INTELIGÊNCIA ARTIFICAL E SEGURANÇA PÚBLICA: O RECONHECIMENTO FACIAL COMO FERRAMENTA DE DISCRIMINAÇÃO ALGORÍTMICA

Giovanna Prudence Santos de Matos (IC) e Eduardo Altomare Ariente (Orientador)

Apoio:PIBIC CNPq

RESUMO

O presente artigo busca demonstrar que o uso de sistemas de inteligência artificial de reconhecimento facial para fins de segurança pública coloca em risco liberdades civis, direitos e garantias fundamentais, por isso devem ser regulamentados garantindo a observância as legislações constitucional e infraconstitucional e aos princípios éticos. Buscará evidenciar que o reconhecimento facial automatizado aplicado à segurança pública não pode funcionar como ferramenta de vigilância massiva e seu uso deve ser uma exceção devendo cumprir requisitos mínimos para que não haja prejuízo à democracia. Por fim, apontar-se-á que se tal tecnologia não for devidamente regulada e constantemente auditada pelos agentes privados e pelo poder público, seus efeitos serão nocivos aos grupos já discriminados e, por conseguinte, à sociedade como um todo, pois como já observado em outros países, o sistema de reconhecimento facial automatizado é potencialmente discriminatório.

Palavras-chave: Reconhecimento facial; Inteligência Artificial; Racismo.

ABSTRACT

This paper seeks to demonstrate that the use of artificial intelligence systems of facial recognition for public security purposes puts civil liberties, fundamental rights and guarantees at risk, and therefore they must be regulated ensuring compliance with constitutional and infra-constitutional legislation, as well as the ethical principles. Will seek to show that the automated facial recognition applyied to public safety cannot function as a massive surveillance tool, and that its use must be an exception so that there is no harm to democracy. Finally, it will be pointed out that if such technology is not properly regulated and constantly audited by private agents and public authorities, its effects will be harmful to already discriminated groups and, consequently, to society as a whole, because, as already observed in other countries, the automated face recognition system is potentially discriminatory.

Keywords: Facial recognition; Artificial Intelligence; Racism.

1. INTRODUÇÃO

Algoritmos podem reproduzir a forma de pensar humana e tomar decisões em segundos, alguns deles funcionam como ferramenta de identificação de pessoas, como o sistema de reconhecimento facial (RF), que identifica uma pessoa através de sua face ou detecta faces em uma imagem. A identificação consiste no reconhecimento de um indivíduo a partir de suas características faciais. Estes sistemas analisam as imagens captadas por câmeras e são capazes de identificar sujeitos de forma automatizada e rápida e já são utilizados em diversos países para fins de segurança pública.

No Brasil, o uso estatal de softwares de reconhecimento facial é uma realidade e opera em uma lacuna legal. Cumpre ressaltar que a Lei Geral de Proteção de Dados (LGPD), um grande avanço em relação à privacidade e proteção de dados, não regula o uso de dados para fins de segurança pública, conforme o disposto no artigo 3º, III, "a" da referida Lei. Tal tecnologia é testada e utilizada pela polícia de diversos estados brasileiros sem qualquer regulamentação, e na maioria dos casos sem transparência. O uso de RF automatizado deve ser cauteloso e por vezes até proibido. Sua comercialização e utilização precisam ser regulamentadas de forma que as regras a ele impostas não impeçam o seu desenvolvimento, mas garantam os direitos fundamentais à igualdade, liberdade, privacidade, proteção de dados pessoais e os princípios do contraditório e ampla defesa e da presunção de inocência, sendo este um dos principais obstáculos desta nova ferramenta.

Mesmo que em alguns países a utilização de reconhecimento facial não tenha resultado em bons frutos, a tecnologia ainda está em processo evolutivo e é atrativa para o poder público por se tratar de técnica investigativa não invasiva, que independe de contato físico e cooperação do indivíduo. Essa característica também pode ser lida como vigilância massiva e coleta compulsória de informações biométricas. Importa destacar que o direito à privacidade e à proteção de dados são limitados, quando em colisão com outros direitos, como por exemplo a preservação da segurança pública, o que pode justificar a restrição destes direitos, sendo especialmente relevante a preservação da segurança pública. (SARLET, 2017, p. 600).

Há iniciativas que visam garantir a ética na utilização de inteligência artificial em diversas cidades e países, como a Declaração de Toronto visa garantir a proteção dos direitos humanos na era da inteligência artificial (CANADÁ, 2018). A União

Europeia, em 2018, publicou uma iniciativa com diretrizes para seus Estados membros sobre o domínio da inteligência artificial, também abordando a utilização ética e jurídica apropriada da tecnologia (UNIÃO EUROPEIA, 2018).

Nos mais diversos documentos que versam sobre utilização de inteligência artificial pelo poder público existem convergências em torno dos princípios éticos que envolvem sua utilização, são eles o princípio de transparência, da não discriminação (*fairness*), da não-maleficência, da responsabilidade e da privacidade, ou, proteção de dados.

Para a Comissão Europeia é necessário garantir um cenário ético e jurídico apropriado para que haja confiança e responsabilidade durante a utilização de IA, o que se faz considerando também o futuro do trabalho, a equidade, a segurança, a inclusão social e a transparência algorítmica (UNIÃO EUROPEIA, 2018).

A prática mais indicada para a prevenção de discriminação algorítmica é a criação de mecanismos de auditoria que garantam os parâmetros éticos. (LAWGORITHM, p. 2). Destaca-se a importância da criação de comissões ou de uma agência nacional específica que regulem a utilização destas tecnologias e que garantam a pluralidade de seus membros, com a participação de pessoas dos principais grupos discriminados e dos mais variados setores.

