FALHAS DA REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO COMBATE À DISCRIMINAÇÃO ALGORÍTMICA REALIZADA PELO RECONHECIMENTO FACIAL

Failures of Artificial Intelligence regulation in the fight against algorithmic discrimination carried out by facial recognition

Amanda Louise Negri[1]
Luís Alexandre Carta Winter[2]

RESUMO

A tecnologia de reconhecimento facial ainda é incapaz de ser utilizada na esfera da persecução penal sem apresentar vieses demográficos. Esforços em regulamentar o uso da inteligência artificial são notórios, principalmente na Europa. O Brasil ao se basear na legislação europeia, busca um maior controle no uso dessas tecnologias, que já são implementadas na identificação de suspeitos, mesmo diante de violações aos direitos fundamentais, principalmente no que se refere a igualdade racial. Com base nesse contexto a pesquisa busca responder a seguinte pergunta: os projetos que almejam a regulamentação da IA, no Brasil, são eficazes no combate à discriminação algorítmica realizada pelo reconhecimento facial? Para isso, a pesquisa utiliza método dedutivo para compreender as diretrizes propostas pelo Anteprojeto da LGPD penal e pelo Marco Legal da Inteligência Artificial e averiguar se essas medidas são capazes de conter a discriminação algorítmica, observada no uso de tecnolo-

ABSTRACT:

Facial recognition technology is still incapable of being used in criminal prosecution without presenting demographic biases. Efforts to regulate the use of artificial intelligence are notable, mainly in Europe. Based on European legislation, Brazil seeks greater control in the use of these technologies, which are already implemented in the identification of suspects, even in the face of violations of fundamental rights, especially with regard to racial equality. Based on this context, the research seeks to answer the following question: are projects that aim to regulate AI in Brazil effective in combating algorithmic discrimination carried out by facial recognition? Within this objective, the research uses a deductive method to understand the guidelines proposed by the Criminal LGPD Draft and the Legal Framework for Artificial Intelligence and determine whether these measures are capable of containing the algorithmic discrimination, especially in the use of facial recognition technologies for criminal prosecution. As a result, the research concluded that even with overcoming technological

[1] Mestre em Direito, pela PUCPR, Professora do Instituto Rhoe e membro do NEADI-PUCPR.

[2] Doutor, Professor na PUCPR, na graduação e no *Strito Sensu;* Professor do Instituto Rhoe; Coordenador do NEADI-PUCPR.

gias de reconhecimento facial para a persecução penal. Como resultado, a pesquisar apontou que mesmo com a superação falhas tecnológicas que ainda comprometem a eficiência da tecnologia, a permissão do seu uso também deve ser embasada no princípio da transparência, essencial na implementação de inteligências artificiais (IA) pelo poder público. Assim, observada a dificuldade no desenvolvimento de IAs que sejam concomitantemente acuradas e transparentes, ainda se torna inviável a implementação da tecnologia de reconhecimento facial sem que haja manutenção da desigualdaderacial

Palavras-chave: globalização, inteligência artificial, reconhecimento facial, desigualdade, discriminação algorítmica

flaws that still compromise the efficiency of the technology, permission for its use must also be based on the principle of transparency, essential in the implementation of artificial intelligence (AI) by public authorities. Thus, given the difficulty in developing AIs that are simultaneously accurate and transparent, it is still unfeasible to implement facial recognition technology without maintaining racial inequality.

Keywords: *globalization, artificial intelligence, facial recognition, inequality, algorithmic discrimination*

SUMÁRIO

Introdução; **1.** Discriminação algorítmica e debate sobre reconhecimento facial no eu ai act; **2.** Reconhecimento facial no brasil; **3.** Reflexões sobre o combate à discriminação algorítmica racial causada pelo reconhecimento facial no brasil; Considerações finais; Referências.

INTRODUÇÃO

Desde meados do século XX, o software é utilizado como uma ferramenta de auxílio ao trabalho e mais adiante, as demais tarefas cotidianas. Com o advento da inteligência artificial (IA), os softwares passam a ter a habilidade de imitar a mente humana para resolução de problemas e tomada de decisão, ou seja, além do trabalho manual, há também um processo de digitalização do trabalho cognitivo. Dentro da IA, a tecnologia que permite a criação de softwares capazes de realizar decisões cognitivas mais complexas é denominada *machine learning* (aprendizado de máquina em português). Softwares dotados dessa tecnologia são capazes de criar

algoritmos[3], que aprendem e tomam decisões com base na observação depadrões.

Muito embora a criação de sistemas automatizado com IAs busquem realizar uma análise homogênea dos indivíduos, nem sempre esse resultado é alcançado. Cada etapa do processo de criação do software é permeada por vieses humanos. Afinal, como são programados por serem humanos, os valores de cada indivíduo podem se manifestar por meio das escolhas realizadas na construção do programa.

Assim como, esse viés também se manifesta em torno da base de dados utilizada para treinar a IA, já que seus dados se remetem a decisões humanas. O treinamento desses modelos requer uma quantidade extensiva de dados[4], que revela preconceitos estruturais que cercam a ação humana, como a discriminação por raça, gênero, religião etc. Como resultado, a inteligência artificial que busca emular a inteligência humana, acaba também por compartilhar seus preconceitos. Considerando a proteção do princípio da igualdade disposto no art. 5 da Constituição Federal a pesquisa se propõe a responder a seguinte pergunta: os projetos que almejam a regulamentação da IA, no Brasil, são eficazes no combate à discriminação algorítmica realizada pelo reconhecimento facial?

Em busca de responder à pergunta proposta, a pesquisa utiliza o método dedutivo e se divide em três partes. Inicialmente, utiliza o método observacional para analisar como discriminação algorítmica realiza a manutenção da desigualdade com base em sistemas que segregam parcelas marginalizadas da população. Com destaque para da tecnologia de reconhecimento facial (também chamada de biometria facial), a pesquisa aponta vieses demográficos, decisões racistas e implicações do uso do *deep learning* e da opacidade dos algoritmos. O método histórico é utilizado

---

[3] Um conjunto finito de instruções, descritas em passo a passo, que se seguidas pela máquina atingem um determinado objetivo (MICROSOFT AZURE,[s.d]).

