



**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO**

INGRID BORGES DE AZEVEDO

**RECONHECIMENTO FACIAL E DIREITO: propostas para uma IA
antidiscriminatória**

**Brasília
2021**

INGRID BORGES DE AZEVEDO

**RECONHECIMENTO FACIAL E DIREITO: propostas para uma ia
antidiscriminatória**

Monografia de final de conclusão do curso de graduação apresentada como requisito parcial à obtenção do título de bacharel em Direito pela Universidade de Brasília, desenvolvida sob a orientação da Prof^a. Dra. Fernanda de Carvalho Lage.

BRASÍLIA
2021

TERMO DE APROVAÇÃO

INGRID BORGES DE AZEVEDO

Monografia apresentada como requisito parcial
à obtenção do grau de Bacharela em Direito pela
Faculdade de Direito da Universidade de
Brasília - UnB.

Brasília, 3 de novembro de 2021.

Prof^a. Dra. Fernanda Lage
Professora Orientadora

Prof. Dr. Fabiano Peixoto Hartmann
Membro da banca examinadora

Prof^a. Dra. Talita Rampin
Membro da banca examinadora

Prof^a. Dra. Débora Bonat
Membro da banca examinadora

Agradecimentos

Estudar na Universidade de Brasília era um sonho desde a adolescência, que se tornou possível graças a Deus e aos meus pais, que sonharam comigo, acreditaram no meu potencial e se esforçaram de todas as maneiras possíveis. À eles, toda a minha gratidão, sempre. Agradeço aos meus irmãos, William e Rayanne, por prestarem suporte em todos os momentos da minha vida, por me incentivarem, por se alegrarem comigo com cada conquista, por serem, além de irmãos, meus amigos.

Agradeço, também, aos meus sobrinhos, Miguel e Rafael, por me proporcionarem tanta alegria e por serem combustível para todo o meu esforço. Eu amo vocês. Obrigada, também, à Pipoca, que mesmo com toda a bagunça que faz, me proporciona boas doses de serotonina quando olha para mim e levanta as orelhas como se entendesse o que eu falo, ou quando pula no meu colo sempre que me vê. Deus não poderia ter me dado uma família melhor.

Agradeço, também, às minhas amigas do ensino fundamental e do ensino médio, respectivamente, Alessandra Silva e Lorena Galvão, por sempre terem me incentivado e por terem acreditado em mim. Obrigada por toda a parceria antes e durante a graduação, ainda que cada uma tenha cursado um curso diferente.

Na UnB, tive a felicidade de conhecer diversas pessoas incríveis que me ajudaram a vivenciar a universidade de maneira leve, mas também desafiadora em trabalhos, disciplinas e projetos. Aos meus dois amigos que estiveram comigo desde o anúncio do resultado do vestibular, Daiana Bandeira e Luiz Vinícius Fernandes, toda a minha gratidão por todas as trocas. Agradeço também à minha amiga de luta no Centro Acadêmico de Direito da UnB, de estudos, de trilhas e de samba, Rayssa Cavalcante.

Às Promotoras Legais Populares, aqui representadas por Juliana Veras, Carolina Freire, Gabriela Souza, Lívia Gimenes, Rosa Maria, Ana Letícia, Laíse, Najara Thalita, Sheilaso Oliveira, Íris Hazel, Laerzi, Isabella Maria, Maysa Dias, meu muitíssimo obrigada por me ensinar tanto. Entrei para as PLPs ainda no segundo semestre do curso com o objetivo de vivenciar a universidade em todas as suas dimensões, além de adquirir horas extras, e me surpreendi com o universo que me foi apresentado pela extensão. Além de ser um local de aprendizado, é um lugar de afeto e de compartilhamento de vivências. Obrigada por cada troca durante os quase três

anos em que estive no projeto. As levarei em meu coração mesmo após o fim do curso.

Agradeço também ao Programa de Educação Tutorial (PET) Direito UnB, representado pela professora tutora Érica Fernandes, que conduz o grupo com muita sabedoria, responsabilidade e comprometimento. Obrigada a todos os meus colegas petianos e ao projeto por me proporcionarem tanto aprendizado.

Agradeço, ainda, a quem contribuiu para a minha jornada profissional em meu estágio no Supremo Tribunal Federal e nos meus três anos no escritório. Muito obrigada por me ensinarem o funcionamento do Judiciário e os princípios da advocacia.

Não poderia deixar de citar os meus amigos de estágio do STF, Samuel Lisboa e Melissa Tosca, que compartilharam tardes de trabalho agradáveis e uma amizade incrível, que ultrapassou as barreiras do Supremo. Obrigada também pelo apoio durante a escrita deste trabalho.

Agradeço a quem me fez feliz nos últimos cinco anos: a Universidade de Brasília. Querida -como eu costumo chamar desde o início do curso-, você me ensinou a ter resiliência, força e resistência ao me mostrar um ambiente plural, democrático e encantador. Obrigada por cada debate proporcionado, por cada projeto de extensão e por cada pesquisa. Que você nunca deixe de ser uma universidade pública, gratuita e de qualidade.

Agradeço também a todos os professores com quem tive a honra e a felicidade de aprender, aqui representados pela Dra. Fernanda Lage, minha estimada orientadora de monografia. Obrigada por colaborar para o desenvolvimento de pensamento crítico, habilidades acadêmicas e anseios profissionais. Obrigada, ainda, por todo o apoio prestado desde o momento em que a convidei para me orientar durante a elaboração do trabalho final do curso. Agradeço pelo apoio, pelas videochamadas e por toda a bibliografia indicada.

(Rodriguez Dominguez Silvio)

Resumo

O presente trabalho se dedica a analisar a implementação do reconhecimento facial na aplicação da lei por agentes públicos e a propor medidas para o emprego de uma IA antidiscriminatória. Desse modo, o trabalho analisa a implementação da inteligência artificial no contexto jurídico, a exemplo dos sistemas utilizados nos tribunais brasileiros, bem como a existência de vieses algorítmicos e a discriminação humana reproduzida pelos sistemas de inteligência artificial. Ademais, analisa a existência de falhas e de reprodução do racismo no uso do reconhecimento facial. A partir daí, propõe medidas para uma regulação capaz de garantir transparência, antidiscriminação e a proteção dos direitos individuais. Dentre as medidas estão a diversificação de rostos inseridos nas máquinas de IA para treinarem a detecção de rostos com faces de diversas etnias e gêneros; a existência de um fórum para que as pessoas relatem as falhas e discriminações dos sistemas; a criação de um grupo de estudo para pesquisar constantemente regulações para se propor sistemas mais justos; a divulgação de relatórios de impacto sobre os vieses algorítmicos e a proteção dos dados dos usuários. a inserção de rostos distintos nos sistemas de IA, a criação de relatórios de impacto da igualdade, depoimentos de violações de direitos ou de falhas cometidas pela IA.

Palavras-chave: inteligência artificial; reconhecimento facial; antidiscriminação; vieses algorítmicos; inteligência artificial e direito.

Abstract

This paper aims to analyze the use of facial recognition technology in law enforcement by public agents and to propose avenues to promote algorithmic fairness. Thereby, the paper analyzes the use of artificial intelligence in the legal context like the systems used in Brazilian courts, as well as the existence of algorithmic biases and the human discrimination reproduced by artificial intelligence systems. Furthermore it analyzes the existence of failure and the racism's reproduction in the recognition facial's use. In this way, propose avenues to a regulation able to guarantee transparency, anti-discrimination and the protection of individual rights. Among the measures are the diversification of faces inserted in AI machines to detect faces of different ethnicities and genders, the creation of a forum for people to report on system failures and discriminations, the creation of a study group to constantly research regulations to propose fairer systems, a disclosure of impact report on algorithmic biases and the protection of user data, the insertion of distinct faces in the AI systems, the creation of equality impact report, depositions of rights violations or failures committed by the AI.

Keywords: artificial intelligence; facial recognition; anti-discrimination; algorithmic biases; artificial intelligence and law.

LISTA DE ABREVIATURAS E SIGLAS

ABIS	Solução Automatizada de Identificação Biométrica
AL	Alagoas
ANPD	Autoridade Nacional de Proteção de Dados
CICC	Centro Integrado de Comando e Controle
CNJ	Conselho Nacional de Justiça
Compas	<i>Correctional Offender Management Profiling for Alternative Sanctions</i>
CPP	Código de Processo Penal
DF	Distrito Federal
EUA	Estados Unidos da América
GO	Goiás
IA	Inteligência Artificial
LAPIN	Laboratório de Políticas Públicas e Internet
LGPD	Lei Geral de Proteção de Dados
NIST	National Institute of Standards and Technology
PE	Pernambuco
PF	Polícia Federal
PL	Projeto de Lei
PR	Paraná
RF	Reconhecimento Facial
RFB	Receita Federal do Brasil
RR	Roraima
RS	Rio Grande do Sul
SERPRO	Serviço Federal de Processamento de Dados
SP	São Paulo
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
UnB	Universidade de Brasília

SUMÁRIO

I. Introdução	11
I. Inteligência Artificial e Direito.....	13
a. O que é e como funciona a Inteligência Artificial	13
b. Aplicações da inteligência artificial no Direito.....	17
c. A discriminação algorítmica na inteligência artificial.....	24
II. IA e Reconhecimento facial	31
a. Como funciona o reconhecimento facial.....	31
b. As problemáticas do uso do reconhecimento facial	35
c. A legislação aplicável ao reconhecimento facial	40
III. A necessidade de parâmetros antidiscriminatórios	48
a. A perpetuação do racismo institucional pela IA	48
b. Uma luta contra o racismo e discriminações: quais medidas devem ser adotadas?	51
V. Conclusão	57
Referências bibliográficas	59

I. Introdução

A inteligência artificial (IA) tem sido fortemente implementada na esfera jurídica mundial, incluindo a brasileira. O Conselho Nacional de Justiça (CNJ) regulamentou sua utilização no Poder Judiciário por meio da Portaria CNJ nº 271/2020¹, medida extremamente necessária, haja vista que os tribunais brasileiros possuem 47 (quarenta e sete) iniciativas de inteligência artificial².

Os sistemas de inteligência artificial estão presentes em diversas medidas diretamente relacionadas ao direito, a exemplo do emprego do reconhecimento facial tecnológico pelo Estado. O reconhecimento facial vem sendo utilizado desde 2011 no Brasil, embora tenha se popularizado no ano de 2019, e está presente em vinte estados brasileiros³. Nos carnavais de Salvador e do Rio de Janeiro, por exemplo, foi utilizado para a verificação de contagem de quantas pessoas compareceram às festividades, mas também para efetuar prisões⁴.

A tecnologia é utilizada para diversas finalidades, como: educação, transporte, controle de fronteiras e segurança pública⁵. O reconhecimento facial, como qualquer outra tecnologia, apresenta falhas, todavia, o erro de uma inteligência artificial pode causar profundos prejuízos, a exemplo da prisão de uma cidadã por equívoco, no Rio de Janeiro⁶. Adicionalmente, a tecnologia empregada possui alta taxa de erro ao tentar identificar rostos não pertencentes a homens brancos.

