sociais existentes, como o racismo e o sexismo. Algoritmos de reconhecimento facial são treinados com grandes conjuntos de dados, que podem conter representações desproporcionais de determinados grupos populacionais. Se esses dados de treinamento forem tendenciosos, os algoritmos resultantes também serão, levando a taxas de erro mais altas para minorias étnicas e de gênero. Um exemplo claro disso é a dificuldade que muitos sistemas de reconhecimento facial têm em identificar pessoas negras, especialmente mulheres negras. Essa dificuldade pode levar a falsas identificações, detenções arbitrárias e outras violações dos direitos humanos.

Além disso, a utilização de TRFs em contextos de vigilância pode levar à profilação racial e à discriminação algorítmica, com a criação de perfis de risco baseados em características físicas e comportamentais, o que pode resultar em maior vigilância e controle sobre determinados grupos[5]. Essa vigilância constante pode levar à autocensura e à limitação das liberdades civis, criando um ambiente de medo e insegurança, especialmente para as minorias.

A falta de transparência nos algoritmos de reconhecimento facial é outro desafio importante. É fundamental que as empresas e órgãos públicos que utilizam essas

direitos-os-usos-e-riscos-de-sistemas-de-reconhecimento-facial-no-brasil-2/. Acesso em: 17 jul. 2024.

[4]**LEI Nº 13.709**, DE 14 DE AGOSTO DE 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 19 jul. 2024.

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

tecnologias sejam transparentes sobre como seus algoritmos funcionam, quais dados são coletados e como são utilizados. A ausência de transparência dificulta a identificação e a mitigação de vieses algorítmicos, além de limitar a capacidade da sociedade civil de realizar auditorias e responsabilizar os desenvolvedores por possíveis abusos.

A regulamentação do uso de TRFs é essencial para garantir a proteção dos direitos fundamentais e a prevenção da discriminação algorítmica. É necessário estabelecer normas claras sobre a coleta, o armazenamento e o uso de dados biométricos, além de exigir que os sistemas de reconhecimento facial sejam auditados regularmente para identificar e corrigir possíveis vieses. A criação de mecanismos de responsabilização também é fundamental para garantir que as empresas e os órgãos públicos sejam responsabilizados por qualquer dano causado pelo uso indevido de TRFs.

As tecnologias de reconhecimento facial apresentam um grande potencial para diversas áreas, mas é fundamental que sejam utilizadas de forma responsável e ética. A conscientização sobre os desafios e os riscos associados a essas tecnologias, juntamente com a implementação de medidas de proteção e regulamentação, é essencial para garantir que os benefícios do reconhecimento facial sejam maximizados e que seus impactos negativos sejam minimizados.

Portanto, é necessário refletir sobre como as TRFs podem agravar situações discriminatórias ao coletar esses dados e o que pode ser feito à respeito dessa questão. Exemplificando, em 2009, os funcionários de uma loja nos Estados Unidos demostraram que câmeras da Hewlett-Packard (HP MediaSmart), com capacidade de identificar e seguir rostos nas imagens, funcionavam conforme o esperado com uma funcionária branca, mas eram incapazes de reconhecer o rosto de seu colega negro[6]. Em caso semelhante, o sistema de desbloqueio do Iphone precisou ser revisto depois de alguns casos em que a identificação biométrica falhou em reconhecer o rosto de proprietários chineses[7].

O Brasil é o quinto país que mais possui câmeras do tipo Hikvision e Dahua, conhecidas por sua alta capacidade de reconhecimento facial. Essas câmeras de vigilância são utilizadas na China e o seu uso já foi apontado como violador de direitos humanos, tendo em vista a capacidade das câmeras de perfilamento das pessoas, com base na raça/etnia. Isso porque as TRFs utilizam inteligência artificial por meio de atividade

[6]CHEN, B. **"HP Investigates Claims of 'Racist' Computers"**. Wired, 22 de dezembro de 2009. Disponível em: https://www.wired.com/2009/12/hp-notebooks-racist/. Acesso em 16 jul. 2024.
[7]HAMILL, J. **"Chinese iPhone X owners claim Apple's Face ID facial recognition cannot tell them apart"**. Metro, 22 de dezembro de 2018. Disponível em: https://metro. co.uk/2017/12/22/iphone-x-racist-cant-tell-chinese-people-apart-apple-customersclaim-7178957/. Acesso em 16 jul. 2024.

algorítmica, algo ainda não regulado e que, muitas vezes, pode ser utilizado em desconformidade com leis e garantias fundamentais[8].