O reconhecimento facial automatizado para fins de segurança pública exige atenção, considerando o histórico de erros que fomentam discriminações, isto porque, além de outras razões, os algoritmos operam e aprendem com base em um banco de dados, que quando não alimentado com fotos de pessoas de diferentes raças, ou, se não treinado suficientemente, resulta em falhas de identificação. Logo, se aplicado à segurança pública, sem constantes auditorias e sem a sujeição à aprovação de especialistas, colocará em risco garantias fundamentais, principalmente a liberdade de indivíduos pertencentes aos grupos raciais cujo sistema falha ao reconhecer ou diferenciar, resultando em injustiças sociais (INTERNETLAB, 2020). Tais falhas de reconhecimento citadas ocorreram principalmente com pessoas negras, e são influenciadas por diversos fatores, como no exemplo citado, banco de dados insuficientemente diversificados (BUOLAMWINI, & GEBRU, 2018, p. 7), ou pelo fato de as equipes multidisciplinares que projetam e controlam estes sistemas serem em sua maioria compostas por pessoas brancas.

Diante das mais diversas ações institucionais que têm um impacto desproporcional sobre os grupos racializados, cresce a necessidade de debruçarmo-nos sobre a temática da justiça racial face a complexidade em que o racismo foi constituído. Dentre as possíveis definições de racismo, destacam-se três delas: a individualista, a institucional e a estrutural (ALMEIDA, 2020, p. 35), neste estudo a análise será feita com base nestas duas últimas que guardam relação mais próxima com as instituições estatais de segurança pública.

Os vieses algoritmos da inteligência artificial de reconhecimento facial nos colocam à frente da seguinte problemática: De que forma tais vieses podem ser reduzidos e quais são as recomendações jurídicas a serem seguidas para evitar a propagação de preconceitos sociais na utilização desta tecnologia?

Buscar-se-á demonstrar que o uso destes sistemas, quando atrelados à segurança pública, coloca em risco as liberdades civis e os direitos e garantias fundamentais. E que devem ser regulados de forma a garantir transparência, possibilitando que as decisões sejam questionáveis, através de ações como a criação de comitês, obrigatoriedade da confecção de relatórios de impactos, garantia de ações afirmativas que preservem a isonomia, o contraditório e a ampla defesa.

Se esta inteligência artificial não for devidamente regulada e constantemente auditada, durante sua utilização pelos órgãos estatais de segurança pública, seus efeitos serão nocivos aos grupos já discriminados e, por conseguinte, à sociedade como um todo, pois como já observado em outros países, o sistema tem potencial de reproduzir discriminações.

2. DESENVOLVIMENTO DO ARGUMENTO

2.1. Reconhecimento Facial e Viés Algorítmico Racial

O algoritmo de IA é um sistema de códigos conduzido por um caminho com passos a serem tomados para se chegar em um resultado de forma autônoma, capaz de auto aprender a maneira que realiza as ações (RUSSEL & NORVIG, 1995, p. 37). Estes códigos desenvolvem um papel relevante na sociedade, porém como continuam sendo obras humanas, podem reproduzir discriminações negativas, isto porque são capazes de enxergar padrões invisíveis aos seus desenvolvedores e reproduzir práticas discriminatórias (O'NEIL, 2016, p. 169). A prática de observar padrões

ignorados ou desconhecidos pelos programadores é denominada de viés algorítmico, e são eles os principais responsáveis pelas injustiças algorítmicas.

Os vieses algorítmicos são padrões observados pela máquina sobre uma pessoa e suas características, que quando lidas pelo algoritmo são descartadas, mal classificadas e/ou não atendidas. São questões que foram ignoradas pelos humanos que desenvolveram a máquina, mas matematicamente observadas pelo algoritmo. Os algoritmos sempre cometerão erros porque são simplificações de tarefas humanas, nenhum modelo algorítmico pode incluir toda complexidade do mundo real. (O'NEILL, 2016, p. 26).

Os vieses podem ser relacionados ao gênero, raça, à nacionalidade, à orientação sexual, à deficiência, à idade.

As falhas baseadas na raça ocorrem quando a máquina leva em consideração, ou não, a raça dos sujeitos, e reproduz uma discriminação negativa a partir disso. Se ela não está suficientemente treinada para produzir resultados corretos para todas as pessoas apresentará acurácia menor para algumas delas. O código enviesado não considera os pilares e convicções racistas que fizeram divisões geográficas, acadêmicas e econômicas entre grupos. O mundo é complexo e é impossível incluir toda esta complexidade em um algoritmo (O'NEILL, 2016, p. 26).

O sistema de reconhecimento facial é um algoritmo de tratamento de dados biométricos baseado em traços do rosto humano. Eles identificam faces a partir do reconhecimento de pontos de medidas únicos, como por exemplo distâncias entre o nariz a boca, olhos ao queixo, marcas, cicatrizes formato da face e extremidades do rosto, arcada dentária, estes pontos variam a depender do programa utilizado (CARLO et. al., 2018, p. 9). A face identificada a partir de uma imagem é comparada com os mesmos pontos em imagens do banco de dados. Existem duas principais formas de operação destes softwares, a primeira é através de *facial matching*, ou, verificação, que é a correspondência entre uma imagem estática e isolada de um indivíduo e uma outra imagem do banco de dados, o algoritmo busca um padrão entre as duas imagens. A segunda forma é através de *automated facial recognition*, ou, identificação, as câmeras identificam pessoas em tempo real, combinando suas faces com todas as imagens do banco de dados (CARLO et. al, 2018, p. 9).