Embora seja implementada em diversos países, há lacunas na regulamentação que interferem na proteção dos direitos individuais, na perpetuação do racismo

¹ BRASIL. CNJ, **Portaria nº 271, de 4 de dezembro de 2021**. Disponível em: <<https://atos.cnj.jus.br/atos/detalhar/3613>>. Acesso em 20 out. 2021.

² CNJ, **Pesquisa revela que 47 tribunais já investem em inteligência artificial**. Agência de notícias, publicada em 2 de março de 2021. Disponível em: <https://www.cnj.jus.br/pesquisa-revela-que-47-tribunais-ja-investem-em-inteligencia-artificial/>. Acesso em: 19 out. 2021.

³ Instituto Igarapé. **Reconhecimento Facial no Brasil**. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 25 out. 2021.

⁴ LISBOA, Vinicius. **Câmeras de reconhecimento facial levam a 4 prisões no carnaval do Rio**. Agência Brasil. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2019-03/cameras-de-reconhecimento-facial-levam-4-prisoas-no-carnaval-do-rio>. Acesso em: 28 out. 2021.

⁵ Instituto Igarapé. **Reconhecimento Facial no Brasil**. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 25 out. 2021.

⁶ **Sistema de Reconhecimento facial da PM do RJ falha e mulher é detida por engano**. G1, Rio de Janeiro, 11 de julho de 2020. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 24 out. 2021.

institucional, bem como na transparência de dados e modelos do reconhecimento facial empregado na aplicação da lei por agentes públicos⁷.

Ademais, o reconhecimento facial também reproduz discriminação de gênero, pois os sistemas reconhecem os rostos de homens com uma taxa de erro significativamente menor do que a taxa de falhas no reconhecimento facial de mulheres. Tratando-se de mulheres negras, o índice é ainda pior, pois a diferença entre a precisão do reconhecimento facial de homens brancos e mulheres negras da empresa é de 34,4% (trinta e quatro inteiros e quatro décimos percentuais)⁸, conforme será demonstrado no trabalho.

Destarte, urge a necessidade de avaliar os desdobramentos da utilização do reconhecimento facial sem o amplo debate acerca da utilização do sistema, pois os erros são capazes de perpetuar o racismo e as injustiças sociais.

O objetivo central deste estudo é apresentar medidas que os programas de inteligência artificial devem cumprir para que haja ao menos uma diminuição na propagação do racismo pelas máquinas, assim como um aumento de transparência com relação ao emprego da tecnologia.

Adicionalmente, possui como objetivos específicos: analisar o atual funcionamento da inteligência artificial na esfera jurídica, especialmente quanto ao reconhecimento facial; analisar a regulação do emprego do reconhecimento facial nos contextos mundial e brasileiro; propor medidas a serem adotadas para que a IA seja antidiscriminatória e para que haja transparência, além da proteção dos direitos individuais quando houver emprego de sistemas de reconhecimento facial.

Para tanto, foi realizada uma pesquisa científica qualitativa da revisão de literatura. Nesse sentido, houve um levantamento bibliográfico acerca do que é inteligência artificial, suas aplicações gerais e sua relação com o direito. O trabalho também destaca o conceito de reconhecimento facial, como ele está inserido no âmbito jurídico e quais são as principais falhas noticiadas. Adicionalmente, explica, a partir do racismo existente no emprego do reconhecimento de pessoas e do racismo estrutural, a necessidade de se propor medidas para que os sistemas implementados sejam antidiscriminatórios.

⁷ FRANCISCO, Pedro Augusto; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais**. Brasil: Instituto Igarapé e Data Privacy Brasil Research, 2020. Disponível em: <https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf>. Acesso em: 26 out. 2021.

⁸ **Gender Shades**, resultados. Disponível em: <http://gendershades.org/overview.html>. Acesso em 27 out. 2021.

I. Inteligência Artificial e Direito

a. O que é e como funciona a Inteligência Artificial

A idealização da Inteligência Artificial (IA) teve início na Antiguidade⁹ e se desenvolveu ao longo dos últimos anos, sendo que em 1812, um matemático inglês chamado Charles Babbage¹⁰ percebeu a possibilidade de máquinas realizarem cálculos. Posteriormente, o trabalho de Babbage teve destaque ao criar, juntamente com Ada Lovelace, um sistema de engenharia analítica que permitia a existência da primeira máquina para jogar o jogo da velha. Passados mais de duzentos anos, as máquinas foram cada vez mais aprimoradas, refletindo no intenso uso da tecnologia na atualidade.

É fato que a IA tem recebido muitos investimentos e atenção ultimamente e, por consequência, diversas preocupações acerca de sua implementação também surgiram. A IA pode ser aplicada com diferentes propósitos em cada ramo de estudo ou de trabalho para qual foi criada, o que gera desconfiança e apreensão na sua inserção como ferramenta nas carreiras profissionais.

O desconhecimento acerca de máquinas que recebem bases de dados e são capazes de prestar serviços realizados por humanos assusta, inicialmente, tendo em vista que a falta de informação acerca do assunto faz disseminar, no meio popular, que a inteligência artificial substituirá todo o trabalho humano.

Todavia, a apreensão acerca da implementação da IA é justificável em que pese fatores como o índice de desemprego no país que está desenvolvendo-a, por exemplo, o que afeta a preocupação dos cidadãos que têm medo de serem substituídos. Ademais, há experiências que demonstram maior eficiência na solução

⁹ MCCORDUCK, Pamela. **Machines who think: a personal inquiry into the history and prospects of artificial intelligence**. 2. ed. Massachusetts: A K Peters, 2004, *apud* COELHO, João Victor de Assis Brasil Ribeiro Coelho. **Aplicações e Implicações da Inteligência Artificial no Direito**. Monografia (Graduação em Direito), Faculdade de Direito, Universidade de Brasília. Brasília, p. 11. 2017. Disponível em: <https://bdm.unb.br/bitstream/10483/18844/1/2017_JoaoVictordeAssisBrasilRibeiroCoelho.pdf>. Acesso em: 18 out. 2021.

¹⁰ MCCORDUCK, Pamela. **Machines who think: a personal inquiry into the history and prospects of Artificial intelligence**. 2. ed. Massachusetts: A K Peters, 2004. p. 03, *apud* HOFFMANN, Alexandra Felipe. **Direito e Tecnologia: a utilização de inteligências artificiais no processo decisório**. Monografia, (Graduação em Direito), Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina (UFSC), Florianópolis, p. 31. 2018. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/192574/TCC_Final.pdf?sequence=1&isAllowed=y>. Acesso em: 18 out. 2021.

de casos pela inteligência artificial do que por humanos, inclusive por aqueles com vasta experiência acadêmica e profissional.

No ramo de direito, por exemplo, a IA pode ser utilizada para a elaboração de contratos de confiança ou até mesmo para a tomada de decisões judiciais. A assertividade e a rapidez com que a IA opera assustam os profissionais que a veem cada vez mais próxima de suas funções. Embora as preocupações existam, é importante destacar que a IA pode ser uma grande aliada no auxílio ao trabalho dos servidores dos tribunais, como será demonstrado a seguir. Ademais, gera celeridade contratual na análise de contratos de confidencialidade.

Não obstante a alta eficiência que a inteligência artificial apresenta em seus resultados, há fatores que devem ser considerados, como quais dados são inseridos nas máquinas e como eles interferem nas conclusões aferidas pela IA. Deve-se observar também a habilidade que a IA tem de aprender e de modificar sua própria estrutura sem que haja previsibilidade na execução, bem como no resultado que decorrerá¹¹. Nesse sentido, é essencial analisar, ainda, quais dados são inseridos nas máquinas, pois evidenciam os vieses daquele grupo que os inseriu.

A Inteligência Artificial possui várias definições, no entanto, de acordo com Stuart Russell e Peter Norvig¹², as que mais se destacam contém, geralmente, as noções de capacidade de processamento, raciocínio e comportamento, de modo que a IA está relacionada à capacidade que a máquina possui de pensar como o ser humano, aprendendo e analisando o próprio comportamento diante dos desafios que lhe são impostos. Nesse sentido, os autores agrupam as definições de IA em quatro sistemas, sendo eles: os que pensam como humanos; os que agem como humanos; os que pensam racionalmente; e os que agem racionalmente, sendo que os dois últimos sistemas envolvem um amplo conhecimento de engenharia, bem como de matemática para o entendimento¹³.

Destarte, conforme ensina Stuart Russell¹⁴, a IA pode ser entendida como um ramo que se propõe a apresentar métodos para que computadores atinjam os objetivos para os quais foram criados. Sendo assim, para servir de estudo de métodos,

¹¹ FRAZÃO, Ana de Oliveira. **Algoritmos e inteligência artificial. Direito Antitruste 4.0: fronteiras entre concorrência e inovação**. Juliana OLiveira Domingues et al, organizadores. São Paulo: Singular, 2019.

¹² RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. 3ª ed. Berkeley: Universidade da Califórnia, 2017.

¹³ Russel e Norvig (2013, p. 25), *apud*. LAGE, Fernanda. **Manual de Inteligência Artificial no Direito Brasileiro**, p. 26.1ª ed. Brasília: Juspodivm, 2020.

¹⁴ *Ibidem*, p. 27.

a inteligência artificial possui dentre suas tarefas a aprendizagem, o raciocínio, o planejamento, a percepção e a compreensão de linguagem robótica.

A inteligência artificial utiliza tecnologias de aprendizado para realizar o objetivo para o qual ela foi criada. Essas tecnologias são a *deep learning* (aprendizagem profunda) e a *machine learning* (aprendizado de máquina), juntamente com a análise de grande quantidade de dados, o *bigdata*, traduzido por Ana Frazão¹⁵ como “a enorme quantidade de dados disponíveis no mundo virtual que, com o devido processamento, pode ser transformada em informações economicamente úteis¹⁶”.

A tecnologia de aprendizado de máquina (*machine learning*), de acordo com Jyoti Dabass¹⁷, consiste na aprendizagem de redes neurais por meio de uma análise de enorme quantidade de dados estatísticos. Dabass defende, ainda, que a *machine learning* é adequada para problemas que envolvem detecção de vocalizações, astúcia e imagem em que as equações matemáticas falham em produzir um resultado final. Smola e Vishwanathan¹⁸ trazem a definição de *machine learning* como uma técnica que possibilita aos computadores internalizarem dados históricos e fazerem previsões, sendo alimentados por algoritmos que, por meio de métodos de análise de dados, são capazes de se autodesenvolverem.

O algoritmo, por sua vez, é um conjunto de diretrizes capaz de solucionar problemas semelhantes, a partir de uma sequência de regras¹⁹. Desse modo, é uma sequência de tarefas menores, realizada por uma máquina, que possibilita a realização de uma tarefa solicitada, sem a necessidade de que um humano realize o trabalho²⁰.