Em suma, o uso crescente das tecnologias de reconhecimento facial traz à tona o relevante debate sobre a utilização destas ferramentas na sociedade contemporânea. As TRFs, por óbvio, representam um avanço importante no campo da inteligência artificial, trazendo diversos benefícios em várias áreas de aplicação. Entretanto, é de fundamental importância a análise dos desafios que acompanham esse progresso, como, por exemplo, o entendimento claro acerca do funcionamento dos algoritmos para que não haja nenhum tipo de discriminação e desrespeito ao direito à proteção de dados dos indivíduos.

3 A NECESSIDADE DE REGULAMENTAÇÃO E PROTEÇÃO DE DADOS PESSOAIS FRENTE ÀS TRFS

A todo instante, compras de mercado são registradas em programas de fidelidade que servem para a construção de perfis de consumo e análises de atividade econômica, pulseiras e relógios aferem batimentos cardíacos e temperatura corporal, compondo bases de dados usadas na gestão de leitos hospitalares e na precificação de seguros de saúde, ônibus e carros particulares carregam sensores de GPS que informam sobre o fluxo do trânsito, auxiliando no trabalho de engenheiros de tráfego e atualizando aplicativos de transporte[9].

Nesse aspecto, o papel do Estado é crucial em regular e supervisionar o uso de tecnologias de reconhecimento facial para garantir que sejam utilizadas dentro do ordenamento jurídico de cada país, assim como trabalhando na proteção dos direitos fundamentais e garantindo a devida transparência na utilização dos dados coletados por essas tecnologias.

Como esse setor praticamente não tem regulação, as empresas e os governos, aos poucos, estão implementando políticas e fazendo exigências maiores para utilização dessa tecnologia, mas tudo ainda é embrionário. No Brasil ainda não há legislação que trate

[8]COSTA, Camila. **All Eyes on Me**: Riscos e desafios da Tecnologia de Reconhecimento Facial à luz da Lei Geral de Proteção de Dados. São Paulo: Editora Almedina, 2022.
[9]DUARTE, Daniel Edler; CEIA, Eleonora Mesquita. **Tecnologia, segurança e direitos**: os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (PDF). Disponível em: https://nev.prp.usp.br/publicacao/tecnologia-seguranca-e-direitos-os-usos-e-riscos-de-sistemas-de-reconhecimento-facial-no-brasil-2/. Acesso em: 17 jul. 2024.

desse tema, entretanto, recentemente foi aprovada na União Europeia a lei que trata do uso das inteligências artificiais.

As disposições da lei europeia proíbem explicitamente certas aplicações de inteligência artificial que violem os direitos dos cidadãos. Entre essas proibições, destacam-se sistemas de categorização biométrica baseados em características sensíveis e a coleta indiscriminada de imagens faciais da internet ou de gravações de câmeras de vigilância para a criação de bancos de dados de reconhecimento facial. E, práticas como o reconhecimento de emoções no ambiente de trabalho e em escolas, sistemas de pontuação cidadã, policiamento preditivo e IA que manipula o comportamento humano ou explora vulnerabilidades serão[10].

A necessidade de regulamentação no país é cada vez mais evidente, principalmente considerando o crescimento exponencial do uso de tecnologias de reconhecimento facial (TRFs) em diferentes setores. O avanço dessas tecnologias, sem uma regulação específica, pode implicar em riscos graves à privacidade e à segurança dos cidadãos, bem como à proteção de seus direitos fundamentais.

Um dos principais desafios reside na forma como os dados pessoais são coletados, armazenados e utilizados por sistemas de reconhecimento facial, que muitas vezes operam de maneira invisível para os indivíduos afetados. O uso massivo de dados biométricos, como as características faciais, é altamente invasivo e pode resultar em perfis detalhados que comprometem a liberdade pessoal, além de permitir um nível de vigilância que desafia os limites democráticos. Isso se agrava com a possibilidade de os dados serem utilizados de maneira discriminatória ou para reforçar estereótipos e preconceitos.