Os softwares de reconhecimento facial são treinados a reconhecer faces humanas através do aprendizado de máquina. Um software desenvolvido para fins de segurança pública treinado pelo banco de dados do sistema penitenciário brasileiro possivelmente associará as faces com características próprias do rosto de pardos e pretos à criminalidade, visto que 66,69% da população prisional é parda e preta (INFOPEN, 2019). Em razão do citado encarceramento em massa da população negra, a máquina também será menos eficiente em reconhecer suspeitos brancos.

2.1.1. Princípio da Igualdade

O princípio da igualdade é invocado principalmente em face dos três poderes, legislativo, executivo e do judiciário, mas o alcance do princípio não se restringe a igualar os cidadãos face as normas legais vigentes, mas garante também que a lei não seja estabelecida ou editada em desconformidade com a isonomia (MELLO, 1998, p. 10).

A sociedade brasileira está inserida em um sistema desigual e estruturalmente racista e nesta concepção, a estrutural, a discriminação racial decorre da própria estrutura social, ou seja, da maneira em que se constituem e se mantém as relações políticas, econômicas, jurídicas e sociais. É através do olhar estrutural sob o racismo que Silvio de Almeida conclui: *"a responsabilização jurídica não é suficiente para que a sociedade deixe de ser uma máquina produtora de desigualdade racial"* (ALMEIDA, 2020, p. 51). A discriminação algorítmica é um reflexo dessa estruturação, o combate desta prática se dará através de regulamentação e da garantia da efetiva observância ao princípio da igualdade e de toda a legislação pré-existente, pelos agentes envolvidos na utilização do aparato tecnológico de reconhecimento facial.

A Convenção Internacional Sobre a Eliminação de Todas as Formas Discriminação Racial, ratificada pelo Brasil em 1967, expressa que qualquer discriminação racial, seja ela teórica ou prática, é moralmente condenável, socialmente injusta, perigosa e não justificável em lugar algum, com exceção das discriminações positivas.

O princípio da igualdade, positivado no artigo 5º da Constituição de 1988, é tanto um dever jurídico de tratamento igual do que é igual, quanto um dever jurídico de tratamento desigual do que é desigual. Eventual tratamento desigual justificável, como são as medidas de inclusão racial, ou, ações afirmativas, mas é certa a vedação

de toda e qualquer desigualdade de caráter arbitrário, injustificável (PIOVESAN, 2018, p. 383), como nos resultados enviesados pelas máquinas de RF automatizado.

Verifica-se que o racismo estruturalmente inserido nas instituições também foi introduzido nas novas tecnologias desenvolvidas, e que estas são potentes ferramentas de discriminação racial indireta, capazes de agravar ainda mais o racismo institucional já presente nas instituições.

2.1.2. Presunção de Inocência, Devido Processo Legal e Ampla Defesa

A inexatidão dos resultados do tratamento dos dados com estas tecnologias pode resultar em equívocos nas investigações criminais, portanto, estamos face a potenciais prejuízos aos direitos e garantias individuais e coletivos. Uma pessoa condenada erroneamente e até mesmo tratada equivocadamente como suspeita desrespeita o princípio da presunção de inocência positivado no artigo 5º, inciso LVII da Constituição Federal.

A falta de obrigatoriedade de transparência dos algoritmos e do acesso às informações sobre seu funcionamento prejudica o devido processo legal, pois, dificulta aos réus questionarem a exatidão e relevância das informações obtidas através dos softwares de reconhecimento facial que influenciam a sentença. Sem informações claras sobre os códigos, os resultados são inquestionáveis, portanto, restará prejudicada a ampla defesa dos réus que forem sentenciados com base ou influência das máquinas de reconhecimento facial. Cumpre ressaltar que na esfera penal os efeitos resultantes destas ações errôneas são mais gravosos, pois as sanções penais incluem a privação de liberdade, restrição de direitos eleitorais, a perda do cargo, multas, além dos previstos no artigo 92 do Código Penal brasileiro.

Diante da nova e desafiadora realidade do uso de sistemas de reconhecimento facial, por vezes, fazer prova contrária aos resultados gerados por estas máquinas pode ser impossível se o código utilizado pelo software não for público ou transparente.

2.1.3. Direito à Privacidade

Os sistemas de RF permitem uma vigilância massiva e, por vezes, injustificada da população, colocando em risco o direito à privacidade garantido pelo artigo 5º, X da Constituição. A privacidade individual pode ser relativizada quando em confronto com

direitos coletivos (SARLET, 2017, p. 600), como o direito à segurança pública, mas tal relativização só seria justificável para o uso de sistemas de reconhecimento facial em área de repetidos crimes, condicionando a instalação de câmeras de vigilância equipadas com reconhecimento facial à análise das taxas de criminalidade.

As câmeras de RF permitem, além da identificação, o rastreamento da localização geográfica do indivíduo. Essa facilidade de acesso injustificado à dados pessoais e sensíveis também ameaça e lesa o direito à privacidade, e coloca fim ao conceito de privacidade que conhecemos hoje, o "direito de estar só" ou "direto de ser deixado só", visto que tais tecnologias invadem violentamente a esfera privada da vida dos cidadãos. A privacidade garantida na Constituição Federal por si só não é mais suficiente sendo clara a necessidade de legislações específicas para cada tipo de afronta tecnológica a este direito, como é o reconhecimento facial automatizado. Diante do exposto, verifica-se que tal tecnologia, na forma que é utilizada hoje pelo Estado é inconstitucional e uma possível arbitrariedade.