Há também a aprendizagem profunda (*deep learning*), que é definida por Dabass²¹ como uma variedade de aprendizado de aparelhos em que várias redes

¹⁵ FRAZÃO, Ana de Oliveira. **Algoritmos e inteligência artificial. Direito Antitruste 4.0: fronteiras entre concorrência e inovação**. Juliana OLiveira Domingues et al, organizadores. São Paulo: Singular, 2019.

¹⁶ Ibidem.

¹⁷ DABASS, Joti. **Scope of Artificial Intelligence in Law**. The Northcap University, 2018.

¹⁸ SMOLA, VISHWANATHAN, 2008, *apud*, Fernanda. Manual de Inteligência Artificial no Direito Brasileiro, p. 26. 1ª ed. Brasília: Juspodivm, 2020.

¹⁹ ELIAS, Paulo Sá. **Algoritmos, Inteligência Artificial e Direito**. Conjur. Disponível em: <https://www.conjur.com.br/dl/algoritmos-inteligencia-artificial.pdf>. Acesso em: 18 out. 2021.

²⁰ VALENTINI, Rômulo Soares. **Julgamento por computadores? As novas possibilidades da juscibernética no século XX e suas implicações para o futuro do direito e do trabalho dos juristas**. Tese de doutorado, Faculdade de Direito da Universidade Federal de Minas Gerais, Universidade Federal de Minas Gerais. Belo Horizonte, p. 43. 2017. Disponível em: <https://repositorio.ufmg.br/handle/1843/BUOS-B5DPSA>. Acesso em: 18 out. 2021.

²¹ DABASS, Joti. **Scope of Artificial Intelligence in Law**. The Northcap University, 2018.

neurais estão conectadas de modo a produzir um resultado ou a alcançar respostas mais profundas. Há, ainda, outra definição de *deep learning* bastante pertinente²²:

deep learning são esses algoritmos complexos construídos a partir de um empilhamento de diversas camadas de “neurônios”, alimentados por quantidades imensas de dados, que são capazes de reconhecer imagens e fala, processar a linguagem natural e aprender a realizar tarefas extremamente avançadas sem interferência humana.

Essas são as premissas básicas da inteligência artificial, haja vista que são as tecnologias que garantem o funcionamento da IA como ferramenta tão eficaz e, muitas vezes, assertiva. É oportuno destacar os conceitos supramencionados devido à utilização de tecnologias como ferramentas auxiliares no âmbito jurídico, como a de revisão de contratos²³ exposta no tópico de aplicações da IA no Direito.

Embora o uso da inteligência artificial seja uma realidade, haja vista a sua utilização nos tribunais²⁴, ainda não há uma legislação que regulamente seu desenvolvimento, bem como sua aplicação. No entanto, é possível que isso ocorra em breve, pois a Câmara dos Deputados aprovou²⁵, no dia 29 de setembro de 2021, o Projeto de Lei nº 21/20²⁶, que estabelece fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da inteligência artificial no Brasil, e dá outras providências.

Consoante dispõe o art. 2º do PL 21/20, o sistema de inteligência artificial é aquele que possui como base o processo computacional, o qual é capaz de processar dados e informações, bem como aprender a interagir com o ambiente externo, a partir de um conjunto de **objetivos definidos por seres humanos**. Desse modo, a própria definição de IA aprovada pela Câmara dos Deputados evidencia a interferência humana nos sistemas de inteligência artificial.

²² **Machine learning e Deeping learning: aprenda as diferenças**. Disponível em: <<https://www.salesforce.com/br/blog/2018/4/Machine-Learning-e-Deep-Learning-aprenda-as-diferencas.html>>. Acesso em: 18 out. 2021.

²³ Startup LawGeex. **IA VS. LAWYERS: THE ULTIMATE SHOWDOWN**. Disponível em: <<https://www.lawgeex.com/resources/whitepapers/aivslawyer/>> Acesso em: 30 de set de 2021.

²⁴ CNJ, **Pesquisa revela que 47 tribunais já investem em inteligência artificial**. Agência de notícias, publicada em 2 de março de 2021. Disponível em: <<https://www.cnj.jus.br/pesquisa-revela-que-47-tribunais-ja-investem-em-inteligencia-artificial/>>. Acesso em: 19 out. 2021.

²⁵ **Câmara aprova projeto que regulamenta uso da inteligência artificial**. Câmara dos Deputados, Brasília, 29 de set. de 2021. Disponível em: <<https://www.camara.leg.br/noticias/811702-camara-aprova-projeto-que-regulamenta-uso-da-inteligencia-artificial/>>. Acesso em 19 out. 2021.

²⁶ BRASIL. Câmara dos Deputados. **Projeto de Lei nº 21, de 03 de fevereiro de 2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da inteligência artificial no Brasil, e dá outras providências. Disponível em: <<https://www.camara.leg.br/propostas-legislativas/2236340>>, Acesso: 19 out. 2021.

Adicionalmente, o Projeto de Lei nº 21/20²⁷ estabelece que a inteligência artificial utiliza as seguintes técnicas, mas não se limita a elas: “sistemas de aprendizagem de máquina (machine learning), incluindo aprendizagem supervisionada, não supervisionada e por reforço; sistemas baseados em conhecimento ou em lógica; abordagens estatísticas”. Destaca, ainda, que a regulamentação não é aplicável àqueles processos de automação que não possuam a capacidade do sistema de aprender e perceber, ou seja, que não incluam *machine learning*.

Todavia, embora a inteligência artificial utilize um sistema que permite o processamento de dados pelas próprias máquinas, ainda há vieses algorítmicos, pois os dados fornecidos inicialmente às máquinas são disponibilizados por humanos, imputando seus posicionamentos aos sistemas²⁸. Destarte, a alimentação das máquinas por humanos traz, por conseguinte, discriminações e vieses algorítmicos, conforme será exposto a seguir.

b. Aplicações da inteligência artificial no Direito

A inteligência artificial possui diversas aplicações no âmbito jurídico brasileiro e internacional, a exemplo da análise de contratos²⁹, do proferimento de sentenças, da busca de jurisprudência avançada, do reconhecimento facial para prender pessoas, da análise preditiva de decisões, dentre outros.

No âmbito internacional, um estudo chamado *AI vs. Lawyers: The Ultimate Showdown*³⁰, desenvolvido pela *startup* LawGeex, trouxe mais destaque para o uso de inteligência artificial na esfera jurídica, especificamente sobre a análise de contratos de confidencialidade. O experimento consistiu em uma disputa de revisão de um contrato de confidencialidade e as aferições demonstram que a IA tem enorme potencial no ramo jurídico, haja visto seu desempenho excepcional. A competição

²⁷ O PL foi aprovado na Câmara dos Deputados e foi remetido ao Senado Federal.

²⁸ CENCI, Gabrielle Casagrande. **A fundamentação da decisão e a inteligência artificial no Direito Penal**. Conjur, 05 de jun. de 2021. Disponível em: <<https://www.conjur.com.br/2021-jun-05/cenci-fundamentacao-decisao-ia-direito-penal>>. Acesso em 19 out. 2021.

²⁹ LawGeex, *startup* especializada na revisão automática de contratos. Disponível em: <https://www.lawgeex.com/?utm_source=google&utm_medium=cpc&utm_campaign=Global_sch_brand&utm_adgroup=27388619163&device=c&placement&utm_term=lawgeex&gclid=CjwKCAjwslbpBRBN EiwAZF8-z8l3hvf_jSeNHWPzLnxXHx0TgvxRal2ebW8l6BRWZ00GKiw8Nt8kBoCLg4QAvD_BwE>. Acesso em: 19 out. 2021.

³⁰ Startup LawGeex. **IA VS. LAWYERS: THE ULTIMATE SHOWDOWN**. Disponível em: <<https://www.lawgeex.com/resources/whitepapers/aivslawyer/>> Acesso em: 19 out. 2021.

entre IA e humanos tinha o propósito de comparar o tempo gasto para a análise de questões legais nos contratos de confidencialidade, bem como o percentual de acertos e, para tanto, foi dado ao time de vinte advogados, especialistas em revisão de cláusulas contratuais, quatro horas para concluírem a revisão.

O resultado demonstrou que o tempo utilizado pelos advogados para analisarem os cinco contratos de confidencialidade foi de noventa e dois minutos, enquanto a máquina de IA solucionou a proposta em vinte e seis segundos, com 94% (noventa e quatro por cento) de acerto, garantindo um resultado impressionante.

O advogado que obteve a melhor performance, por sua vez, atingiu, também, 94% (noventa e quatro por cento). Todavia, a diferença de tempo necessário pelos humanos e pela IA é exorbitante, considerando que o advogado com o melhor resultado solucionou o problema com um tempo mais de duzentas vezes superior ao gasto pela inteligência artificial da startup.

A Inteligência Artificial da startup foi treinada com milhares de contratos de confidencialidade, utilizando as tecnologias de *deep learning* e *machine learning* para aprender e se aperfeiçoar executando a revisão dos contratos de confidencialidade. Os advogados selecionados para revisar os contratos possuem competência e experiência em revisão de contratos, embora o advogado com o menor desempenho tenha obtido um nível de acerto de apenas 64% (sessenta e quatro por cento).

A discrepância de tempo utilizado pela Inteligência Artificial e pelos advogados demonstra o alto nível de eficiência da IA em decorrência da capacidade de encontrar erros ao analisar trinta dispositivos legais dos contratos de confidencialidade em apenas vinte e seis segundos.

Sendo assim, é perceptível que a implementação de inteligência artificial, em algumas medidas, pode ser demasiadamente proveitosa para o âmbito jurídico, que deve ter o maior nível de eficiência possível em revisões de contrato devido à responsabilidade contratual.

Nesse sentido, o direito opera com a máxima atenção às leis e aos fatos. No âmbito de direito contratual, especialmente no que se refere aos contratos de confidencialidade, as partes recebem proteção da legislação para que não haja cláusulas abusivas em relação a nenhum dos pactuantes. A IA teve um desempenho que assegura a possibilidade de verificar as disposições legais rapidamente, acelerando o procedimento contratual. Desse modo, a efetivação de inteligência artificial na revisão de contratos é demasiadamente útil, célere e eficiente.

Embora a implementação da IA seja eficiente na hipótese de elaboração de contratos de confidencialidade, conforme demonstrado ainda, deve-se analisar a utilização da IA em cada caso, pois os vieses algorítmicos podem influenciar nas decisões, prejudicando indivíduos. Nos Estados Unidos da América (EUA), o sistema de pontos Compas (sigla em inglês para *Correctional Offender Management Profiling for Alternative Sanctions*) tem gerado discussão.