Apesar de não haver lei promulgada sobre o tema, existem iniciativas legislativas brasileiras, como o projeto de lei 2.338/23, que trata do emprego de IA. Este projeto tem como objetivo regulamentar aspectos pertinentes ao uso destas tecnologias em território nacional, com o objetivo de proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico[11].

Há também o PL 21/2020 que estabelece fundamentos e princípios para o desenvolvimento e a aplicação da inteligência artificial no Brasil, assim como diretrizes

[10]**Aprovação da lei da inteligência artificial na UE e desafios no Brasil**. Disponível em: <https://www.migalhas.com.br/depeso/405358/aprovacao-da-lei-da-inteligencia-artificial-na-ue-e-desafios-no-brasil>. Acesso em: 19 jul. 2024.
[11]Senado Federal. **PL 2338/2023** -. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 19 jul. 2024.

para o fomento e a atuação do poder público nessa área. Estabelece ainda que o desenvolvimento e a aplicação da inteligência artificial no Brasil têm como fundamentos a não discriminação, a pluralidade, o respeito às diversidades regionais, a inclusão e o respeito aos direitos e garantias fundamentais do cidadão[12].

A busca em delinear traços comuns humanos para antecipar comportamentos não é nova, Cesare Lombroso, por exemplo, ao estudar traços faciais e compleições corporais, procurou estabelecer uma ligação entre essas características com as tendências criminosas dos delinquentes. No entanto, a tecnologia referente a essa temática começou a ser desenvolvida de forma mais expressiva na década de 90, quando o avanço na capacidade de processamento e a disponibilização de amplas bases de dados para treinamento dos algoritmos levaram ao ganho de precisão e à redução de custos.

A obra "All Eyes on Me: Riscos e desafios da Tecnologia de Reconhecimento Facial à luz da Lei Geral de Proteção de Dados"[13], apresenta mecanismos de mitigação de riscos e sugere estratégias jurídicas e técnicas para minimizar violações de privacidade e o uso indevido das tecnologias de reconhecimento facial. Entre as estratégias sugeridas, destaca-se a criação de políticas claras de consentimento informado, que reforçam a importância de obter o consentimento explícito e informado dos indivíduos antes da coleta de seus dados biométricos, garantindo que sejam devidamente esclarecidos sobre como seus dados serão utilizados, armazenados e protegidos, em conformidade com os princípios da LGPD.

Além disso, enfatiza-se a necessidade de transparência no processamento de dados, recomendando que se forneçam informações detalhadas sobre os propósitos da coleta, as entidades envolvidas e os mecanismos de segurança empregados para evitar acessos não autorizados ou vazamentos de dados. Outrossim, ressalta-se a importância da implementação de medidas técnicas robustas de segurança da informação, como o uso de tecnologias de criptografia avançada para proteger os dados biométricos em todas as etapas do processamento, desde a coleta até o armazenamento, além da realização de auditorias regulares nos sistemas de reconhecimento facial para identificar e corrigir

[12]Senado Federal - **PL 21/2020**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/151547>. Acesso em: 18 jul. 2024.
[13]DUARTE, Daniel Edler; CEIA, Eleonora Mesquita. **Tecnologia, segurança e direitos**: os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (PDF). Disponível em: https://nev.prp.usp.br/publicacao/tecnologia-seguranca-e-direitos-os-usos-e-riscos-de-sistemas-de-reconhecimento-facial-no-brasil-2/. Acesso em: 17 jul. 2024.

possíveis vulnerabilidades[14].

O princípio da minimização de dados também é sugerido como uma estratégia eficaz para reduzir riscos, implicando que sejam coletados e processados apenas os dados biométricos estritamente necessários para a finalidade pretendida, evitando-se a coleta excessiva ou desnecessária de informações sensíveis. Essas estratégias combinam esforços jurídicos e tecnológicos para garantir um uso mais seguro e responsável dessas tecnologias[15].

As políticas de consentimento informado e a transparência no processamento de dados são essenciais para assegurar que os indivíduos tenham controle sobre seus dados e entendam como estes serão utilizados, mitigando o risco de discriminação. Se os usuários não estiverem cientes de como seus dados são coletados e utilizados, eles podem ser alvos involuntários de decisões algorítmicas discriminatórias.