2.1.3.1. Proteção de Dados Pessoais

O direito à proteção de dados está intimamente vinculado ao direito à privacidade, o que se pode entender como "intimidade informática" (SARLET, 2017, p. 600). Por isso, a proteção de dados pode ser lida como um novo direito fundamental (MENDES, 2014, p. 140). A sociedade atual produz dados como nunca, por isso, tal proteção assumiu um papel extremamente relevante na garantia de direitos.

A Lei Geral de Proteção de Dados, Lei n. 13.709, de 2018, no artigo 40, III, "a" e "d" exclui da sua abrangência os dados tratados para fins de segurança pública e de investigações penais: *"Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: III - realizado para fins exclusivos de: a) segurança pública; (...) d) atividades de investigação e repressão de infrações penais*." Portanto, verifica-se uma lacuna legal na proteção de dados na seara da segurança pública.

A face é um dado pessoal sensível, pois conforme a definição legal disposta no artigo 5º, II da referida lei, é um dado pessoal sobre origem racial ou étnica e biométrico vinculado a uma pessoa natural. A Lei garante à dados dessa natureza maior proteção, e para o tratamento de tais dados se faz necessária a autorização específica e destacada, com finalidades também delimitadas.

Por mais que a legislação não abarque os dados pessoais tratados para fins de segurança pública, da análise do artigo 11º, II, "g", que trata dos processos de identificação e cadastro em sistemas eletrônicos para fins de segurança do titular, verifica-se uma exceção à utilização de dados pessoais sensíveis, quando os direitos e liberdade fundamentais dos titulares exigirem a proteção de dados pessoais. Os sistemas de RF automatizado colocam em risco tais direitos, e a partir da inteligência do referido artigo, entende-se que prevalecem as garantias fundamentais citadas face a tais sistemas.

2.2 A UTILIZAÇÃO DE SISTEMAS DE RECONHECIMENTO FACIAL PARA FINS DE SEGURANÇA PÚBLICA

2.2.1 Experiências Internacionais

Na Flórida, EUA, em 2018, no caso Willie Allen Lynch v. State of Florida, Allen Lynch foi acusado pela prática de tráfico de entorpecentes. Os policiais fotografaram um suspeito e o sistema de RF indicou que às imagens correspondiam à de Willie Allen Lynch. O réu solicitou o acesso às demais fotografias indicadas pelo sistema como "possíveis combinações", a corte de apelações negou o pedido afirmando que cabia ao acusado demonstrar que o resultado da identificação facial seria diferente se as demais fotos fossem acessadas (WILLIE ALLEN LYNCH, Appellant, v. STATE OF FLORIDA, Appellee). Em 2020 em Detroit, Robert Williams foi preso injustamente quando um sistema de RF analisou as imagens da câmera de segurança de uma loja e concluiu que o suspeito era Robert. Ele foi libertado após um dia, quando os policiais reconheceram o erro do software (DE MELO, 2021). Em um recente estudo publicado pelo MIT identificou-se que a taxa de erro dos softwares de reconhecimento facial foi 43 vezes maior para mulheres de pele escura que para homens de pele clara. (JOY & GEBRU, 2018, p. 7).

A polícia britânica e a polícia do País de Gales utilizavam o sistema de reconhecimento facial NeoFace, da NEC. Os dados divulgados demonstram que esse sistema apresentou 93% de reconhecimentos imprecisos de 2016 a 2019 na Inglaterra. Já no País de Gales a polícia armazenou indevidamente fotos de 2.451 pessoas inocentes por um ano, e investigou 31 delas, o que além de ferir o direito à intimidade e privacidade, gerou desconforto e danos psicológicos aos cidadãos (CARLO, KRUECKEBERG & FERRIS, 2018, p. 8).

O governo chinês realiza vultosos investimentos em vigilância, a China foi uma das nações pioneiras na utilização de RF automatizado, em 2017 o país já contava com 170 milhões de câmeras para estes fins. Hoje no país somente através do cadastramento da face é possível acessar a internet, comprar uma linha de celular ou abrir as catracas dos transportes públicos, é através do rastreamento da face que o governo faz a análise de cada cidadão e os atribui notas de acordo com seus atos cotidianos no chamado de "Sistema de Crédito Social". (GUIMARÃES, 2019) (KANTAYYA, 2020).

2.2.2. Experiência Brasileira

No Brasil, testes com esta tecnologia já são realizados em diversos estados, principalmente nos aeroportos internacionais. Em Feira de Santana, Bahia, o sistema de vídeo-monitoramento capturou mais 1,3 milhões de rostos, gerou 903 alertas, 18 mandados de prisão e captura de 15 pessoas (ABRAMCZYK, 2019), desde o início dos testes com a ferramenta no Brasil, 90,5% das pessoas presas são negras. (MOURA, 2019). Um estudo do Instituto Igarapé, publicado em 2019, levantou que 15 cidades brasileiras utilizavam reconhecimento facial para fins de segurança pública e existiam ao menos 47 casos do uso da tecnologia (INSTITUTO IGARAPÉ, 2019).