O Compas é um algoritmo criado pela empresa Northpointe, que atualmente se chama Equivant, para fazer avaliações sobre reincidentes, prestar informações para decisões, mitigar riscos do cometimento de crimes no futuro e orientar juízes dos tribunais dos Estados Unidos³¹. O sistema avalia os indivíduos por meio de um questionário, atribuindo pontos de um a dez para afirmar a probabilidade de cometer um crime novamente. A avaliação é utilizada, inclusive, para definir o tipo de sentença que o indivíduo terá, se poderá pagar fiança e, caso já esteja preso, se terá direito à liberdade condicional³².

Consoante dispõe Leonardo Vieira³³, o *software* analisa diversos critérios na avaliação, dentre eles: “história criminal, criminalidade da família, colegas, abuso de substâncias, residência/estabilidade, ambiente social, educação, trabalho, lazer/recreação, isolamento social, personalidade criminosa, raiva e atitudes criminosas”. Afirma, ainda, que o questionário utiliza 137 (cento e trinta e sete) perguntas para classificar os indivíduos e, embora cor não fosse uma variável evidente, raça e gênero estão presentes em outras variáveis, a exemplo do local de moradia, dos estudos e das redes sociais utilizadas. Adicionalmente, o sistema utiliza os juízes a decidirem com base na comparação com outros indivíduos, o que contraria o devido processo legal.

Não se sabe ao certo como a classificação é criada, pois o algoritmo é propriedade de uma empresa, que não revela o total funcionamento do sistema. Isso é um reflexo do problema de transparência na utilização da inteligência artificial no

³¹ VIEIRA, Leonardo Marques. **A problemática da inteligência artificial e dos vieses algorítmicos: caso Compas.** Brazilian Technology Symposium, 2019. Disponível em: <<https://www.lcv.fee.unicamp.br/images/BTSym-19/Papers/090.pdf>>. Acesso em: 23 out. 2021.

³² MAYBIN, Simon. **Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA.** BBC News, 31 de outubro de 2016. Disponível em: <https://www.bbc.com/portuguese/brasil-37677421>. Acesso em: 23 out. 2021.

³³ VIEIRA, Leonardo Marques. **A problemática da inteligência artificial e dos vieses algorítmicos: caso Compas.** Brazilian Technology Symposium, 2019. Disponível em: <<https://www.lcv.fee.unicamp.br/images/BTSym-19/Papers/090.pdf>>. Acesso em: 23 out. 2021.

âmbito jurídico, pois os dados são inseridos por programadores, de modo que os juízes e demais agentes do sistema de justiça pouco sabem a respeito dos algoritmos.

No contexto brasileiro, apesar de o projeto de lei que versa acerca da IA ainda estar em trâmite, o Conselho Nacional de Justiça (CNJ) regulamentou o uso de inteligência artificial no Poder Judiciário por meio da Portaria CNJ nº 271/2020³⁴, que criou a plataforma virtual Sinapses. A Portaria caracteriza como de inteligência artificial os projetos voltados a:

- I - criar soluções para automação dos processos judiciais e administrativos e de rotinas de trabalho da atividade judiciária;
- II - apresentar análise da massa de dados existentes no âmbito do Poder Judiciário; e
- III - prover soluções de apoio à decisão dos magistrados ou à elaboração de minutas de atos judiciais em geral.

Nesse sentido, a Portaria cria uma plataforma de inteligência artificial em parceria com o Tribunal de Justiça do Estado de Rondônia, para disponibilizar modelos de inteligência artificial para outros tribunais³⁵. Dentre os modelos disponíveis estão: o Movimento Inteligente, que possui o objetivo de sugerir o movimento a ser aplicado no despacho, como a gratuidade de justiça; a Triagem de Grande Massa, que possui a finalidade de classificar as petições conforme os temas pré-estabelecidos; a Prevenção, que é capaz de identificar a possível prevenção entre processos³⁶.

A portaria supramencionada surgiu a partir da preocupação com o preconceito presente nas máquinas de IA, uma vez que são alimentadas por seres humanos. Sendo assim, com o objetivo de detectar a tendência discriminatória da IA, o CNJ estabeleceu uma plataforma para conter os modelos desenvolvidos nos tribunais. Na hipótese de conter algum viés, os desenvolvedores do sistema deverão realizar as modificações necessárias para cessar a reprodução discriminatória ou o viés algorítmico³⁷.

³⁴ BRASIL. CNJ, Portaria nº 271, de 4 de dezembro de 2021. Disponível em: <<https://atos.cnj.jus.br/atos/detalhar/3613>>. Acesso em 20 out. 2021.

³⁵ APUD, Art. 5º A administração da plataforma de inteligência artificial do Poder Judiciário, abrangendo seus subsistemas e modelos, ficará sob a responsabilidade e coordenação do CNJ, contando com o apoio e suporte técnico da equipe do Tribunal de Justiça do Estado de Rondônia, conjuntamente com os tribunais que nela depositam seus modelos e que contribuem com seu aprimoramento.

§ 1º Todo o código fonte e suas atualizações ficarão centralizadas no repositório de código do CNJ, no sítio, não se admitindo cópias sem a devida autorização e nem versões derivadas.

§ 2º Os modelos liberados para produção estarão disponíveis para consulta no endereço, contendo a descrição, acurácia, caso de uso e URL da API para consumo.

³⁶ Inteligência Artificial: tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário Brasileiro. Disponível em: <https://ciapj.fgv.br/sites/ciapj.fgv.br/files/estudos_e_pesquisas/ia_1afase.pdf>.

³⁷ *Ibidem*, p. 21.

Nesse diapasão, é de suma importância a existência de medidas que combatam os vieses algorítmicos, dentre elas uma legislação eficiente que estabeleça os limites da utilização da inteligência artificial. O CNJ também publicou a Resolução CNJ nº 332, de 21 de agosto de 2020, que dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. A norma determina que o uso da IA no Judiciário visa a promoção do bem-estar aos jurisdicionados, bem como a prestação equitativa, devendo observar os direitos fundamentais previstos na Constituição e em tratados internacionais dos quais o Brasil seja signatário.

A Resolução do CNJ ressalta que as decisões judiciais que utilizam IA devem assegurar aos jurisdicionados a igualdade, a não discriminação, a pluralidade e a solidariedade, além de minimizar a marginalização dos indivíduos e os erros decorrentes de julgamentos preconceituosos. Adicionalmente, discorre acerca da transparência dos dados, o que é fundamental para compreender os possíveis vieses que a máquina pode reproduzir, determinando que o modelo de IA deverá ser homologado a fim de identificar os preconceitos e as generalizações constantes em seu funcionamento³⁸.

Adicionalmente, o CNJ determina que o desenvolvimento e a implementação dos serviços de inteligência deverão observar a diversidade de gênero, raça, etnia, cor, orientação sexual, pessoas com deficiência, geração e demais características individuais³⁹. As máquinas deverão observar a representatividade e respeitar os dados pessoais sensíveis dos indivíduos⁴⁰.

A regulamentação pelo CNJ é demasiadamente importante, haja vista que, atualmente, a IA está presente em mais da metade dos tribunais brasileiros, sendo 64 projetos em 47 tribunais⁴¹.

³⁸ BRASIL, Conselho Nacional de Justiça (CNJ). Resolução CNJ nº 332, de 21 de agosto de 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>.

³⁹ *Idem*, Art. 20. A composição de equipes para pesquisa, desenvolvimento e implantação das soluções computacionais que se utilizem de Inteligência Artificial será orientada pela busca da diversidade em seu mais amplo espectro, incluindo gênero, raça, etnia, cor, orientação sexual, pessoas com deficiência, geração e demais características individuais.

⁴⁰ *Idem*, Art. 6º. Quando o desenvolvimento e treinamento de modelos de Inteligência exigir a utilização de dados, as amostras devem ser representativas e observar as cautelas necessárias quanto aos dados pessoais sensíveis e ao segredo de justiça. Parágrafo único. Para fins desta Resolução, são dados pessoais sensíveis aqueles assim considerados pela Lei nº13.709/2018, e seus atos regulamentares.

⁴¹ CNJ, **Pesquisa revela que 47 tribunais já investem em inteligência artificial**. Agência de notícias, publicada em 2 de março de 2021. Disponível em: <https://www.cnj.jus.br/pesquisa-revela-que-47-tribunais-ja-investem-em-inteligencia-artificial/>. Acesso em

Conforme o estudo elaborado pelo Centro de Inovação, Administração e Pesquisa do Judiciário da Fundação Getúlio Vargas⁴², a utilização de IA no Judiciário permite a classificação de informações, as decisões interlocutórias, a triagem de processos, dentre outras medidas, todavia, deve-se observar os limites da implementação da automação nos tribunais, ainda que gere celeridade processual e baixo custo.

O estudo evidencia que o acesso aos dados inseridos fica restrito às empresas desenvolvedoras de *softwares*, de modo que os magistrados sabem pouco sobre o perfil de suas decisões, bem como sobre os elementos que compõem os atos jurisdicionais. Sendo assim, é necessário tornar os dados mais acessíveis não somente para os magistrados, mas também aos demais agentes envolvidos no sistema de justiça. Isso não significa que a IA não possa ser utilizada nos tribunais, mas somente que deve haver parâmetros para a implementação de sistemas de inteligência artificial antidiscriminatórios.

Conforme demonstrado pela pesquisa, dezoito estados brasileiros possuem iniciativas de inteligência artificial em seus tribunais, são eles: Roraima, Amazonas, Acre, Rondônia, Pará, Mato Grosso, Mato Grosso do Sul, Goiás, Distrito Federal, Paraná, Rio Grande do Sul, Santa Catarina, Rio de Janeiro, Espírito Santo, São Paulo, Bahia, Ceará e Pernambuco⁴³. Ademais, a maioria dos projetos foi desenvolvida nos anos de 2019 e 2020, sendo que 47 (quarenta e sete) foram elaborados pela própria equipe dos tribunais, três foram desenvolvidos em parcerias com universidades, treze receberam parceria com empresa privada e um foi desenvolvido por outro órgão⁴⁴.

O relatório detalha todos os projetos-pilotos, os que estão em desenvolvimento e os que se encontram em produção, inclusive no âmbito dos tribunais superiores. O Supremo Tribunal Federal (STF) implementou a inteligência artificial por meio do sistema denominado Victor, criado com o objetivo de reduzir a quantidade de processos que aguardam julgamentos no país⁴⁵.

⁴² **Inteligência Artificial: tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário Brasileiro.** Disponível em: <https://ciapj.fgv.br/sites/ciapj.fgv.br/files/estudos_e_pesquisas_ia_1afase.pdf>. Acesso em 19 de out. de 2021.

⁴³ *Ibidem*, p. 65.

⁴⁴ *Ibidem*, p. 69.

⁴⁵ ASSIS, Alexandre Alfaix de. **Inteligência artificial chegou ao STF com o robô Victor.** TCE-GO, Goiás, 27 de jun. de 2019. Disponível em: <<https://portal.tce.go.gov.br/-/inteligencia-artificial-chegou-ao-stf-com-victor>>.