[4] Possibilitados principalmente pelos avanços da tecnologia digital como a conectividade e a mobilidade. Nesse contexto surge o *Big Data*, coleções extremamente grandes e diversas de dados estruturados, não estruturados e semiestruturados, com volume variedade e velocidade tão complexos que exigem alto poder computacional para sua análise (GOOGLE CLOUD,[s.d]).

para analisar a iniciativa europeia *EU AI Act* e sua busca pela regulamentação do uso de IAs, assim como, o debate em torno da legalidade do uso de tecnologias de monitoramento.

Na segunda parte, o método histórico é empregado na análise do Anteprojeto da LGPD penal e do Marco Legal da Inteligência Artificial, que se remetem a iniciativas europeias, com enfoque nas disposições que tratam sobre o uso de tecnologias de monitoramento e nos requisitos que permitem sua utilização. O método observacional é utilizado para estabelecer um paralelo entre as propostas e alguns princípios já em vigor na legislação nacional, por meio da Lei Geral de Proteção de Dados(LGPD).

Por fim, utiliza o método observacional para compreender as adversidades tecnológicas e jurídicas que embasam a discussão em torno do banimento da tecnologia de reconhecimento facial e o método comparativo para averiguar se as restrições propostas pelos projetos brasileiros são suficientes para superar a discriminação algorítmica decorrente do uso de tecnologias de reconhecimento facial para persecução penal. Nas considerações finais, ao pontuar a inviabilidade do uso justo e ético da tecnologia, responde à pergunta inicialmente proposta.

1 DISCRIMINAÇÃO ALGORÍTMICA E DEBATE SOBRE RECONHECIMENTO FACIAL NO EU AI ACT

O uso da inteligência artificial como forma de manutenção do preconceito reflete mais uma camada do descaso com grupos já marginalizados pela sociedade. Não se traduz necessariamente em uma escolha, mas tampouco é um resultado surpreendente ou inevitável. No entanto, nem sempre a identificação dos vieses é suficiente para eliminar a discriminação algorítmica. O software de recrutamento da Amazon, aprendeu a tomar decisões discriminatórias contra mulheres, ao rebaixar sistematicamente currículos femininos para vagas de empregos de conhecimento técnico. Mesmo após a identificação do problema, a empresa foi incapaz de eliminar o viés de gênero e precisou desativar o software (LAVANCHY, 2018).

Assim como o viés de gênero, a discriminação racial é frequente em decisões automatizadas. Safiya Noble (2018, p. 1-2) relata que os resultados discriminatórios são frutos de decisões digitais que reforçam relações sociais opressivas e implementam novos modos de perfilamento racial. Essas decisões partem de uma ausência de cuidado com qual será o resultado de processos automatizados para grupos vulneráveis.

Nesse contexto, Cathy O'Neil (2017, p. 26-27, 66) analisa o viés racial com base no software LSI-R, que utilizava um questionário como base para avaliar o risco de reincidência de presos, e acabava por tomar decisões de cunho racista. O software, na busca por aprender padrões, acaba por menosprezar o comportamento do indivíduo em prol da análise de como "pessoas como ele" se comportaram no passado, tomando decisões enviesadas.

Além dos vieses, outro ponto relevante na discriminação algorítmica é a dificuldade de compreender as decisões realizadas por inteligências artificias. Frank Pasquale (2011, p. 3) se refere a esses softwares como caixas pretas, é possível "observar suas entradas e saídas, mas não podemos dizer como um se torna o outro". O uso da tecnologia *deep learning*[5] realiza cálculos para a observância dos padrões, que frequentemente extrapolam a capacidade de compreensão humana. Para proteger o valor econômico de seus algoritmos, as empresas aliam a opacidade natural desses softwares a proteção do segredo industrial. Como resultado, Noble (2018, p. 28, 181), O'Neil (2017, p. 29) e Pasquale (2011, p. 40) apontam a ausência de transparência nesses sistemas e a dificuldade de auditar seus resultados, o que por sua vez, prejudica a contestação de resultados discriminatórios.

Dentro desse contexto a biometria facial é uma tecnologia que "utiliza filtros gerados por computador para transformar imagens faciais em expressões numéricas que podem ser comparadas para determinar sua similaridade" (LEWIS; CRUMPLER, 2021). Para isso, são extraídas carac-

[5] *Deep learning* é uma subárea do *machine learning* que utiliza redes neurais artificiais para alcançar conclusões sem a necessidade de intervenção humana, no qual cada uma das camadas contidas dentro do neurônio escolhe um recurso específico para aprender. (SINGAPORE COMPUTER SOCIETY,[s.d]).

terísticas mensuráveis, estáveis e distintas, como por exemplo as distâncias entre pontos de referência no rosto como olhos, nariz, boca e orelhas (NATIONAL CYBER SECURITY CENTRE, [s.d]).

Assim como outros softwares que utilizam técnicas sofisticadas de IA, o reconhecimento facial está sujeito a vieses principalmente pela ausência de diversidade demográfica na base de dados que será responsável pelo treinamento dos algoritmos. A disparidade racial se tronou notória em 2018 (DOOLEY, 2022, p. 1), após a pesquisa de Joy Buolamwini e Timnit Gebru. Em análise de softwares de reconhecimento facial do Google, Microsostf, IBM e Face++, as autoras descobriram presença de vieses, principalmente no reconhecimento de rostos de mulheres negras, que em média apresentaram uma taxa de erro de 34,7% (contra 0,8% de homens brancos) (BUOLAMWINI; GEBRU, 2018, p. 1-2,6-7).

A sub-representação de indivíduos pretos e principalmente mulheres nos bancos de dados repercute não só na manutenção da desigualdade e do racismo estrutural[6], como no retrocesso de direitos sociais já consolidados ao perseguir grupos marginalizados, projetando seu passado no seu futuro (O'Neil, 2017, p. 47, 135, 141). Não obstante aplicação do reconhecimento facial em diversas esferas, se torna relevante sua análise na esfera penal, onde é utilizado para identificação de suspeitos.

Em Detroit, o uso do reconhecimento facial para a prisão de suspeitos já resultou em 3 alegações de prisões injustas. As vítimas, todas pretas, foram erroneamente identificadas através da biometria facial e presas por crimes que não cometeram (ACLU, 2023). No Reino Unido o grupo *Big Brother Watch* realizou uma análise de policiamento preditivo[7] por IA, os dados revelam que mais de 89% dos alertas de reconhecimento facial da polícia até o momento identificaram erroneamente cidadãos como potenciais suspeitos. As taxas de imprecisão se concentram princi-

---

[6] O termo se refere ao racismo como uma construção histórica, que imputa e perpetua estigmas sociais a pessoa preta, o que por sua vez promove segregação e preconceito racial (POSSA, 2022, p.134).