Além disso, a ênfase na minimização de dados se relaciona diretamente à discriminação algorítmica. A coleta excessiva de dados pode gerar perfis detalhados que são usados para categorizar indivíduos de maneira prejudicial, enquanto a coleta restrita aos dados estritamente necessários reduz a probabilidade de discriminação.

Por fim, a implementação de medidas técnicas robustas e auditorias regulares nos sistemas de reconhecimento facial também pode identificar e corrigir falhas que poderiam levar a decisões enviesadas, contribuindo assim para um uso mais ético e responsável da tecnologia. Portanto, as estratégias apresentadas por Schlottfeldt não apenas visam proteger a privacidade, mas também são cruciais para combater a discriminação algorítmica, promovendo um ambiente mais justo e igualitário no uso dessas tecnologias.

CONCLUSÃO

A crescente adoção das TRF em diversas esferas, como segurança pública,

[14]DUARTE, Daniel Edler; CEIA, Eleonora Mesquita. **Tecnologia, segurança e direitos**: os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (PDF). Disponível em: https://nev.prp.usp.br/publicacao/tecnologia-seguranca-e-direitos-os-usos-e-riscos-de-sistemas-de-reconhecimento-facial-no-brasil-2/. Acesso em: 17 jul. 2024.

[15]DUARTE, Daniel Edler; CEIA, Eleonora Mesquita. **Tecnologia, segurança e direitos**: os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (PDF). Disponível em: https://nev.prp.usp.br/publicacao/tecnologia-seguranca-e-direitos-os-usos-e-riscos-de-sistemas-de-reconhecimento-facial-no-brasil-2/. Acesso em: 17 jul. 2024.

monitoramento comercial e até mesmo nas interações cotidianas, trouxe à tona preocupações éticas e sociais profundas. Entre as principais questões abordadas, está a propensão dessas tecnologias a refletirem e reproduzirem preconceitos existentes na sociedade, gerando discriminação contra minorias raciais, grupos marginalizados e outros indivíduos vulneráveis.

Enquanto as TRF oferecem grandes avanços tecnológicos com potencial para melhorar a eficiência em várias áreas, elas também apresentam riscos significativos à medida que algoritmos mal calibrados ou treinados com conjuntos de dados enviesados podem falhar em identificar corretamente certos grupos, ou ainda, fazer isso de maneira prejudicial. A discriminação algorítmica é, portanto, uma questão central quando se trata de justiça e equidade no uso dessas tecnologias.

É possível verificar conforme as informações trazidas, que o combate à discriminação algorítmica exige uma abordagem multidisciplinar e integrada. Isso significa que soluções técnicas, éticas e legais devem ser trabalhadas em conjunto para criar um ecossistema onde o uso de TRF não comprometa direitos fundamentais.

Como observado, a legislação atual, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, estabelece diretrizes importantes para a proteção da privacidade dos indivíduos. No entanto, ainda há lacunas quando se trata de TRF, especialmente em relação à discriminação algorítmica. Embora a LGPD seja um marco regulatório relevante, ela não trata de forma específica das peculiaridades da tecnologia de reconhecimento facial, nem aborda diretamente os riscos de discriminação algorítmica. Isso implica na necessidade de reformas legislativas que sejam mais direcionadas às novas tecnologias emergentes e suas implicações sociais.

Outro ponto importante é o debate sobre a responsabilidade civil e penal em casos de uso inadequado das TRF. Se por um lado a criação de algoritmos enviesados ou a utilização de sistemas discriminatórios pode violar direitos fundamentais, por outro, ainda existem poucos mecanismos para responsabilizar empresas, desenvolvedores ou até mesmo agentes públicos pelo uso inadequado dessas ferramentas. É imprescindível que novas regulamentações tratem dessa questão, prevendo punições e compensações para as vítimas de discriminação algorítmica, bem como a responsabilização das entidades envolvidas.

Outrossim, tendo em vista que essas tecnologias são amplamente utilizadas em todo o mundo, as regulamentações locais, apesar de importantes, podem não ser suficientes para garantir que os direitos fundamentais sejam protegidos de forma universal.