O Victor foi desenvolvido pela equipe interna do STF e implementado no ano de 2019. O sistema de IA é capaz de identificar e separar as cinco principais peças do processo para análise da Corte, ou seja, o acórdão recorrido, o juízo de admissibilidade do recurso extraordinário, a petição de recurso extraordinário, a sentença e o agravo interno⁴⁶.

Adicionalmente, consegue executar e identificar os recursos que se encaixam em um dos temas mais recorrentes de repercussão geral. O resultado da inteligência artificial implementada no STF é impressionante, pois reduz significativamente o tempo demandado por um servidor para realizar a tarefa. Com o sistema Victor, uma tarefa realizada em 44 (quarenta e quatro) minutos é feita em cinco segundos⁴⁷.

No âmbito do Superior Tribunal de Justiça (STJ) há três sistemas de inteligência artificial em funcionamento e um em desenvolvimento, sendo que os mais relevantes são o Athos e o Sócrates, ambos implementados em 2019. O Athos foi treinado a partir da leitura de 329.000 (trezentas e vinte e nove mil) ementas de acórdãos proferidos pelo tribunal entre 2015 e 2017 e separou as petições de mais de dois milhões de processos. O sistema é capaz de agrupar similares, de buscar por similares e de monitorar os grupos, além de realizar pesquisa textual. Nesse sentido, o Athos está apto a agrupar processos que possuem a mesma controvérsia jurídica para fixar teses vinculantes. Adicionalmente, identifica matérias de notória relevância, bem como distinções ou superações de precedentes.

O sistema possui diversos resultados, dentre eles: redução de processos recebidos no tribunal; uniformização da jurisprudência a partir da utilização dos precedentes qualificados; criação de mais de 51 (cinquenta e uma) controvérsias, que são um “conjunto de processos com sugestão de afetação ao rito dos repetitivos”; identificação de matérias relevantes. Sendo assim, é evidente a importância da utilização do sistema Athos na identificação e no agrupamento de processos no âmbito do STJ.

O sistema Sócrates, também em funcionamento no STJ, utiliza o mesmo motor de inteligência artificial constante no Athos e, assim como o outro sistema, monitora e agrupa processos. Ele é capaz de identificar precedentes e de localizar processos

⁴⁶ **Inteligência Artificial: tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário Brasileiro.** Disponível em: <https://ciapj.fgv.br/sites/ciapj.fgv.br/files/estudos_e_pesquisas/ia_1afase.pdf>. Acesso em 19 de out. de 2021.

⁴⁷ *Ibidem*.

semelhantes em um campo de cem mil processos, comparando-os em menos de quinze minutos. O Sócrates serve de apoio para a análise de litígios e auxilia na seleção de representativos de controvérsias pelos gabinetes dos ministros. Quando recebe um caso, o Sócrates é qualificado para compará-lo com os demais processos que versam sobre a temática dentro de uma amostra de dois milhões de processos e oito milhões de peças processuais, em 24 (vinte e quatro) segundos. Adicionalmente, monitora automaticamente mais de mil processos que são encaminhados ao tribunal diariamente.

Destarte, é notório que a utilização da inteligência artificial no STJ promove celeridade na análise dos processos, haja vista o agrupamento automático dos litígios similares, bem como a identificação de controvérsias. No entanto, é necessário atentar-se à transparência dos sistemas de IA a fim de detectar a reprodução de comportamentos discriminatórios por meio do viés algorítmico.

c. A discriminação algorítmica na inteligência artificial

Os algoritmos são regras para a solução de problemas, execução de tarefas ou, até mesmo, tomada de decisões e existem há bastante tempo, no entanto, apenas no século XX ganharem destaque como *sequências finitas de ações executáveis para a solução de um problema específico*, consoante dispõe Ana Frazão⁴⁸.

Esses algoritmos são utilizados na técnica de aprendizagem automática de *machine learning*, pois alimentam as máquinas, as quais internalizam dados históricos e fazem previsões, de modo que é possível que os algoritmos se autodesenvolvam a partir da análise de dados⁴⁹.

Nesse sentido, os mecanismos de inteligência artificial possuem diversos modelos, que são criados por programadores e, geralmente, representam complexidades do mundo real. Na criação dos modelos, os programadores selecionam quais informações são importantes o suficiente para serem incluídas,

⁴⁸ FRAZÃO, Ana. **Discriminação algorítmica: compreendendo o que são os julgamentos algorítmicos e o seu alcance na atualidade**. Conjur, 26 de jun. de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-16062021>. Acesso em:

⁴⁹ SMOLA, VISHWANATHAN, 2008, *apud*, Fernanda. Manual de Inteligência Artificial no Direito Brasileiro, p. 26. 1ª ed. Brasília: Juspodivm, 2020.

restando alguns pontos cegos, pois nem tudo é inserido na IA⁵⁰. Conforme os ensinamentos de Cathy O'neil⁵¹, uma máquina com muitos pontos cegos reflete o posicionamento de seu criador, o que nem sempre é problemático, a exemplo de quando o Google Maps omite os prédios das ruas ao direcionar um indivíduo. Todavia, os casos em que a precisão é sacrificada em detrimento da eficiência são preocupantes.

Cathy O'neil cita como exemplo de quando a precisão altera a eficiência da máquina o modelo aplicado nas escolas de Washington, que avalia os professores por meio das notas dos alunos nas provas, sem considerar especificidades, como o modo como lidam com os alunos, como gerem as aulas ou como ajudam os alunos na resolução de conflitos pessoais e familiares. Observa-se que o modelo considera apenas a eficiência, sacrificando diferentes percepções⁵².

Após a elaboração do modelo pelo programador, a máquina é alimentada com dados que possibilitam a realização do aprendizado de máquina, ocasião em que a IA analisa as informações fornecidas conforme as instruções recebidas pelos algoritmos, a fim de encontrar padrões e, por conseguinte, prever resultados⁵³. Nesse diapasão, as informações fornecidas são muito importantes, pois impactam nos resultados da IA, confirmando padrões discriminatórios advindos dos dados inseridos nas máquinas⁵⁴.

Destarte, a inteligência artificial é alimentada por dados tendenciosos que possuem discriminações, uma vez que são inseridos por humanos. Sendo assim, a IA correlaciona os conceitos e cumpre seu objetivo de encontrar uma solução para um problema por meio de atividades, no entanto, não os compreende e replica padrões discriminatórios⁵⁵.

⁵⁰ Nunes, Dierle; Marques, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. *Revista de Processo*, v. 285, pp. 421-447, 2018. Disponível em: <https://bit.ly/3jsJjwH>. Acesso em: 22 out. 2021.

⁵¹ O'NEIL, Cathy. *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York: Crown Publishers, 2016. p. 27, *apud* Nunes, Dierle; Marques, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. *Revista de Processo*, v. 285, pp. 421-447, 2018. Disponível em: <https://bit.ly/3jsJjwH>. Acesso em:

⁵² *Ibidem*.

⁵³ Nunes, Dierle; Marques, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. *Revista de Processo*, v. 285, pp. 421-447, 2018. Disponível em: <https://bit.ly/3jsJjwH>. Acesso em: 22 out. 2021.

⁵⁴ *Ibidem*.

⁵⁵ CENCI, Gabrielle Casagrande. **A fundamentação da decisão e a inteligência artificial no Direito Penal**. *Conjur*, 05 de jun. de 2021. Disponível em: <<https://www.conjur.com.br/2021-jun-05/cenci-fundamentacao-decisao-ia-direito-penal>>. Acesso em 22 out. 2021.

Esses padrões discriminatórios podem ser chamados de vieses algorítmicos e se referem aos resultados que contenham erro ou tratamento desigual entre dois grupos, sem justificativa, conforme definição da Comissão Australiana de Direitos Humanos. De acordo com a Comissão, os erros podem ser causados por problemas dos sistemas da inteligência artificial ou por aumentar desigualdades injustificadamente, apenas pelas circunstâncias em que são utilizados. Isso acarreta privilégio para determinado grupo que a IA foi criada para favorecer⁵⁶.

A inteligência artificial replica discriminação de gênero, raça e de classe, conforme será exposto a seguir, e possui como resultados a preferência de determinado grupo em detrimento de outro, causando danos. Os sistemas de recomendação funcionam por meio de algoritmos e possuem relevante papel na vida cotidiana, de modo que seu funcionamento deve ser justo. No entanto, um estudo inglês⁵⁷ demonstrou que há discriminação de gênero dos sistemas de recomendação de *streaming* de música. Consoante os resultados demonstram, somente 25% dos artistas indicados são mulheres, evidenciando que o algoritmo favorece os homens na escolha aleatória de música. Cumpre destacar, ainda, que os sistemas são alimentados por seres humanos.

No Brasil, a discriminação de gênero humana refletida nos sistemas de recomendação de músicas também pode ser observada, considerando que as mulheres representavam 6% da lista de 50 músicas mais tocadas no Youtube. Já no Spotify, o índice é de 12%, mas cumpre destacar que a população feminina no Brasil é de 51%⁵⁸.

A discriminação de gênero também foi apontada em um infográfico elaborado pela *Australian Human Rights Commission*⁵⁹ (Comissão Australiana de Direitos Humanos) que evidencia a existência de viés histórico nos sistemas de inteligência

⁵⁶ **Addressing the problem of algorithmic bias.** Technical Paper. Australian Human Rights Commission, 2020. Disponível em: <https://humanrights.gov.au/our-work/rights-and-freedoms/publications/using-artificial-intelligence-make-decisions-addressing>. Acesso em: 24 out. 2021.

⁵⁷ FERRARO, Andres; SERRA Xavier; BAUER Christine. **Break the loop: gender imbalance in music recommenders.** CHIIR. Publicado em 14 de março de 2019, Canberra, Austrália. Disponível em: <<https://dl.acm.org/doi/10.1145/3406522.3446033>>. Acesso em: 24 out. 2021.

⁵⁸ RAVACHE, Guilherme. **Algoritmo do Spotify privilegia músicos homens, diz pesquisa.** Uol, 06 de maio de 2021. Disponível em: <https://www.uol.com.br/splash/colunas/guilherme-ravache/2021/05/06/algoritmo-do-spotify-privilegia-musicos-homens-diz-pesquisa.htm?cmpid=copiaecola>. Acesso em: 24 out. 2021.

⁵⁹ **INFOGRAPHIC: historical bias in AI systems.** Australian Human Rights Commission. Disponível em: <https://humanrights.gov.au/about/news/media-releases/infographic-historical-bias-ai-systems>. Acesso em: 24 out. 2021.

artificial. Os sistemas são alimentados por dados e, a partir deles, fazem suposições que refletem no mundo real. Caso esses dados privilegiem indivíduos de determinado grupo em relação a outro, o sistema de IA também privilegiará esse grupo quando selecionar pessoas. O viés histórico ocorre quando os dados inseridos na IA em determinado momento não refletem mais a realidade passado determinado tempo.