[7] Prática que consiste em análises individuais fim de determinar o risco de uma pessoa cometer infrações ou de reincidir.

palmente dentre pessoas pardas, pretas, mulheres e afetam até mesmo crianças pretas (BIG BROTHER WATCH, 2023).

De frente com os problemas gerados pela aplicação de IAs, em 2020 a União Europeia discutiu o *EU AI Act*, um quadro legal com o objetivo de regulamentar o uso geral da inteligência artificial. O regulamento ainda não foi adotado e faz parte de um vasto conjunto de regras digitais. A essência da proposta reside na classificação do uso de IAs com base no risco que elas representam: inaceitável, alto, limitado e mínimo/nenhum (HOFFMANN,2023, p. 2-4). Desde a proposta inicial em 2021, três versões foram apresentadas. A primeira do Conselho Europeu em 2022, a segunda com as alterações proposta pelo Parlamento Europeu em 2023 e a terceira em dezembro de 2023, com o acordo entre o Conselho e o Parlamento, que culminou na posterior aprovação do quadro legal em maio de 2023 (EUROPEAN COUNCIL, 2023).

O art. 5 do *EU AI Act* classifica como IAs de risco inaceitáveis, aquelas que representem ameaça para pessoas e por isso tem sua utilização banidas, a exemplo de softwares que incluem: avaliações de risco de pessoas singulares, a fim de avaliar ou prever o risco de uma pessoa singular cometer uma infração penal, com base exclusivamente no perfil de uma pessoa ou na avaliação dos seus traços e características de personalidade; sistemas de IA que criam ou expandem bancos de dados de reconhecimento facial por meio da coleta não direcionada de imagens faciais da Internet ou de imagens de CFTV; a utilização de sistemas de identificação biométrica remota em tempo real, em espaços acessíveis ao público para fins de aplicação da lei, a menos e na medida em que tal utilização seja estritamente necessário etc.

Não obstante o uso do reconhecimento facial realizado por IA esteja banido na UE, sua proibição não é integral e admite três exceções: a busca de vítimas específicas de rapto, tráfico humano, exploração sexual ou pessoas desaparecidas; prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física ou de uma ameaça real e presente ou genuína e previsível de um ataque terrorista; localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal (desde a

investigação até a sanção) contida em lista de 15 crimes[8], quando punidas com uma pena privativa de liberdade ou pena restritiva de liberdade pelo período máximo de pelo menos quatro anos (UNIÃO EUROPEIA, 2023).

Com enfoque na identificação biométrica remota, é relevante observar que houve uma discordância entre a posição do Conselho e do Parlamento. Na primeira versão, o Conselho permite, de forma excepcional, a utilização dos softwares desde que mediante registro e uma autorização judicial ou de uma entidade administrativa independente, com base em uma lista restrita de situações pré-definidas (que incluíam 32 crimes) e medidas voltadas ao combate à opacidade (COUNCIL OF THE EUROPEAN UNION, 2022).

Com base no proposto pelo Conselho, excepcionalidade do uso do reconhecimento facial se justifica perante a necessidade da aplicação da lei, de forma que o interesse público supera os riscos de sua utilização (COUNCIL OF THE EUROPEAN UNION, 2022). A mesma posição não é sustentada na segunda versão do *EU AI Act*, que defende sua proibição. Nessa versão, o Parlamento aponta os riscos da utilização do reconhecimento facial e na concentração de poder na mão dos operadores que utilizam essa tecnologia em espaços acessíveis ao público. Além disso, destaca as imprecisões técnicas da biometria facial realizada por IA e a possibilidade de resultados tendencioso que implicam em efeitos discriminatórios, principalmente no que se refere a idade, etnia, sexo ou deficiência (EUROPEAN PARLIAMENT, 2023).

Por fim, após acordo entre o Conselho e o Parlamento, a versão final do quadro legal torna a permitir de forma excepcional a utilização de sistemas de identificação biométrica em locais de acesso público, com base em uma lista menor, de 15 crimes. Além disso seu uso está

[8] terrorismo, tráfico humano, exploração sexual de crianças e pornografia infantil, tráfico ilícito de entorpecentes ou substâncias psicotrópicas, tráfico ilícito de armas, munições ou explosivos, homicídio, lesões corporais graves, comércio ilícito de órgãos ou tecidos humanos, tráfico ilícito em materiais nucleares ou radioativos, sequestro, retenção ilegal ou tomada de reféns, crimes da competência do Tribunal Penal Internacional, apreensão ilegal de aeronaves ou navios, violação, crime ambiental, assalto organizado ou à mão armada, sabotagem, participação numa organização criminosa envolvida em um ou mais dos crimes listados acima (UNIÃO EUROPEIA,2023).

condicionado à conformidade e autorização de cada direito nacional, com base em uma avaliação de impacto sobre direitos fundamentais (prevista no art. 27) e na necessidade do sistema estar registrado na base de dados da UE (dispensável em casos de urgência). Além disso, inclui outras medidas de segurança, à exemplo da publicação de relatórios sobre o uso desses sistemas e da ponderação sobre as consequências da sua utilização para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências.

Assim como a Europa, o Brasil enfrenta adversidades no uso da IA. É possível notar que a legislação brasileira se remete a União Europeia (UE) em matéria de regulamentação técnológica, a Lei Geral de Proteção de Dados tem como inspiração a *General Data Protection Regulation* (GDPR) da UE. O mesmo ocorre com relação ao reconhecimento facial, tratado no Anteprojeto de Lei de Proteção de Dados para Segurança Pública, e no Projeto de Lei nº 2338/23 que se baseiam respectivamente na Diretiva 680/16 do Parlamento Europeu e no *EU AI Act*. Com base nessas legislações, será realizada uma análise da forma como a legislação brasileira tentará barrar os abusos cometidos pelas tecnologias de reconhecimento facial.

2 RECONHECIMENTO FACIAL NO BRASIL

Na América Latina, a expansão do uso do reconhecimento facial está ligada a segurança pública, na tentativa de mitigar a violência da região (FRANCISCO, 2020, p. 2). Ao final de 2023, o Brasil contabilizava 165 projetos de utilizam a biometria facial, somando mais de 47 milhões de brasileiros potencialmente vigiados por essa tecnologia (O PANÓTIPO, 2023). Para além dos impasses que a própria tecnologia já impõe, o Brasil conta com um contexto que traz ainda mais percalços na utilização do reconhecimento facial.