A Defensoria Pública do Rio de Janeiro publicou um relatório, analisando 47 processos recebidos, entre 1º de junho de 2019 até 10 de março de 2020, cujo reconhecimento dos acusados fora feito em sede policial através de fotografia, das 58 pessoas acusadas apenas 10 são brancos, 40 são pretas ou pardas e 8 não se tinha registro. A prisão preventiva foi declarada em 86,2% dos casos, em média os acusados ficaram 7 meses e 28 dias presos. A pesquisa também foi feita a nível nacional, abrangendo 10 estados brasileiros, 83% dos acusados são pretos ou pardos. Os dois relatórios tinham como critério (1) o reconhecimento pessoal em sede policial ter sido feito por fotografia; (2) o reconhecimento não ter sido confirmado em Juízo; (3) a sentença ter sido absolutória. (DEFENSORIA PÚBLICA DO RIO DE JANEIRO, 2021). Nestes casos o reconhecimento não foi feito por uma máquina e sim pelas vítimas, e pode-se verificar que a falha de reconhecimento mesmo quando feitas por humanos é falha e as falhas recaem principalmente sobre pretos e pardos.

O Serviço Federal de Processamento de Dados (Serpro) se vale de tecnologia de reconhecimento facial para validação de identidades partindo das fotos da base de dados do sistema da Carteira Nacional de Habilitação. Em 2021 o Aeroporto de

Congonhas realizou um embarque 100% digital, sem que fosse necessário que os passageiros apresentassem cartão de embarque ou documento de identidade, a verificação das identidades foi realizada por reconhecimento facial pelo software desenvolvido pelo Serpro, a tecnologia já foi testada para a mesma finalidade em Florianópolis, Salvador, Rio de Janeiro e Belo Horizonte (MINISTÉRIO DA INFRAESTRUTURA, 2021).

O Tribunal de Justiça do Distrito Federal desenvolveu o sistema Amon que reconhece a face dos visitantes que frequentam todas as dependências do referido órgão. Assim como o Tribunal de Justiça do Amazonas que desenvolveu o projeto "Integra TJAM" que instalou 40 câmeras de reconhecimento facial em suas instalações, o projeto foi desenvolvido juntamente com o Instituto de Tecnologia do Norte com aportes da Samsung (CNJ, 2020).

O Laboratório de Políticas Públicas e Internet (Lapin) publicou um relatório que aponta o reconhecimento facial automatizado foi utilizado cerca de vinte e cinco vezes pela administração pública brasileira em 2021, para os mais diversos fins, identificou ainda que em alguns casos as empresas que forneciam as tecnologias tinham livre acesso aos dados tratados e que as entidades públicas tinham pouco conhecimento e treinamento para lidar com as ferramentas utilizadas (REIS, ALMEIDA, DA SILVA & DOURADO, 2021). A ausência de regulação por si só já é um indicador da necessidade de se frear o uso estatal destes sistemas, mas quando somada ao despreparo técnico dos utilizadores, ao tráfego irregular de dados com as entidades privadas e principalmente ao potencial racismo advindo dos mecanismos, verifica-se que o uso de câmeras de RF no Brasil não está sustentado pela ética e pela legislação.

2.3. REGULAÇÃO E ÉTICA DO USO SISTEMA DE RECONHECIMENTO FACIAL PARA FINS DE SEGURANÇA PÚBLICA

2.3.1. Regulação

Nos Estados Unidos, o projeto de Lei S.4084 – Facial Recognition and Biometric Technology Moratorium Act of 2020 defende a proibição do uso de reconhecimento facial pelo Estado para fins de vigilância. A excepcionalidade do uso de reconhecimento facial para fins de investigações está condicionada à autorização expressa do Congresso (ESTADOS UNIDOS, 2020). Essa iniciativa é um marco

importante para a preservação da privacidade nos Estados Unidos e precisa ser considerada quando se trata de regulação da IA de reconhecimento facial.

Diante da realidade aqui retratada, identifica-se a necessidade de regulamentar esta tecnologia, observa-se que toda vigilância massiva pode se tornar um poder de controle excessivo do Estado sobre a população. Entende-se que toda utilização de reconhecimento facial pelo poder público para fins de segurança pública deve ser utilizada em caráter de exceção, como é no referido projeto de lei, visto que a vigilância biométrica coloca em risco os direitos e garantias fundamentais, as liberdades civis e a democracia.

2.3.2. Princípios e Garantias Éticas

As diversas diretrizes sobre ética e IA convergem na garantia dos seguintes princípios: não maleficência, ou seja, a IA não pode causar danos a outrem; não discriminação, igualdade e justiça de forma a coibir a discriminação algorítmica; responsabilidade, capaz de responsabilizar os sujeitos ativos envolvidos no tratamento dos dados pelos danos eventualmente causados; privacidade e proteção de dados, e; transparência, essencial para a garantia do contraditório e ampla defesa. Entende-se que tais princípios se aplicam à todas as formas de inteligência artificial, são princípios gerais comuns à IA como um todo, incluindo o RF automatizado.

A Comissão Europeia destaca quatro princípios básicos de uma IA ética, quais sejam: (i) a autonomia humana, garantindo que a máquina se sujeite integralmente ao ser humano; (ii) a prevenção de danos, não podem gerar danos ou agravar danos já existentes; (iii) equidade, a distribuição justa dos benefícios e dos custos da Inteligência Artificial e a proibição de sistemas enviesados, e; (iv) explicabilidade, informações abertas acerca da IA de forma clara (UNIÃO EUROPEIA, 2018).

Além destes princípios comuns, há outras garantias a serem inseridas na legislação futura, destacam-se algumas delas: a segurança digital, o bem comum, a sustentabilidade, a autonomia e controle humano, a coesão social, a ligação com as ciências políticas e o futuro do trabalho. (HAGENDORFF, 2019, p. 2). A futura legislação deve considerar principalmente a preservação da dignidade humana, todos os seus desdobramentos e possíveis afetações negativas, coibindo qualquer prática contrária a este princípio.