Por fim, é importante ressaltar que a governança das TRF deve ser pensada a partir de uma perspectiva de longo prazo. O desenvolvimento de uma tecnologia justa e inclusiva demanda um esforço contínuo para adaptação às novas realidades sociais e tecnológicas que emergem constantemente. Isso significa que qualquer regulamentação ou política pública sobre TRF deve ser flexível o suficiente para acompanhar as inovações, sem abrir mão de princípios fundamentais como a equidade, a transparência e o respeito aos direitos humanos. Somente assim será possível construir um cenário em que as TRF possam ser utilizadas de maneira benéfica, minimizando os riscos de discriminação e assegurando a proteção da privacidade e da dignidade humana.

Em síntese, as Tecnologias de Reconhecimento Facial têm um papel potencialmente transformador na sociedade, mas seu desenvolvimento e uso requerem uma vigilância constante para garantir que suas aplicações respeitem e promovam os direitos humanos. A luta contra os algoritmos discriminatórios deve ser contínua, e isso só será possível através de uma combinação de inovação tecnológica responsável, regulação jurídica eficaz e uma conscientização social que exija o respeito pela dignidade de todos os indivíduos. Assim, a busca por justiça e equidade nas TRF não é apenas um desafio técnico, mas uma questão essencial para o futuro das relações entre tecnologia e sociedade.

REFERÊNCIAS

CHEN, B. **“HP Investigates Claims of ‘Racist’ Computers”**. Wired, 22 de dezembro de 2009. Disponível em: https://www.wired.com/2009/12/hp-notebooks-racist/. Acesso em 16 jul. 2024.

COSTA, Camila. **All Eyes on Me**: Riscos e desafios da Tecnologia de Reconhecimento Facial à luz da Lei Geral de Proteção de Dados. São Paulo: Editora Almedina, 2022.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. **Deep Learning**. Cambridge, Massachusetts: The MIT Press, 2016.

HALL, Edward T. **A Dimensão Oculta**. Rio de Janeiro, Ed. Francisco Alves, 1977.

HAMILL, J. **“Chinese iPhone X owners claim Apple’s Face ID facial recognition cannot tell them apart”**. Metro, 22 de dezembro de 2018. Disponível em: https://metro.co.uk/2017/12/22/iphone-x-racist-cant-tell-chinese-people-apart-apple-customersclaim-7178957/. Acesso em 16 jul. 2024.

Negri, S. M. C. de Ávila, de Oliveira, S. R., & Costa, R. S. (2020). **O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL BASEADAS EM INTELIGÊNCIA ARTIFICIAL E O DIREITO À**

PROTEÇÃO DE DADOS. Direito Público, 17(93). Recuperado de https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740 LAKATOS, E. M.; MARCONI, M. A. Metodologia científica. 6. ed. São Paulo: Atlas, 2011.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 19 jul. 2024.

MINAYO, Maria Cecilia de Souza (org.). **Pesquisa Social**: teoria, método e criatividade. 31 ed. Petrópolis: Vozes, 2012.

SILVEIRA, Sergio Amadeu. **Governos dos algoritmos**. Revista de Políticas Públicas, São Luís, v. 21, n. 1, 2017. Poder Político e Gestão Pública: questões e debates contemporâneos. Disponível em: https://periodicoseletronicos.ufma.br/index.php/rppublica/article/view/6123/4492. Acesso em: 15 jul. 2024.

Aprovação da lei da inteligência artificial na UE e desafios no Brasil. Disponível em: <https://www.migalhas.com.br/depeso/405358/aprovacao-da-lei-da-inteligencia-artificial-na-ue-e-desafios-no-brasil>. Acesso em: 19 jul. 2024.

Senado Federal. **PL 2338/2023** -. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 19 jul. 2024.

Senado Federal - **PL 21/2020**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/151547>. Acesso em: 18 jul. 2024.

DUARTE, Daniel Edler; CEIA, Eleonora Mesquita. **Tecnologia, segurança e direitos**: os usos e riscos de sistemas de reconhecimento facial no Brasil. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (PDF). Disponível em: https://nev.prp.usp.br/publicacao/tecnologia-seguranca-e-direitos-os-usos-e-riscos-de-sistemas-de-reconhecimento-facial-no-brasil-2/. Acesso em: 17 jul. 2024.

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