Marcado pelo racismo estrutural, homens pretos são alvos da abordagem policial. Entre 2011 e 2020 foram contabilizadas 90 prisões in-

justas com base em reconhecimento fotográfico (não necessariamente intermediados por IA), 81% dos identificados eram pessoas pretas (DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO, 2021).No Rio de Janeiro onde a população preta e parda representa 43% do total de cidadãos, 63% relata já ter sido abordado pela polícia (CESEC, 2022).

Exemplos do uso do reconhecimento facial no Brasil denotam diversos problemas nas bases de dados utilizadas. Além dos já mencionados erros na identificação de suspeitos que também resultam em prisões injustas no Brasil, muitos desses casos vem acompanhados do uso de fotos antigas, de baixa qualidade ou até mesmo de fotos de cidadãos inocentes que em virtude de algum erro acabam por integrar a base de dados dos suspeitos da polícia.

A repórter Hellen Guimarães (2021) reuniu diversos casos de prisões fundamentadas em erros de reconhecimento facial por IA. Dentre eles, Alexandre Camargo, preso preventivamente por 37 dias com base em uma foto 3x4 que constava na sua identidade, incorporada à base de dados do Detran, e que erroneamente passou a integrar os registros de suspeitos da Polícia Civil.

Não obstante o Brasil ainda não tenha nenhuma regulamentação a respeito do uso de reconhecimento facial, destaca-se a existência de projetos que tratam do tema. O Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigação Criminal tem como embasamento o art. 4º, III da LGPD , que traça as delimitações da lei e prevê a criação de legislação específica para a utilização de dados nas esferas da segurança pública, defesa nacional e segurança do Estado. Comumente conhecido como LGPD penal, o Anteprojeto foi apresentado a Câmara dos Deputados em 2020, com base nos princípios preestabelecidos na LGPD além de "oferecer balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal" (REIS, 2021, p. 3, BRASIL, 2019) .

Menções ao reconhecimento facial são realizadas no capítulo VII, dedicado às tecnologias de monitoramento e tratamento de dados de elevado risco. O art. 43 permite a utilização das chamadas "tecnologias de

vigilância acrescida de técnicas de identificação de pessoas indeterminadas em tempo real" somente para fins de persecução penal e mediante autorização por lei e decisão judicial (BRASIL, 2019)

A criação de lei que permita o uso de tecnologias monitoramento, deve conter a análise de impacto regulatório (AIR) e relatório de impacto à proteção de dados pessoais (RIPD). Ambos impõem a observância de princípios bases do Anteprojeto, como a não- discriminação (art. 26, 42, §1 e §2) e a transparência (art. 26). Além de citar a necessidade de descrever quaisquer impactos potencialmente díspares do tratamento de dados e da tecnologia de vigilância ou de sua política de uso em quaisquer populações específicas (art. 42, §2º) e de comprovar a adoção das garantias adequadas para os direitos e liberdades do titular, incluído o direito de solicitar a revisão da decisão por uma pessoa natural (art. 23) (BRASIL,2019).

O obstáculo tecnologias de monitoramento e a possibilidade de tratamento discriminatório são reconhecidos pelo Anteprojeto, seu uso seguro encontra guarida na base principiológica do Anteprojeto que trata do princípio a não discriminação no art. 6, XI (BRASIL, 2019). Assim como, se encontra em consonância com o mesmo princípio estabelecidos no art. 6, IX da LGPD (BRASIL, 2018) (BRASIL, 2019). Do mesmo modo, a transparência é um dos princípios guias do Anteprojeto (art. 6, VIII e 6, VI na LGPD) e se torna relevante no contexto do reconhecimento facial e suas reiteradas violações de garantias fundamentais, já que além de munir o titular de direitos com uma maior compreensão da decisão tomada pela inteligência artificial, também oferece uma base para contestá-la (BRASIL, 2019; BRASIL, 2018).

Já o Marco Legal da Inteligência Artificial (Projeto de Lei nº 2338/23) segue a mesma estrutura do *EU AI Act* e subdivide o uso da inteligência artificial em graus de risco. Também é guiado por princípios base (art. 3) para o desenvolvimento, implementação e uso da inteligência artificial. com destaque para: participação humana no ciclo da inteligência artificial e supervisão humana efetiva, não discriminação, justiça, equidade e inclusão, transparência, explicabilidade, inteligibilidade e auditabilidade,

devido processo legal, contestabilidade e contraditório, rastreabilidade das decisões etc. (BRASIL, 2023).

No âmbito da segurança pública, o art. 15 trata do uso do reconhecimento facial de forma contínua em espaços acessíveis ao público é classificado como uma exceção dos riscos excessivos. Restrito ainda a hipótese de previsão de lei federal específica, autorização judicial em conexão com a atividade de persecução penal individualizada e somente para crimes que possuam uma pena máxima de reclusão superior a dois anos, na busca de vítimas de crimes ou pessoas desaparecidas ou em casos de crime em flagrante (BRASIL, 2023).

Em seu parágrafo único, adverte sobre a necessidade de o uso do reconhecimento facial prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, o que inclui a observação dos princípios dispostos na Lei, em especial ao que se refere ao princípio da não discriminação (art. 3, IV) e a necessidade de revisão da inferência realizada pela IA por parte do agente público responsável (art. 3, III) (BRASIL,2023).

Em análise do Anteprojeto e principalmente do Projeto de Lei, o Laboratório de Políticas Públicas e Internet (LAPIN) advertem sobre o potencial abusivo do uso de tecnologias de reconhecimento facial. O LAPIN considera que a prática deveria ser banida, por se tratar "de medida desproporcional, que privilegia um ambiente de constante e excessivo monitoramento". Mesmo a supervisão não é capaz de contornar a sua massiva capacidade discriminatória, em contrariedade ao princípio da não discriminação disposto na Lei e na LGPD (AZEVEDO *et all*, 2023, p. 40).

Também em contrariedade a posição adotada pelas legislações propostas, o relatório redigido pelo Conselho Nacional de Justiça através do Grupo de Trabalho de reconhecimento de pessoas (CNJ, 2022, p. 44), adverte contra o uso de tecnologias de reconhecimento facial dada a sua propensão ao racismo algorítmico. O estudo destaca a seletividade racial no sistema de justiça criminal brasileiro, que resulta na sobre representação de pessoas negras dentre os investigados, processados e condenados e encarcerados. Como consequência, os bancos de dados empregados

ao reconhecimento facial são compostos majoritariamente de pessoas pretas o que potencializa os riscos de falsos positivos e de criminalização desse grupo.