A Declaração de Toronto prevê algumas formas de evitar o enviesamento dos sistemas e práticas discriminatórias: a responsabilização e obrigatoriedade de prevenção às discriminações, a exigência de que os sujeitos ativos protejam os direitos humanos e previnam os riscos de discriminação desde a projeção até o desenvolvimento e utilização dos algoritmos de IA (CANADÁ, 2018).

Para garantia do contraditório e da ampla defesa, necessita-se que a lei, além de abarcar os referidos princípios, estabeleça um nível e critérios de confiabilidade nos resultados da máquina, impedindo uma ultraconfiança neles. Deve-se prever e garantir a repercussão pública e educação sobre o RF automatizados e seus riscos, promovendo acesso às informações a respeito destes e um canal de denúncias que possibilite que os sujeitos passivos possam denunciar práticas abusivas.

É essencial que se promova a educação pública a respeito do funcionamento dos sistemas. Possibilitando o conhecimento sobre a forma em que os dados foram empregados e fornecidos para que se chegasse àquele resultado, garantindo o pleno exercício do acesso à justiça, a utilização de mecanismos oculto viola o devido processo legal, o que é desconhecido não é questionável. (LEONARDO & ESTEVÃO, 2020, p. 25).

2.3.2.1. Pluralidade e Multidisciplinaridade dos Agentes de IA

A tecnologia pode criar as condições prejudiciais à justiça (MENDES, 2014, p. 107). A grande parte das diretrizes alienígenas e nacionais sobre IA não são escritas por equipes multidisciplinares, ou seja, não são compostas por grupos de filosofia, sociologia ou outras disciplinas, mas sim por pesquisadores com formação voltada para a ciência da computação e matemática. A falta de diversidade no campo de pesquisa e desenvolvimento de inteligência artificial e nas culturas do local de trabalho moldam a indústria de tecnologia. Um pequeno grupo de homens predominantemente brancos determina como e para quais propósitos os sistemas de IA são projetados (HAGENDORFF, 2019, 9).

É fundamental para a garantia da justiça que pessoas negras e outras minorias ocupem espaços de poder e prestígio dentro destas instituições. Mas a mera representatividade não impede que a IA atue de forma racista porque a ação dos indivíduos é orientada pelas instituições e tem os princípios da sociedade como pano de fundo (ALMEIDA, 2020, p. 47-49).

A única forma de combater o racismo inerente às instituições sociais é investindo em políticas internas que promovam a igualdade e diversidade, a remoção de obstáculos para a ascensão de minorias em posições de direção, a manutenção de espaços para debates e revisões de práticas institucionais e a promoção da composição de conflitos raciais (ALMEIDA, 2020, p. 47-48). Por isso, é primordial para uma inteligência artificial ética que seus desenvolvedores e demais agentes garantam equipes plurais e multidisciplinares que elaborem relatórios de impactos, prévios a implantação e utilização da IA, capazes de prever os desdobramentos sociais da tecnologia e não somente o resultado matemático correto.

3. CONSIDERAÇÕES FINAIS

O estudo realizado lançou luz sobre a potencialidade lesiva da tecnologia de RF quando aplicada à segurança pública e sobre as possíveis lesões ao direito à privacidade, proteção de dados e à igualdade, sendo este último o principal afetado em razão da complexidade da estrutura racial e a impossibilidade de todos os seus desdobramentos serem considerados pela máquina. Identificou-se também que são colocadas em risco as garantias à ampla defesa, ao devido processo legal e à presunção de inocência. Isto porque os modelos utilizados são propriedade intelectual de entes privados e obscuros, a falta de transparência impossibilita que as decisões do algoritmo sejam questionadas.

Os danos ao princípio da igualdade e justiça são alarmantes, isto porque o racismo estrutural, pilares nos quais as instituições foram fundadas e se mantêm até hoje, está sendo reproduzido também pelos sistemas de reconhecimento facial, visto que as falhas observadas se deram principalmente no tratamento de dados da população negra ou parda. O racismo assume novas formas no decorrer dos anos, passando a ser reproduzido nos mais diversos âmbitos da sociedade, inclusive nas aplicações tecnológicas. Como nas tecnologias de reconhecimento facial, tais falhas são frutos do racismo implícito, muitas vezes explícito, das instituições desenvolvedoras das referidas tecnologias, que não envidam esforços em prever e coibir vieses em seus produtos antes de comercializá-los ou utilizá-los.

A vigilância massiva da população também é uma problemática, porque além de gerar danos psicológicos aos cidadãos, não é justificável e nem razoável. A colheita massificada dos dados biométricos dos transeuntes constitui violação da privacidade em todos os níveis e, quando injustificada, não há que se falar em ponderação de direitos. Tal vigilância possibilita ao Estado um controle excessivo e desproporcional

da sociedade, sendo uma brecha democrática que tende ao autoritarismo. Ainda, se considerarmos as ameaças democráticas enfrentadas atualmente pelo Brasil, tal ferramenta pode gerar maior insegurança jurídica.

Da análise das experiências internacionais foi possível observar que os sistemas falharam ao reconhecer pessoas negras e que algumas destas falhas resultaram em prisões injustas. No Brasil, o reconhecimento facial não automatizado já prejudica pretos e pardos e sua automação reproduziria e pioraria estes resultados, considerando o histórico de falhas das tecnologias de RF.

O encarceramento em massa da população negra é um fator decisivo para a criação dos vieses algorítmicos. Se os bancos de dados utilizados para treinamento da máquina forem o do sistema penitenciário brasileiro. De toda forma, se tais bancos não forem suficientemente plurais e diversificados a máquina tenderá a cometer falhas ao identificar os grupos menos representados.