Nesse sentido, historicamente há uma disparidade salarial entre homens e mulheres, devido à construção da sociedade, de modo que devido ao arranjo estrutural imposto, as mulheres têm menos probabilidade de ganhar o mesmo salário que os homens ao exercer a mesma função. Na hipótese de a renda ser um fator determinante para a adequação de um indivíduo como cliente de algum serviço e se a tarefa da IA for detectar possíveis clientes, ela privilegiará os homens, pois foi alimentada com dados que informam que homens recebem salários maiores⁶⁰.

Embora a disparidade salarial de gênero ainda exista, tem diminuído nos últimos. Conforme demonstrado pela Comissão Australiana de Direitos Humanos, o índice de diferença salarial entre homens e mulheres era de 24,6% em 2014, passando para 20,8% em 2019⁶¹. Desse modo, caso utilize os dados inseridos em 2014, o sistema de inteligência artificial rejeitará mulheres como potenciais clientes em razão da desatualização dos dados, evidenciando a existência do viés histórico.

O estudo também demonstrou que a utilização unicamente de dados recentes é incapaz de evidenciar um resultado justo, porque o treinamento de dados se torna insuficiente. Sendo assim, utilizar apenas dados recentes também pode ser problemático. Diante do impasse, retiraram o gênero, mas ainda assim havia questões que possibilitavam classificar os indivíduos como homem ou mulher, a exemplo do histórico de navegação. Há, desse modo, a classificação das pessoas com base em sítios mais visitados por mulheres, presumindo-se que o indivíduo que navegou por aquele sítio também é uma mulher⁶².

À vista disso, percebe-se que retirar o gênero não é suficiente para atenuar o viés algorítmico. Como proposta para a diminuição, o estudo sugere a seguinte

⁶⁰ **INFOGRAPHIC: historical bias in AI systems.** Australian Human Rights Commission. Disponível em: <https://humanrights.gov.au/about/news/media-releases/infographic-historical-bias-ai-systems>. Acesso em: 24 out. 2021.

⁶¹ *Ibidem.*

⁶² *Ibidem.*

medida: “coletar dados mais apropriados, ajustar os critérios de seleção para o grupo desfavorecido e treinar o sistema de IA para incorporar justiça em suas decisões”⁶³.

Em suas considerações acerca da discriminação algorítmica, Ana Frazão aponta que a controvérsia atual relaciona-se com a utilização de algoritmos complexos para a solução de problemas e de tarefas que incluem análises qualitativas e subjetivas, a exemplo do ranqueamento de pessoas. Ressalta que a utilização dos algoritmos para julgar e prever comportamentos das pessoas no que diz respeito às suas preferências, às suas inclinações, aos seus perfis não é inocente, pois são implementadas com objetivos bastante específicos⁶⁴.

Frazão afirma que o mercado utiliza-se dessa ferramenta para conferir tratamento discriminatório, como a diferenciação de consumidores para verificar quem pode adquirir um determinado produto por um valor mais elevado, ou para negar acesso a algum serviço⁶⁵. Como exemplo de negação a um serviço, um algoritmo utilizado por provedores de saúde nos Estados Unidos para prever a necessidade de cuidados médicos extras favoreceu pacientes brancos. A raça não foi utilizada como um critério, no entanto, em razão da utilização de despesas médicas anteriores como um parâmetro para a definição de quais pacientes precisavam de mais atenção médica, pessoas brancas foram novamente privilegiadas. Isso ocorreu porque, historicamente, negros tiveram acesso a atendimentos médicos de custos mais baixos, o que fez com que o algoritmo atribuísse mais pontos aos pacientes brancos menos doentes do que os negros⁶⁶.

Como resultado, a discriminação algorítmica reduziu a ajuda extra que os pacientes negros igualmente ou mais doentes deveriam receber. Diante da descoberta do viés algorítmico, os responsáveis pelo *Optum*, o algoritmo utilizado, trabalham para corrigir o problema, tendo reduzido a disparidade em mais de 80% (oitenta por cento) ao criar uma versão capaz de prever os custos futuros que os pacientes podem ter, bem como o número de vezes que podem ter uma doença crônica no anos seguinte.

⁶³ *Ibidem*.

⁶⁴ FRAZÃO, Ana. **Discriminação algorítmica: compreendendo o que são os julgamentos algorítmicos e o seu alcance na atualidade**. Jota, 16 de jun. de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-16062021>. Acesso em: 24 out. 2021.

⁶⁵ *Ibidem*.

⁶⁶ JEE, Charlotte. **A biased medical algorithm favored White people for health-care programs**. MIT Technology Review. Disponível em: <https://www.technologyreview.com/2019/10/25/132184/a-biased-medical-algorithm-favored-white-people-for-healthcare-programs/>. Acesso em: 24 out. 2021.

A respeito da discriminação racial pelos algoritmos, cumpre destacar novamente o sistema de pontos Compas (sigla em inglês para *Correctional Offender Management Profiling for Alternative Sanctions*). O sistema algorítmico atribuiu pontuação a dois indivíduos: Borden, que foi preso por roubo e furto de itens avaliados em oitenta dólares e possuía apenas um registro por contravenções quando era melhor de idade; e Prater, que foi preso por furto de itens avaliados em oitenta e seis dólares, e possuía registro por assalto à mão armada. Ao conferir uma pontuação a cada um, o Compas determinou que Borden, um homem negro, era mais propício a cometer um crime novamente, ainda que só tivesse registro de contravenções, enquanto Prater, um homem branco que já havia realizado assalto à mão armada, foi classificado como de baixo risco. Dois anos após a classificação, Bardon não havia cometido um novo crime, enquanto Prater cumpria sentença de prisão por invasão e roubo de milhares de dólares eletrônicos⁶⁷.

O caso evidencia, novamente, a existência de racismo algorítmico na classificação de indivíduos pela inteligência artificial, que recebeu dados inseridos por humanos e foi treinada a partir deles. Ademais, os sistemas de inteligência artificial utilizados no reconhecimento facial também reproduzem racismo, conforme demonstra Tarcizio Silva em uma linha do tempo construída para evidenciar a existência do racismo algorítmico. De acordo com Silva, as câmeras da Nikon não entendiam os rostos asiáticos, pois acreditavam que alguém havia piscado na foto, em 2010⁶⁸. Recentemente, em 2021, a inteligência artificial utilizada pela rede social *Facebook* rotulou um homem negro como primata ao questionar se o usuário gostaria de continuar acompanhando conteúdos sobre primatas a partir de um vídeo que continha um homem negro⁶⁹. Ou seja, passados onze anos, os sistemas de inteligência artificial utilizados no reconhecimento facial continuam reproduzindo racismo. Ademais, a situação supramencionada ratifica a inexistência de

⁶⁷ ANGWIN, Julia. LARSON, Jeff. MATTU Surya. KIRCHNER, Lauren. **Machine Bias: there's software used across the country to predict future criminals.** And it's biased against blacks. ProPublica, 23 de maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 24 out. 2021.

⁶⁸ SILVA, Tarcizio. **Linha do Tempo do Racismo Algorítmico.** Blog do Tarcizio Silva, 2020. Disponível em: <http://https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo>. Acesso em: 24 out. 2021.

⁶⁹ **Inteligência Artificial do Facebook rotulou homem negro como primata.** Folha de S. Paulo, São Paulo, 4 de setembro de 2021. Disponível em: <https://www1.folha.uol.com.br/mercado/2021/09/inteligencia-artificial-do-facebook-rotulou-homem-negro-como-primata.shtml>. Acesso em: 24 out. 2021.

imparcialidade nas tarefas realizadas pela inteligência artificial, o que demonstra a necessidade de se pensar em parâmetros para uma IA antidiscriminatória.

II. IA e Reconhecimento facial

a. Como funciona o reconhecimento facial

O reconhecimento facial (RF) é capaz de identificar ou verificar a identidade de uma pessoa pela imagem de seu rosto. A partir da coleta de imagem de um rosto por uma câmera, o sistema de inteligência artificial verifica as suas características, tais como a distância entre os olhos, largura do queixo e o comprimento da boca. Após a coleta dessas informações, um *software* analisa o material, chegando a uma assinatura facial, que o Laboratório de Políticas Públicas e Internet (Lapin) define como: “a chave para identificação dessa pessoa”. A assinatura facial do indivíduo é comparada com diversas outras assinaturas faciais que foram inseridas no sistema de IA e, caso a assinatura coletada pela imagem naquele momento seja compatível com alguma da base de dados, verifica-se a identidade do sujeito de modo automatizado⁷⁰.

A assinatura facial é classificada como um dado biométrico porque reúne características faciais específicas de cada indivíduo, o que evidencia o tratamento de dados sensíveis pelo reconhecimento facial.

O não-reconhecimento de uma assinatura facial ou a sua atribuição equivocadamente a outra pessoa geram problemas de discriminação no uso da IA⁷¹.

Importante ressaltar que o reconhecimento facial localiza um rosto em uma imagem a partir de um treinamento em que recebe várias fotos de rostos para aprender a fazer a detecção. Após receber as imagens, aprende a diferenciar objetos de rostos e, isso combinado com um algoritmo de análise permite a existência do reconhecimento facial. Caso os sistemas sejam alimentadas sem uma diversidade de rostos, terá dificuldade de ler rostos de pessoas não-brancas e de mulheres, propagando discriminações⁷².

No Brasil, as tecnologias de reconhecimento facial utilizam a inteligência artificial para detectar rostos e são utilizadas desde 2011, tendo sido reportados 47

⁷⁰ *Ibidem*.

⁷¹ 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. Disponível em: <https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/>. Acesso em: 25 out. 2021.

⁷² KLOSOWSKI, Thorin. **Facial Recognition Is Everywhere. Here's what we can do about it**. Wirecutter, 15 de julho de 2020. Disponível em: <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>. Acesso em: 24 out. 2021.

(quarenta e sete) casos de implementações pelo setor público até o ano de 2019. O RF tem sido utilizado principalmente em quatro segmentos, são eles: transporte, segurança pública, educação; e controle de fronteiras⁷³.

No transporte, o RF é utilizado para combater fraude no uso gratuito de transporte público por meio de cartão conhecido como passe livre e existe desde 2011, quando foi implementado em Ilhéus, na Bahia. Em 2016, o município de Jaboatão, em Pernambuco, passou a utilizar o reconhecimento facial para controlar a evasão escolar⁷⁴. O sistema também tem sido utilizado na identificação de pessoas desaparecidas ou foragidas, bem como no acesso a benefícios sociais⁷⁵.

De acordo com estudo elaborado pelo Lapin em 2021, o reconhecimento facial para a finalidade de segurança pública tem sido utilizado nos seguintes estados: Bahia; Ceará; Paraíba; Distrito Federal; São Paulo; Rio de Janeiro; Paraná; Santa Catarina. Adicionalmente, nos municípios de Campinas (SP), Boa Vista (RR), Curitiba (PR), Porto Alegre (RS).