Além das legislações o uso de uma tecnologia com alto potencial de segregação racial é contrário aos princípios constitucionais (art. 5, XLI), ao promover a cultura do encarceramento de populações negras e vulneráveis (AZEVEDO *et all*, 2023, p. 40). Nesse sentido, Alisson Possa estabelece um paralelo entre o reconhecimento facial mediado por IA e o Estado de Coisas Inconstitucional, uma figura de violação permanente de direitos caracterizada por três requisitos: i. uma causa estrutural ou histórica; ii. não pode ser atribuída a um único ente, mas ao Estado em seu conjunto; iii. exige a adoção de medidas de longo prazo (POSSA, 2022, p. 133).

O primeiro se mostra evidente na presença do racismo estrutural e do estereótipo social de pessoas negras como criminosas. O envolvimento do Estado, por meio dos três poderes: executivo por meio da força policial que utiliza o sistema, legislativo através da omissão de proibição do uso da tecnologia de reconhecimento facial e o judiciário ao validar as prisões muitas vezes errôneas realizadas através desse sistema. Por fim, a necessidade de medidas de longo prazo, com base no racismo como um processo histórico e estrutural perpetuado pelo uso da tecnologia de reconhecimento facial que enfraquece a luta contra desigualdade e possibilita a perda de liberdade em prol da segurança pública (POSSA, 2022, p. 143-144).

O LAPIN ainda destaca que a possibilidade de utilização dessa tecnologia para prisões em flagrante, como descrita no Projeto de Lei, "é incompatível com a concessão de prévia autorização judicial e dispensa a expedição de lei federal específica". Também no que concerne ao Projeto, é contraditório que o art. 15 disponha que no âmbito de atividades de segurança pública, somente é permitido o uso de sistemas de identificação biométrica à distância, muito embora o art. 17, XI, XII classifique como inteligência artificial de alto risco o uso de IAs que realizam policiamento preditivo[9](AZEVEDO *et all*, 2023, p. 38-39; BRASIL, 2023).

[9] A LAPIN ressalta a necessidade de proibir o uso da inteligência artificial na prevenção de crimes. Segundo o centro de pesquisa, a prática constitui vigilância em massa e

Para além disso, é interessante observar que mesmo com as restrições de segurança que demarcam os projetos de legislações mencionadas, ainda se discute até que ponto elas seriam o suficiente para garantir o uso desse tipo de tecnologia sem a apresentação dos vieses mencionados, motivo esse que embasa a tentativa de banimento por parte do Parlamento da UE e será tema de uma análise aprofundada.

3 REFLEXÕES SOBRE O COMBATE À DISCRIMINAÇÃO ALGORÍTMICA RACIAL CAUSADA PELO RECONHECIMENTO FACIAL NO BRASIL

O uso da inteligência artificial na realização do reconhecimento facial fomenta debates sobre ameaças aos direitos fundamentais como à privacidade, às liberdades de ir e vir, de reunião e manifestação. Não obstante seu uso questionável, a tecnologia ganha espaço no mercado. Estima-se que o reconhecimento facial cresça 10,40% ao ano resultando em um volume de mercado de US$ 10,34 bilhões até 2030 (STATISTA, [s.d]).

Em um excepcional uso eficiente da tecnologia, o reconhecimento facial empregado para reconhecer os invasores do Capitólio, nos Estados Unidos em 2021. Imagens dos suspeitos da invasão, gravadas no Capitólio ou até mesmo pelos próprios invasores foram analisadas pelos investigadores e comparadas a fotografias e vídeos encontrados nas redes sociais, foram também utilizadas bando de dados que continham fotos de carteiras de motorista e até mesmo passaportes (HARWELL; TIMBERG, 2021). Destaca-se, no entanto, que além das imagens realizadas no Capitólio serem de boa qualidade, dentre os 400 invasores presos ou acusados, 93% são brancos e 86% são homens (CPOST, 2022, p.5).

Ainda assim, suas retiradas falhas em reconhecer tons de pele escuro geram dúvidas relativa à eficácia dessa tecnologia e a torna um potencial reprodutor de racismo estrutural. Com base nesses riscos, a biometria

subverte o princípio da presunção da inocência, já que enquadra todas as pessoas de uma determinada região ou análise como possivelmente culpadas (REIS *et all,* 2021, p. 38-40; AZEVEDO *et all*, 2023, p. 38).

facial foi submetida aos debates observados na UE, a diversas restrições e até mesmo foi banida em alguns estados norte-americanos como Boston e São Francisco (NAJIBI, 2020). A IBM (2020, [s.d]) anunciou que deixaria de investir em tecnologias de reconhecimento facial, a empresa se opõe ao uso de tecnologias que promovem discriminação e injustiça racial. Ela ainda adverte, que seu uso para auxiliar a polícia na proteção de comunidades deve ser acompanhado de maior transparência e testes para averiguar a presença devieses.

Desde 2018, após o estudo de Buolamwini e Gebru revelar um flagrante viés demográfico nas tecnologias de reconhecimento facial, esforços foram empreendidos em extinguir a discriminação algorítmica. Samuel Dooley *et all* (2022, p. 3) apontam 3 segmentos na resolução de vieses relativos ao reconhecimento facial: pré-processo, durante o processo e após o processo. O trabalho de pré-processamento concentra-se principalmente na curadoria de conjuntos de dados e pré-processamentos, como por exemplo os bancos de dados. Durante o processo as pesquisas são método de treinamento de *machine learning* ou a otimização do algoritmo por si só. Por fim, o pós-processamento busca ajustar a decisão no momento da inferência para alinhar com as definições de justiça quantitativa. Além disso, é importante destacar a existência de softwares com o objetivo de neutralizar esses vieses, como o *IBM AI Fairness 360* e o *Google The What-If Tool* (IBM, [s.d]; GOOGLE RESEARCH,[s.d]).