Atualmente a transparência destas tecnologias é mínima ou inexistente o que dificulta a contestação da acurácia de suas decisões, e, se as decisões potencialmente prejudicam negros, as suas defesas restarão também prejudicadas.

Também foram identificados princípios e garantias gerais a serem inseridos na futura legislação acerca da Inteligência Artificial, como: o princípio da transparência que garante o contraditório e ampla defesa nas decisões tomadas pela IA; a não discriminação, garantindo que algoritmos que não reproduzam qualquer tipo de discriminação; a não-maleficência, ou seja, que não causem quaisquer danos à sociedade; igualdade e justiça, exigindo que os modelos sejam justos durante o tratamento dos dados, em observância ao princípio constitucional da igualdade em todo o processo; o princípio da responsabilidade, isto é, a responsabilização dos desenvolvedores e utilizadores da IA; a privacidade e a proteção de dados.

A regulação futura deve abarcar a obrigatoriedade da produção de relatórios de impactos, testes prévios dos sistemas de reconhecimento facial, estabelecer uma métrica de confiabilidade nos resultados e exigir que os sistemas sejam certificados por uma agência nacional reguladora.

É necessário a criação da Agência Nacional de Inteligência Artificial (ANIA) para maior controle das aplicações, submetendo-as à autorização prévia, testes,

licenciamento e prestação de contas, de forma a controlar as aplicações de inteligência artificial prevenindo e coibindo a discriminação algorítmica e que também conte com um canal de denúncias que garanta proteção dos denunciantes.

A Inteligência Artificial possui natureza complexa, com diversos desdobramentos e exige conhecimentos técnicos específicos que são pouco difundidos atualmente, por isso, um órgão com dedicação exclusiva à esta temática é a forma ideal de controle das aplicações tecnológicas inteligente. A Agência Nacional de Proteção de Dados é insuficiente, assim como qualquer agência reguladora pré-existente em razão da referida especificidade da inteligência artificial.

A atuação da ANIA se daria através de comitês especializados e pluralmente compostos, regulando todo o processo que envolve tais tecnologias, desde o seu desenvolvimento até o seu uso e comercialização. A agência preencheria a lacuna hoje existente em razão falta de regulação das aplicações de IA e principalmente a regulação das tecnologias de reconhecimento facial prevenindo e coibindo o racismo algorítmico.

Outra principal questão que envolve o sistema de reconhecimento facial fazendo-os gerar discriminação algorítmica observada é a falta de pluralidade e multidisciplinariedade dos agentes de IA, isto é, seus desenvolvedores e utilizadores são equipes compostas por homens brancos e com formações voltadas para as ciências computacionais e matemáticas. Por isso, são desenvolvidos softwares que não observam as questões éticas e legais que envolvem as relações humanas.

Por fim, através da presente pesquisa foi possível identificar que a forma em que as máquinas de inteligência artificial de reconhecimento facial estão sendo empregadas na segurança pública é inconstitucional e devem ser freadas e regulamentadas, garantindo a plena aplicação das legislações constitucional e infraconstitucional, sob pena de gerarem danos irreparáveis à população, ao Direito, principalmente aos negros, em razão do viés algorítmico racial.

Há princípios e garantias que precisam obrigatoriamente ser abarcados pela possível legislação, pois garantem a dignidade da pessoa humana e coíbem práticas discriminatórias, são eles: a igualdade, a não maleficência, a responsabilidade, a privacidade, proteção de dados e a transparência; além da segurança digital, do bem comum, da sustentabilidade, da autonomia e controle humano, da coesão social, da

ligação com as ciências políticas e do futuro do trabalho. A lei futura deve prever também a obrigatoriedade de educação da população a respeito dos softwares, fazendo com que as ações destes sejam questionáveis por qualquer cidadão, independente da sua formação ou nível intelectual, mantendo a salvo o contraditório, a ampla defesa e o devido processo legal.

Sistemas de IA de reconhecimento facial são incapazes de prever todos seus impactos sociais negativos, por isso, em se tratando de RF automatizado, seu uso deve se dar em caráter estritamente excepcional, por isso, seu uso indiscriminado deve ser proibido ou permitido apenas em caráter de exceção.

É certo que a regulação do reconhecimento facial automatizado é urgente, visto que a tecnologia é atrativa ao Poder Público e que este cada vez mais a emprega, desconsiderando os seus desdobramentos racialmente nocivos, fato que agrava ainda mais o racismo no Brasil e ferindo a igualdade assegurada pela Constituição. É impossível a coexistência de câmeras de reconhecimento facial controladas pela segurança pública, da forma em que são utilizadas hoje, e do direito à igualdade, privacidade, liberdade, proteção de dados pessoais e garantias como a presunção de inocência, o contraditório e a ampla defesa.

4. REFERÊNCIAS

ALMEIDA, Silvio. **Racismo Estrutural**. 1. ed. São Paulo: Pólen Livros, 2019.

AMARAL, Fernando. **Introdução à Ciência dos Dados**. Alta Books: Rio de Janeiro. 2016.

BORGES, Juliana. **O que é encarceramento em massa?** Belo Horizonte: Letramento, 2018.

BRASIL, C. I. **Rio: programa de reconhecimento facial entra em operação no carnaval.** Agência Brasil, Rio de Janeiro, 27 jan. 2019. Disponível em <https://agenciabrasil.ebc.com.br/geral/noticia/2019-01/rio-programa-de-reconhecimento-facial-entra-em-operacao-no-carnaval>. Acesso em 25 mar. 2020.