Para a finalidade de escolas e programas sociais, o reconhecimento facial é utilizado nos estados de Alagoas e de Tocantins, bem como, nos municípios de Pilar (AL), Recife (PE), Anápolis (GO)⁷⁶.

O estudo também demonstra que o RF é utilizado pelo segmento de mobilidade urbana no município de São Paulo (SP) e no Distrito Federal (DF). Adicionalmente, a Receita Federal utiliza o reconhecimento facial em 14 (catorze) aeroportos⁷⁷ para “identificar inequivocamente os indivíduos de potencial interesse e encaminhá-los para fiscalização minuciosa”.

⁷³ Instituto Igarapé. **Reconhecimento Facial no Brasil**. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 25 out. 2021.

⁷⁴ *Ibidem*.

⁷⁵ 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. Disponível em: <https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/>. Acesso em: 25 out. 2021.

⁷⁶ *Ibidem*.

⁷⁷ O sistema é utilizado nos seguintes aeroportos: Tancredo Neves (Belo Horizonte – MG); Juscelino Kubitschek (Brasília – DF); Viracopos (Campinas - SP); Afonso Pena (Curitiba – PR); Hercílio Luz (Florianópolis – SC); Pinto Martins (Fortaleza - CE); Eduardo Gomes (Manaus – AM); Augusto Severo (Natal – RN); Salgado Filho (Porto Alegre – RS); Gilberto Freyre/ Guararapes (Recife - PE); Antônio Carlos Jobim/ Galeão (Rio de Janeiro – RJ); Luís Eduardo Magalhães (Salvador – BA); Governador André Franco Montoro/Cumbica (Guarulhos – SP); Cataratas (Foz do Iguaçu – PR). Disponível em: https://br.nec.com/pt_BR/press/PR/20160409060302_11186.html.

Para o fim de validação de identidade, o Brasil utiliza o Serviço Federal de Processamento de Dados (SERPRO), uma empresa de tecnologia da informação vinculada ao Ministério da Economia⁷⁸.

No Brasil, conforme mencionado acima, o reconhecimento facial tem sido utilizado pela Receita Federal do Brasil (RFB) em catorze aeroportos com objetivo de identificar viajantes com risco aduaneiro pré-identificado. Desse modo, o sistema de gerenciamento de riscos seleciona previamente os indivíduos e os servidores dos órgãos os identificam nos aeroportos⁷⁹. De acordo com o sítio da empresa que fornece a tecnologia de reconhecimento facial para a RFB, a biometria facial é realizada “de forma automática e não invasiva, por meio de fotos, imagens de sistemas de CFTV, vídeos gravados e webcams”⁸⁰.

A leitura de rostos funciona com a integração de diversos sistemas, do seguinte modo:

1. Assim que o embarque de um voo internacional é finalizado, as informações sobre os passageiros e tripulantes são enviadas pelas empresas aéreas a um banco de dados internacional.
2. Caso o voo tenha destino a um aeroporto brasileiro, esse banco de dados envia as informações para o Sisbraip, um sistema desenvolvido pelo Serpro e operado pela Polícia Federal.
3. O Sisbraip processa as informações e envia aquelas que são de interesse do e-DBV, também desenvolvido pelo Serpro e operado pela Receita Federal. Entre elas estão, por exemplo, dados biográficos e conteúdo de bagagens.
4. De posse dessas informações, o e-DBV pode realizar, mediante o sistema de câmeras da sala de desembarque, o reconhecimento facial dos passageiros, traçar perfis biográficos de interesse e definir dados para que os agentes alfandegários tomem decisões⁸¹.

Destarte, a utilização do reconhecimento facial para a identificação de viajantes com risco aduaneiro previamente identificado integra a base de dados da Polícia Federal e da Receita Federal, por meio de um algoritmo. Ademais, utiliza dados enviados por empresas privadas para guiar a tomada de decisões dos agentes alfandegários, o que pode ser problemático diante da ausência de informações acerca

⁷⁸ 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. Disponível em: <https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/>. Acesso em: 25 out. 2021.

⁷⁹ Ibidem.

⁸⁰ **Receita Federal utilizará tecnologia de identificação facial da NEC em 14 aeroportos internacionais do País**. NEC. Disponível em: https://br.nec.com/pt_BR/press/PR/20160409060302_11186.html. Acesso em: 25 out. 2021.

⁸¹ FREIRE, Victor. **Reconhecimento facial intensifica segurança nos aeroportos**. Serpro. Disponível em: http://intra.serpro.gov.br/tema/noticias-tema/reconhecimento-facial-intensifica-seguranca-nos-aeroportos/nitf_galleria. Acesso em: 24 out. 2021.

de quais dados são utilizados e quando as pessoas expressaram consentimento para isso.

Embora ainda não exista legislação nacional específica de regulação do reconhecimento facial, a Polícia Federal intensificará seu uso com a compra do Abis (Solução Automatizada de Identificação Biométrica). O programa integra registros de provenientes de reconhecimento facial e impressões digitais para identificar pessoas. Segundo a PF, o programa possibilitará a unificação de dados das secretarias de segurança pública estaduais, que, conforme demonstrado anteriormente, já utiliza o reconhecimento facial no auxílio de prisões⁸².

No âmbito mundial, o reconhecimento facial tem sido utilizado para diversas finalidades, inclusive, para solucionar problemas. Em 2020, uma tecnologia de reconhecimento facial contribuiu para uma família localizar um filho que havia sido sequestrado e vendido em 1988. A polícia investigou o caso por 32 (trinta e dois) anos e conseguiu solucionar o caso com a ajuda de um sistema de reconhecimento facial. A polícia utilizou o RF para analisar uma foto da criança, projetando como estaria na fase adulta, e comparou a imagem com as fotografias da base de dados. Após diversas comparações, a polícia localizou um homem que se parecia com a imagem projetada a partir da fotografia infantil, confirmando por meio de exame de DNA que se tratava da criança sequestrada na década de 1980⁸³.

O reconhecimento facial também foi utilizado na resolução de uma pista do jogo Perplex City, criado em 2005, quinze anos após ter acabado. O jogo possuía cartões que permitiram o progresso a partir da descoberta dos enigmas dos cartões e tinha como prêmio o valor de cem mil euros. O jogo foi resolvido em 2007, no entanto, o último cartão, que continha a foto de um homem japonês com a frase “encontrem-me”, nunca havia sido desvendado⁸⁴.

Em 2020, Luca Sager utilizou a ferramenta PimEyes, na Alemanha, para desvendar a pista do último cartão do jogo. O enigma não foi resolvido por meio do Google porque este lê os *pixels* da imagem, sem distinguir os traços dos rostos,

⁸² **PF compra sistema que cruzará dados biométricos de 50 milhões de brasileiros.** Folha de S. Paulo, São Paulo, 7 de julho de 2021. Disponível em: <https://www1.folha.uol.com.br/tec/2021/07/pf-compra-sistema-que-cruzara-dados-biometricos-de-50-milhoes-de-brasileiros.shtml>.

⁸³ **Reconhecimento facial ajuda criança sequestrada a encontrar família após 32 anos.** CNN Brasil, 21 de maio de 2021. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/reconhecimento-facial-ajuda-crianca-sequestrada-a-encontrar-familia-apos-32-anos/>. Acesso em: 26 out. 2021.

⁸⁴ **Reconhecimento facial resolve em segundos enigma que durava 15 anos.** Folha de S. Paulo, São Paulo, 23 de junho de 2021. Disponível em: <https://f5.folha.uol.com.br/voceviu/2021/06/pimeyes-resolve-em-segundos-um-enigma-que-durava-15-anos.shtml>. Acesso em: 26 out. 2021.

segundo Sager. Ele informou que carregou a foto de Satoshi, o jovem japonês, no PimEyes e recebeu uma foto com diversas pessoas em uma festa de uma empresa. Posteriormente, incluiu a foto localizada no Reddit e encontrou as fotos de Satoshi na empresa.

Destarte, é evidente que a utilização do reconhecimento facial possui aspectos positivos, especialmente no que diz respeito à localização de pessoas sequestradas, no entanto tem sido utilizado em diversos locais sem necessidade e sem o devido tratamento de dados. Nesse sentido, a Clearview, prestadora de serviço tecnológico de reconhecimento facial para a polícia, foi processada por uso indevido de bilhões de imagens extraídas da internet sem permissão⁸⁵.

Adicionalmente, há a reprodução de práticas discriminatórias e racistas pela tecnologia de reconhecimento facial ao identificar pessoas como pertencentes a classes perigosas, intensificando a violência na periferia⁸⁶. Diante da utilização do reconhecimento facial pelo Estado em diversas áreas, surge o questionamento de quais são os desdobramentos de seu uso, qual é a legislação aplicável e se há transparência no emprego dos sistemas de RF.

b. As problemáticas do uso do reconhecimento facial

A inteligência artificial utiliza técnicas de aprendizado para concluir a tarefa para a qual foi criada e, por receber dados inseridos pelos programadores, contém vieses dos humanos e os reproduz. Conforme demonstrado acima, o reconhecimento facial é utilizado para diversas finalidades, o que ressalta a necessidade de discutir a discriminação reproduzida pela inteligência artificial.

O reconhecimento facial também possui viés algorítmico que resulta em discriminação e racismo. O projeto Gender Shades⁸⁷, criado por Joy Buolamwini e Timnit Gebru, fez um experimento para verificar o enviesamento do reconhecimento facial.

⁸⁵ HERNANDES, Raphael. **Reconhecimento facial salva vidas, mas cerceia liberdades**. Folha de S. Paulo, São Paulo, 19 de fevereiro de 2020. Disponível em: <https://temas.folha.uol.com.br/inteligencia-artificial/ia-no-mundo-real/reconhecimento-facial-salva-vidas-mas-cerceia-liberdades.shtml>. Acesso em: 26 out. 2021.

⁸⁶ NAÍSA, Letícia. **Reconhecimento facial: lado bom não compensa efeito perverso, diz sociólogo**. Tilt Uol, 30 de agosto de 2021. Acesso em: 26 out. 2021.

⁸⁷ **Gender Shades**, resultados. Disponível em: <http://gendershades.org/overview.html>. Acesso em 27 out. 2021.

O projeto analisou 1270 (um mil duzentas e setenta) imagens de sujeitos de três países africanos e três países europeus, agrupando-os por gênero, tipo de pele e interseção dos dois. Do total de participantes, 44,6% foi classificado como pertencente ao gênero feminino e 54,4%, ao masculino. Quanto ao tipo de pele, havia seis classificações, sendo três equivalentes a pele mais clara e três a mais escura. Do total, 46,4% foi definido como de pele mais escura e 53,6% de pele mais clara⁸⁸.