Não obstante os estudos conduzidos na área, não é possível afirmar que a discriminação algorítmica no uso do reconhecimento facial foi resolvida e, portanto, não existe embasamento tecnológico para conceder a autorização legal de sua utilização. Nesse contexto, Christian Rathgeb *et all* relatam a síntese de opiniões e descobertas de diversos pesquisadores que participaram do evento Justiça Demográfica em Sistemas Biométricos, realizado pela Associação Europeia de Biometria em 2021. Segundo os pesquisadores, não obstante a crescente atenção dedicada a neutralização dos vieses, o campo ainda não foi pesquisado de forma exaustiva e apresenta diversos problemas que interferem no funcionamento ético dessa tecnologia (RATHGEB *et all*, 2022, p. 1-2).

Um sistema biométrico justo precisa produzir o mesmo resultado dentre diferentes grupos demográficos. Para isso, os desenvolvedores carecem de uma métrica pré-definida, de preferência padronizada. Contudo, não obstante as tentativas nenhum consenso global[10] foi alcançado. Mesmo com a definição da métrica, existem outros obstáculos nesse campo, como por exemplo a necessidade não só de comparar algoritmos biométricos individuais, mas também para mensurar seus desempenhos em relação ao dos seres humanos (RATHGEB *et all*, 2022, p. 3-4).

A performance do reconhecimento facial também é afetada por imagens com ruídos, ou seja, elementos externos como fatores ambientais e iluminação. Nesse âmbito, Dolley *et all* realizaram uma pesquisa na busca de vieses em imagens com ruído em sistemas acadêmicos e comerciais. Ambos os sistemas apresentaram disparidades demográficas estatisticamente significativas no que se refere a indivíduos: idosos, que se apresentam como masculino[11], pele mais escura e pouca iluminação (DOLLEY *et all*, 2022, p. 2,10).

Como mencionado anteriormente a composição demográfica dos bancos de dados é outro problema que afeta a eficiência do reconhecimento facial. No entanto, muito embora idealmente seja possível medir os diferenciais demográficos, desde que o conjunto de dados possua uma variedade de grupos demográficos que permita avaliações baseadas em cenários distintos, essa variedade não necessariamente resulta em decisões mais justas. Segundo os pesquisadores, isso ocorre porque existe uma relação inversamente proporcional entre os diferenciais demográficos e a precisão do reconhecimento. Existe uma limitação tecnológica que, por ora, impede a criação de um sistema biométrico que mantenha a

---

[10] Iniciativas locais em torno da busca por padrões já podem ser observadas. Na Austrália a ISO/IEC 19795.1:2022 é utilizada para especificar requisitos sobre protocolos de teste com o objetivo de reduzir preconceitos devido à coleta de dados ou procedimentos analíticos inadequados (STANDARDS AUSTRALIA, 2023).

[11] Se comparada com outras pesquisas de vieses, a pesquisa de análise dos resultados de imagens de reconhecimento facial com ruído apresenta contraste no viés de gênero. Segundo os autores, essa diferença provavelmente se justifica no tamanho da cabeça de indivíduos que se apresentam como femininas, que é significativamente maior em razão do cabelo (um marcador de gênero) (DOLLEY *et all*, 2022, p. 9)

eficiência dentre diversos grupos demográficos ao mesmo tempo (RATHGEB *et all*, 2022, p. 4-5).

Dessa forma, inevitavelmente o uso da tecnologia de reconhecimento facial permanece como ferramenta de desigualdade. A reiterada menção do princípio da não-discriminação, torna notório o esforço empreendido tanto pelo Anteprojeto da LGPD Penal quanto no Marco Legal da Inteligência Artificial em traçar requisitos para assegurar decisões mais justas, muito embora ainda não exista a possibilidade de que essas inteligências artificias sejam capazes de cumprí-los. Logo, no âmbito dessas legislações, seu uso legal se resume a duas possibilidades: um relaxamento dos requisitos que permita sua utilização, mesmo diante da opressão algorítmica ou a imposição do princípio da não discriminação que resulta, em termos práticos, na sua proibição.

Além das adversidades tecnológicas, existem impasses jurídicos em torno da coleta de dados e sua conformidade com legislações de segurança de dados, como a LGPD. A base de dados utilizada para a tecnologia de reconhecimento facial é composta de dados biométricos, considerados como dados sensíveis por ambas as legislações, e por isso, requerem a consentimento de seu titular, de forma específica e destacada e para finalidades específicas (BRASIL, 2018).

Ambos os projetos norteiam a regulamentação da inteligência artificial no princípio da transparência (também disposto na LGDP), com isso buscam a utilização de IAs que sejam manejadas de forma compreensível, auditável e contestável. Dolley *et all* (2022, p. 6) apontam que "um processo de tomada de decisão mais transparente é um requisito fundamental para alcançar uma biometria confiável", assim como 70% dos especialistas acreditam na supervisão independente para implementações de sistemas de decisão algorítmicos, incluindo abiometria.

Contudo, a transparência por si só, além de configurar um impasse jurídico, também impõe obstáculos tecnológicos. Não obstante a regulamentação seja primordial no desenvolvimento de IAs mais justas e na melhoria da relação de confiança da população com essa tecnologia, pa-

radoxalmente, a imposição de diretrizes na forma como a IA deve ser desenvolvida, pode retardar a criação de sistemas biométricos mais justos.

Cumprir com os requisitos de transparência adiciona custos na produção da IA. Além disso, Aline Macohin (2023, p. 114, 116-117) também menciona a "dificuldade de equilibrar a capacidade de compreensão dos resultados do sistema e sua acurácia". Os algoritmos interpretáveis ou explicáveis podem resultar em diminuição de eficiência, enquanto aqueles sistemas considerados mais eficientes, por sua vez, muitas vezes têm como base o uso *deep learning* que é naturalmente opaco, de forma que nem os desenvolvedores possuem total compreensão da forma como o modelofunciona.

Mesmo assim, a autora advoga pela necessidade do uso de inteligências artificias explicáveis pela administração pública, como no caso da utilização de sistemas de reconhecimento facial para a persecução penal. Isso porque a administração pública tem um dever perante o cumprimento dos princípios da publicidade, motivação e consequentemente à transparência. Logo, não só o poder público deve estar restrito ao uso de IAs das quais possui pleno entendimento e que não violem nenhuma garantia fundamental, assim como, deve estar preparado para responder questionamentos que emanarem das decisões automatizadas e ser capaz de prestar contas ao cidadão (MACOHIN, 2023, p. 153).

Portanto, é possível observar que mesmo diante das diretrizes e requisitos dispostos no Anteprojeto da LGPD Penal e do Projeto de Lei XXX, os impasses tecnológicos e jurídicos que cercam reconhecimento facial impedem sua aplicação, sem que haja transgressão de direitos fundamentais e a manutenção da discriminação racial.