BRASIL, Comissão de Juristas. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. 2019. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-

legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em 20 abr. 2021.

BRASIL, Defensoria Pública do Estado do Rio De Janeiro. **Relatório Sobre Reconhecimento Fotográfico em Sede Policial**. Disponível em: https://defensoria.rj.def.br/uploads/arquivos/54f8edabb6d0456698a068a65053420c.pdf. Acesso em 01 mar. 2021.

BRASIL. Ministério da Infraestrutura. **Brasil testa primeira ponte aérea com reconhecimento facial do mundo**. 2021. Disponível em: https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/06/brasil-testa-primeira-ponte-aerea-com-reconhecimento-facial-do-mundo. Acesso em 20 ago. 2021.

BUOLAMWINI, Joy, & GEBRU, Timnit. (2018). **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency**. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 23 abr. 2020.

CARLO, S., KRUECKEBERG, J., e FERRIS, G. (2018). **FaceOff: The lawless growth of facial recognition in UK policing**. (Maio), 56. Disponível em www.bigbrotherwatch.org.uk

CNJ. **Tribunal de Justiça do Amazonas Inaugura 1ª Fase do Sistema de Segurança Institucional**. 2020. Disponível em: https://www.cnj.jus.br/tribunal-de-justica-do-amazonas-inaugura-1a-fase-do-sistema-de-seguranca-institucional/. Acesso em 20 ago. 2021.

DE MELO, João Ozorio. **Ação pede banimento da tecnologia de reconhecimento facial nos EUA.** 2021. Disponível em: https://www.conjur.com.br/2021-abr-26/acao-banimento-tecnologia-reconhecimento-facial-eua. Acesso em: 30 abr. 2021.

ESTADOS UNIDOS. **Lei S.4084 – Facial Recognition and Biometric Technology Moratorium Act of 2020**. 2020. Disponível em:

https://www.congress.gov/116/bills/s4084/BILLS-116s4084is.pdf. Acesso em 12 jun. 2021.

HAGENDORFF, Thilo. (2019). **The Ethics of AI Ethics An Evaluation of Guidelines implemented in decision routines of autonomous**. 2018, p. 1–16.

INFOPEN. **Composição da População por Cor/Raça no Sistema Prisional. Período de julho a dezembro 2019**. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiN2ZlZWFmNzktNjRlZi00MjNiLWFhYmYtNjExNmMyNmYxMjRkIiwidCI6ImViMDkwNDIwLTQ0NGMtNDNmNy05MWYyLTRiOGRhNmJmZThlMSJ9

INTERNETLAB. **As contribuições do InternetLab para a Estratégia Nacional de Inteligência Artificial**. Disponível em: https://www.internetlab.org.br/pt/privacidade-e-vigilancia/as-contribuicoes-do-internetlab-para-a-estrategia-nacional-de-inteligencia-artificial/. Acesso em: 12 jun. 2020.

INSTITUTO IGARAPÉ. **Infográfico do Reconhecimento Facial no Brasil**. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 10 mai. 2021.

KANTAYYA, Shalin. **Coded Bias**. 11 nov. 2020. Netflix.

LAWGORITHM (A Associação de Pesquisa em Direito e Inteligência Artificial) e Núcleo Jurídico do OIC–IEA/USP. **Estratégia Nacional de Inteligência Artificial. Respostas à consulta do MCTIC**. Disponível em: https://docs.google.com/document/d/1ibN5fA0K-TImnwKEXOluGVzcHe5hCi0-GEyfXolklPw/edit. Acesso em: 12 jun. 2020.

MELLO, Celso Antonio Bandeira de. **Conteúdo jurídico do princípio da igualdade**. São Paulo: Malheiros. 1998. ISBN 8574200476.

MENDES, Laura Schertel. Série IDP - Linha de pesquisa acadêmica - **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. Ed. São Paulo: Editora Saraiva, 2014.

MOURA, R. **Novas tecnologias para os suspeitos de sempre**. Rede Observatório da Segurança, Rio de Janeiro, 16 out. 2019. Disponível em <http://observatorioseguranca.com.br/tag/reconhecimento-facial/>. Acesso em 25 mar. 2020.

O'NEIL, Cathy. **Weapons of math destruction: How big data increases inequality and threatens democracy**. Nova Iorque: Broadway Books, 2016.

PIOVESAN, Flávia. **Temas de direitos humanos**. 11. ed. São Paulo: Editora Saraiva, 2018.

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando. **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil**. Brasília: Laboratório de Políticas Públicas e Internet. 2021.

SARLET, Ingo Wolfgang. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017.

THE DAILY: **The end of privacy as we know it?** [Locução de]: Kashmir Hill e Annie Brown. [S.l.]: The New York Times, 10 fev. 2020. Podcast. Disponível em: https://open.spotify.com/episode/3ANRQSAgjGnTTb8quXZyu6?si=nJUnq40YRcOnViLLVrrnNw. Acesso em: 20 fev. 2020.

UNIÃO EUROPEIA, Comissão Europeia. **Inteligência Artificial para a Europa**. 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018DC0237&from=EN. Acesso em 25 mar. 2021.

WILLIE ALLEN LYNCH, Appellant, v. STATE OF FLORIDA, Appellee. Disponível em: https://law.justia.com/cases/florida/first-district-court-of-appeal/2018/16-3290.html. Acesso em: 19 jan. 2021.

Contatos: giovanna_prudence@hotmail.com e eduardo.ariente@mackenzie.br