CONSIDERAÇÕES FINAIS

Os esforços realizados pelo Anteprojeto da LGPD Penal e pelo Marco Legal da Inteligência Artificial, ainda não serão suficientes para garantir o uso de tecnologias de reconhecimento facial sem que haja discriminação algorítmica e violação de direitos fundamentais. O cerne de

seu funcionamento racista está em uma ausência de eficiência da própria tecnologia, o que torna inviável legalizar algo que por essência não funciona de forma neutra.

Primeiro, porque a construção de um aparato tecnológico enfrenta bases ontológicas complexas. Considerando ser uma tecnológica importada, mas que se pretende adequar ao sistema brasileiro, o conceito de ética e de justiça, está longe de ser, aqui, universal.

Segundo, mesmo anos após a exposição de Buolamwini e Gebru os desenvolvedores ainda não foram capazes de anular os vieses presentes nos sistemas de reconhecimento facial. Alguns desses problemas são reflexos históricos, como a representação excessiva de homens brancos que se reflete na amostragem dos bancos de dados e até mesmo dos preconceitos dos programadores que incutem seus vieses (mesmo de que forma inconsciente) nos softwares que desenvolvem. Outras limitações decorrem da própria tecnologia, que ainda tem dificuldade em aliar uma representação demográfica mais ampla e justa com resultados acurados. Logo, é possível observar que nenhuma tecnologia de reconhecimento facial ainda é capaz de observar o princípio da não discriminação, preponderante para a utilização dessa tecnologia nas duas propostas analisadas.

Na hipótese do desenvolvimento de sistemas de reconhecimento facial adequado, o princípio da transparência impõe novos obstáculos, principalmente para a realidade brasileira. O Brasil, como importador de tecnologia, contrata tecnologias das quais não necessariamente tem acesso ao seu funcionamento interno. A explicabilidade dos algoritmos esbarra no seu alto valor econômico, haja vista a desvantagem de mercado em revelar informações que muitas vezes estão protegidas por segredo industrial. Além disso, o reconhecimento facial conta com a opacidade natural de softwares *deep leaning*, que dificultam a possibilidade de tornar esses sistemas mais transparentes, sem que haja prejuízo na acurácia do software.

Terceiro, o Brasil ainda conta com problemas anteriores a tecnologia, como bases de dados de suspeitos que muitas vezes possuem fotos antigas, de baixa qualidade ou até de cidadãos inocentes. Além de um

contexto de persecução penal marcado pelo racismo estrutural, que se revela em uma disparidade no número de abordagens, reconhecimentos e prisões realizadas contra pessoas pretas. De forma que todos esses fatores levam a conclusão de que ainda não há possibilidade dessa tecnologia ser empregada em território nacional. Mesmo com a concretização dos projetos analisados, seu uso resultará inevitavelmente na manutenção da desigualdade racial.

REFERÊNCIAS

ACLU. AMERICAN CIVIL LIBERTIES UNION. **After Third Wrongful Arrest, ACLU Slams Detroit Police Department for Continuing to Use Faulty Facial Recognition Technology**, 6 ago. 2023. Disponível em: https://www.aclu.org/press-releases/after-third-wrongful-arrest-aclu-slams-detroit-police-department-for-continuing-to-use-faulty-facial- recognition-technology. Acesso em: 07 out. 2023.

AZEVEDO, Cynthia Picolo Gonzaga de; BUARQUE, Gabriela; PEREIRA, José Renato Laranjeira de. **Nota técnica sobre PL 2338/2023 que busca regular a IA**. Brasília: LAPIN, 2023. 56 p.

BRASIL [Lei Geral de Proteção de Dados]. **Lei nº 13.709, de 14 de agosto de 2018**. Diário Oficial da União, Brasília, DF, 1984. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.Acesso em: 08 out. 2023.

BRASIL. Câmara dos Deputados. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**, de 26 de novembro de 2019. Brasília: Câmara dos Deputados, 2019. Disponível em: https://static.poder360.com.br/2020/11/DADOS- Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 08 out. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei n° 2338, de 2023**, de 3 de maio de 2023. Brasília: Câmara dos Deputados, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 08 out. 2023.

BIG BROTHER WATCH. **65 parliamentarians call for "immediate stop" to live facial recognition surveillance**, 6 out. 2023. Disponível em: https://bigbrotherwatch.org.uk/2023/10/65-parliamentarians-call-for-immediate-stop-to--live- facial-recognition-surveillance/. Acesso em: 07 out. 2023.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *In:* Proceedings of Machine Learning Research, v. 81, p. 1–15, 2018. New York, **Conference on Fairness, Accountability, and Transparency**. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 07 out. 2023.

CESEC. CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA. **Negros são os mais abordados pela polícia no rio em qualquer situação**, diz pesquisa, 15 fev. 2022. Disponível em: https://cesecseguranca.com.br/reportagens/negros--sao-os-mais-abordados-pela-policia- no-rio-em-qualquer-situacao-diz-pesquisa/. Acesso em: 08 out. 2023.

CNJ. CONSELHO NACIONAL DE JUSTIÇA. **Grupo de trabalho reconhecimento de pessoas**. Brasília: CNJ, 2022. 172 p.

COUNCIL OF THE EUROPEAN UNION. **Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain Union legislative acts - General approach, 25 November 2022.** Brussels, 2022. Disponível em: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf. Acesso em: 07 out. 2023.

CPOST. CHICAGO PROJECT ON SECURITY AND THREATS. **American Face of Insurrection**: Analysis of Individuals Charged for Storming the US Capitol on January 6, 2021. Chicago: CPOST, 2022. 34 p.

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO. **Relatórios apontam falhas em prisões após reconhecimento fotográfico**, 24 fev. 2021. Disponível em: https://www.defensoria.rj.def.br/noticia/detalhes/11088-Relatorios-apontam-falhas-em-prisoes-apos-reconhecimento-fotografico. Acesso em: 08 out. 2023.

DOOLEY, Samuel *et all.* Robustness Disparities in Face Detection. *In:* **36th Conference on Neural Information Processing Systems**, 2022. Disponível em: https://proceedings.neurips.cc/paper_files/paper/2022/file/f9faef4e1b4dbbd48ef-60056ffe14c9 0-Paper-Datasets_and_Benchmarks.pdf. Acesso em: 07 out. 2023.

EUROPEAN COUNCIL. **Artificial intelligence act:** Council and Parliament strike a deal on the first rules for AI in the world, 9 dez. 2023. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial--intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide--rules-for-ai/. Acesso em: 18 dez. 2023.

EUROPEAN PARLIAMENT. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and

of the **Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), 14 jun. 2023.** Strasbourg, 2023. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html. Acesso em: 07 out. 2023.

FRANCISCO, Pedro Augusto P; HURE, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público**: avaliação de experiências internacionais. Rio de Janeiro: Instituto Igarapé, 2020. 20 p.

GOOGLE RESEARCH. **The What-If Tool:** Interactive Probing of Machine Learning Models, [s.d]. Disponível em: https://research.google/pubs/the-what-if-tool-interactive- probing-of-machine-learning-models/. Acesso em: 08 out. 2023.

GOOGLE CLOUD. **What is Big Data?,** [s.d]. Disponível em: https://cloud.google.com/learn/what-is-big-data. Acesso em: 07 out. 2023.

GUIMARÃES, Hellen. **Nos erros de reconhecimento facial, um "caso isolado" atrás do outro**, 24 set. 2021. Disponível em: https://piaui.folha.uol.com.br/nos-erros-de- reconhecimento-facial-um-caso-isolado-atras-do-outro/. Acesso em: 07 out. 2023.

HARWELL, Drew; TIMBERG, Craig**. How America's surveillance networks helped the FBI catch the Capitol mob**, 02 abr. 2021. The Washington Post. Disponível em: https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/. Acesso em: 08 out. 2023.

HOFFMANN, Mia. **The EU AI Act: A Primer**, 26 set. 2023. CSET. Disponível em: https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/#:~:text=The. Acesso em: 07 out. 2023.

IBM. **AI Fairness 360**, [s.d]. Disponível em: https://aif360.res.ibm.com/. Acesso em: 08 out. 2023.

IBM. **IBM CEO's Letter to Congress on Racial Justice Reform**, 11 nov. 2020. Disponível em: https://www.ibm.com/policy/facial-recognition-sunset-racial-justice-reforms/#:~:text=Each%20Of%20the%20citizens%20of,race%2C%20color%20or%20creed. Acesso em: 08 out. 2023.

LAVANCHY, Maude. **Amazon's sexist hiring algorithm could still be better than a human,** nov. 2018. IMD Business School. Disponível em: https://www.imd.org/research-knowledge/digital/articles/amazons-sexist-hiring-algorithm--could-still-be-better-than-a- human/. Acesso em: 07 out. 2023.

LEWIS, James Andrew; CRUMPLER, William. **How Does Facial Recognition Work?,** 10 jun. 2021. CSIS. Disponível em: https://www.csis.org/analysis/how-does-facial-recognition-work. Acesso em: 07 out. 2023.

MACOHIN, Aline. **Inteligência artificial e a transparência na administração pública brasileira.** 2023. Tese (Doutorado em Direito das Relações Sociais) – Ciências Jurídicas, Universidade Federal do Paraná, Curitiba, 2023. Disponível em: https://acervodigital.ufpr.br/xmlui/handle/1884/84997. Acesso em: 08 out. 2023.

MICROSOFT AZURE. **Machine learning algorithms,** [s.d]. Disponível em: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-machine- learning algorithms#:~:text=Each%20algorithm%20is%20a%20finite,to%20achieve%20a%20certain%20goal]. Acesso em: 07 out. 2023.

NAJIBI, Alex. **Racial Discrimination in Face Recognition Technology**, 24 out. 2020. Disponível em: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face- recognition-technology/. Acesso em: 08 out. 2023.

NATIONAL CYBER SECURITY CENTRE. **Biometric recognition and authentication systems**, [s.d]. Disponível em: https://www.ncsc.gov.uk/collection/biometrics/face.Acesso em: 07 out. 2023.

NOBLE, Safiya Umoja. **Algorithms of Oppression**: how search engines reinforce racism. 1ª edição. New York: New York University Press, 2018. 229 p.

O'NEIL, Cathy. **Weapons of Math Destruction**: How Big Data Increases Inequality and Threatens Democracy. Reprint ed. New York: Crown Publishing Group, 2017. E-book. 277 p.

O PANÓTIPO. **Monitor de novas tecnologias na segurança pública do brasil**, 07 dez. 2023. Disponível em: https://www.opanoptico.com.br/#regioes.Acesso em: 08 out. 2023.

PASQUALE, Frank. **The Black Box Society**: the secret algorithms that control money and information. 1ª ed. Cambridge: Harvard University Press, 2015. 311 p.

POSSA, Alisson. O reconhecimento facial como instrumento de reforço do estado de coisas inconstitucionais no brasil. **IDP Law Review**, *[S. l.]*, v. 1, n. n.2, 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/lawreview/article/view/5943. Acesso em: 7 out. 2023.

RATHGEB, Christian *et all*. Demographic Fairness in Biometric Systems:What do the Experts say? **IEEE Technology and Society Magazine,** [s.l], v. 41, n. 4, dec. 2022. Disponível em: https://arxiv.org/pdf/2105.14844.pdf. Acesso em: 08 out. 2023.

REIS, Carolina *et all*. **Nota técnica sobre o anteprojeto de lei de proteção de dados para a segurança pública e investigação criminal**. Brasília: LAPIN, 2021, 88 p.

SINGAPORE COMPUTER SOCIETY. **Simplifying the difference:** machine learning vs deep learning, [s.d]. Disponível em: https://www.scs.org.sg/articles/machine-learning-vs-deep-learning. Acesso em: 07 out. 2023.

STANDARDS AUSTRALIA. **Biometric systems: How Standards Australia is supporting the growing industry**, 11 jul. 2023. Disponível em: https://www.standards.org.au/news/biometric-systems-how-standards-australia-is-supporting-the-growing-industry. Acesso em: 08 out. 2023.

STATISTA. **Facial Recognition** – Worldwide, [s.d]. Disponível em: https://www.statista.com/outlook/tmo/artificial-intelligence/computer-vision/facial-recognition/worldwide#:~:text=The%20market%20size%20in%20the,US%2410.34bn%20by%202030. Acesso em: 08 out. 2023.

UNIÃO EUROPEIA. **AI Act:** European Parliament 'Corrigendum' of 16th April 2024. Parlamento Europeu, 16 abr. 2024. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_PT.pdf. Acesso em: 03 maio 2024.