O estudo supramencionado utilizou serviços de reconhecimento facial fornecidos pelas empresas IBM Watson, Face++ e Microsoft. Os resultados apresentaram discrepância significativa entre a taxa de acurácia do reconhecimento facial de homens e de mulheres. As empresas IBM Watson, Face++ e Microsoft possuem uma taxa de precisão do reconhecimento facial em mulheres de 79,7%, 78,7% e 89,3%, respectivamente. Já as taxas de precisão do reconhecimento facial em homens são de 94,4%, 99,3% e 97,4%, evidenciando que os sistemas possuem mais dificuldade em reconhecer pessoas classificadas como pertencentes ao gênero feminino⁸⁹.

A análise interseccional, ou seja, de raça e de gênero em conjunto, evidencia uma enorme disparidade na precisão do reconhecimento facial de mulheres negras. Os desempenhos das empresas IBM Watson, Face++ e Microsoft na precisão do reconhecimento de homens de peles mais escuras foram, respectivamente, 88%, 99,3% e 94%. Os índices de homens de peles mais claras foram 99,7%, 99,3% e 100%, respectivamente, evidenciando uma maior precisão para identificar rostos de homens brancos⁹⁰.

Os índices de precisão do reconhecimento facial de mulheres de peles mais escuras das empresas IBM Watson, Face++ e Microsoft são de 65,3%, 65,5% e 79,2%, ao passo que os índices do reconhecimento facial de mulheres de peles mais claras são 92,9%, 94% e 98,3%. Esses índices demonstram que os sistemas de reconhecimento facial continuam privilegiando quem sempre esteve em posição superior na sociedade: homens brancos. A diferença entre a precisão do reconhecimento facial de homens brancos e mulheres negras da empresa IBM é de 34,4%⁹¹.

⁸⁸ *Ibidem.*

⁸⁹ *Ibidem.*

⁹⁰ *Ibidem.*

⁹¹ *Ibidem.*

A *National Institute of Standards and Technology* (NIST) também realizou um estudo que comprova a discriminação realizada pelos algoritmos. O teste analisou 189 (cento e oitenta e nove) algoritmos enviados por 99 (noventa e nove) desenvolvedores de sistemas de reconhecimento facial, incluindo instituições acadêmicas e empresas como *Idemia, Intel, Microsoft, Panasonic, SenTime* e *Vigilant Solutions*. Foram utilizadas 18 (dezoito) milhões de fotos de mais de 8 (oito) milhões de pessoas, todas retiradas do banco de dados de departamentos estatais. Os testes foram feitos tanto para desbloquear telefones, como para procurar um suposto suspeito em meio a um conjunto de fotos⁹².

Os resultados demonstraram falhas em que os sistemas identificaram dois rostos distintos como se fossem iguais, bem como não conseguiu perceber que duas fotografias se tratavam do mesmo rosto e os identificou como rostos distintos. A análise apontou que o reconhecimento facial identifica os rostos brancos com mais facilidade, de modo que a probabilidade de faces de asiáticos e afro americanos serem identificadas erroneamente foi até cem vezes maior do que a de homens brancos⁹³. É evidente, portanto, que o reconhecimento facial é enviesado, perpetua a discriminação existente na sociedade e pode gerar efeitos nefastos, como será demonstrado nos exemplos.

O reconhecimento facial tem acarretado ilegalidades em diversos países. Nos Estados Unidos, Robert Williams, um homem negro e periférico, foi preso pela polícia de Detroit, em 2018, na frente de sua família, mesmo sem ter cometido crime algum⁹⁴. Williams foi classificado pelo sistema de reconhecimento facial da Polícia do Estado de Michigan, que o confundiu com um ladrão de relógios que a polícia procurava. A prisão se deu após o segurança da loja, que sequer testemunhou o roubo, o reconhecer por meio da sua foto de carteira de motorista, que foi colocada em uma fileira com fotos de outros homens negros. A partir de uma imagem de baixa qualidade

⁹² HARWELL, Frew. **Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use.** The Washington Post, 19 de dezembro de 2019. Disponível em: <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>. Acesso em: 24 out. 2021.

⁹³ *Ibidem*.

⁹⁴ BURTON-HARRIS, Victoria. MAYOR, Philip. **Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart.** American Civil Liberties Union, 24 de junho de 2020. Disponível em: <https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart/>. Acesso em: 24 out. 2021.

de um sistema de vigilância, o segurança afirmou que Robert Williams era o indivíduo que havia cometido o crime, mas a única semelhança entre ambos era a cor da pele⁹⁵.

Após passar horas na prisão indevidamente, Robert Williams foi solto, no entanto, sua prisão havia sido oficialmente registrada. Cumpre destacar que ele apenas soube da utilização do sistema de IA quando um oficial afirmou que o computador provavelmente tivesse errado ao identifica-lo como a pessoa procurada. O caso de Williams evidencia diversos aspectos negativos do uso do reconhecimento facial, como o racismo reproduzido pela IA, a existência de viés algorítmico que prejudica um determinado grupo de pessoas –homens negros, neste caso-, e a ausência de transparência acerca da utilização do *software*.

Em 2019, Nijeer Parks foi preso ilegalmente por onze dias, em *New Jersey*, após ser classificado como um homem que havia cometido uma série de crimes, dentre eles assalto, porte de arma, falsidade ideológica e resistência à prisão. Sua foto foi comparada com uma identidade falsa deixada no local do crime, o que ensejou a prisão. Apesar da alegação de que o reconhecimento facial é utilizado apenas para investigação, há casos em que é utilizado como a única evidência para embasar uma prisão, trazendo novamente a problemática acerca do uso da inteligência artificial de reconhecimento facial pelo Estado⁹⁶.

Adicionalmente, evidencia a ausência de transparência acerca do uso da IA, pois de acordo com Nijeer Parks, ele não soube qual foto foi utilizada pelo sistema, nem de qual local se originou. Segundo Albert Fox, diretor-executivo da Technology Oversight Project, uma organização sem fins lucrativos opositora ao uso do reconhecimento facial pelo Estado, não há o número exato de tecnologias de reconhecimento facial utilizadas nos Estados Unidos, de modo que algumas pessoas são presas equivocadamente e sequer sabem da existência ou do funcionamento desses sistemas⁹⁷.

Além de os sistemas utilizados na aplicação da lei não estarem disponíveis para auditoria pública, os *softwares* são propriedades de empresas, o que dificulta a pesquisa sobre quais imagens foram inseridas para orientar sua detecção e identificação de rostos. A inexistência de informações sobre o funcionamento dos

⁹⁵ *Ibidem*.

⁹⁶ GENERAL, John. SARLIN, Jon. **A false facial recognition match sent this innocent black man to jail**. Cnn Business, 29 de abril de 2021. Disponível em: <https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html>. Acesso em: 24 out. 2021.

⁹⁷ *Ibidem*.

algoritmos impossibilita que os indivíduos saibam se esses sistemas estão sendo utilizados adequadamente⁹⁸.

Infelizmente, os casos de Robert Williams e Nijeer Parks não são acontecimentos isolados. No Brasil, em 2019, uma mulher foi detida equivocadamente em Copacabana, no Rio de Janeiro, após falha no sistema de reconhecimento facial da polícia. De acordo com a Secretaria Estadual de Polícia Militar, as câmeras apontaram-na como uma foragida da justiça acusada de ter cometido os crimes de homicídio e ocultação de cadáver. Após ser direcionada à delegacia, a identidade da mulher foi confirmada, constatando-se de que não era a pessoa foragida⁹⁹.

O sistema de inteligência artificial utilizado no caso supramencionado funciona em parceria com o Centro Integrado de Comando e Controle (CICC) da Polícia Militar e, para identificar os foragidos, as câmeras que realizam o reconhecimento facial são integradas ao banco de dados da Polícia Civil. Ou seja, um computador utiliza as imagens das câmeras de segurança, medindo as características dos rostos, como “a distância entre os olhos, o tamanho do nariz, da boca e do queixo, além de identificar a linha da mandíbula”¹⁰⁰.

Apesar de medir as características dos rostos e de receber os dados da Polícia Civil, o sistema é falho, haja vista a prisão ilegal de uma mulher enquanto caminhava pelo bairro de Copacabana. Além das falhas gerarem casos de pessoas presas equivocadamente, o sistema de reconhecimento facial é incapaz de identificar mudanças das características físicas do indivíduo. Como exemplo, em 2018, a biometria facial utilizada no transporte público do Distrito Federal (DF) não reconheceu Giulia Soares, estudante da Universidade de Brasília (UnB), após retirar procedimento químico do cabelo, deixando-o com seus cachos naturais¹⁰¹.

A foto utilizada na base de dados era de 2016, quando a estudante possuía o cabelo liso e mais longo. Ao utilizar o cartão estudantil, que concede direito à gratuidade ao pagamento do valor da passagem, a câmera compara o usuário à foto

⁹⁸ KLOSOWSKI, Thorin. **Facial Recognition Is Everywhere. Here's what we can do about it.** Wirecutter, 15 de julho de 2020. Disponível em: <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>. Acesso em: 24 out. 2021.

⁹⁹ **Sistema de Reconhecimento facial da PM do RJ falha e mulher é detida por engano.** G1, Rio de Janeiro, 11 de julho de 2020. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 24 out. 2021.

¹⁰⁰ *Ibidem*.

¹⁰¹ TEIXEIRA, Isadora. **Biometria facial nos ônibus não reconhece mudança visual de alunos.** Metrôpoles, Brasília, 12 de maio de 2018. Disponível em: <https://www.metropoles.com/distrito-federal/transporte-df/biometria-facial-nos-onibus-nao-reconhece-mudanca-visual-de-alunos>.

do arquivo. Caso detecte diferenças, o sistema entende que uma pessoa distinta utiliza o benefício e suspende o uso do cartão, abrindo um prazo de dez dias para que o usuário se manifeste. Se houver algum problema quanto ao uso do e-mail cadastrado no sistema, como aconteceu com Giulia Soares, presume-se a fraude e o cartão é bloqueado¹⁰².

O sistema utilizado em Brasília, que se tornou obrigatório desde abril de 2018¹⁰³, não reconhece pessoas que passaram por transição de gênero, como é o caso de Maria Eduarda Krasny, também estudante da UnB. Ela teve o passe livre suspenso porque a fotografia constante na base de dados foi tirada antes da transição de gênero e, mesmo após adquirir a segunda via do cartão, sua imagem antiga ainda constava nele, bem como seu nome anterior à transição.

A biometria facial utilizada no transporte público do Distrito Federal não observa as alterações físicas dos estudantes ao longo do tempo, evidenciando a inexistência de atualização das imagens da base de dados utilizada para comparar o usuário que insere o cartão no leitor no ônibus com a fotografia na máquina.

O sistema já identificou mais de 2.200 (duas mil e duzentas) fraudes no uso do Passe Livre Estudantil no DF¹⁰⁴, o que leva a refletir se realmente houve mais de duas mil fraudes ou se vários estudantes foram prejudicados pelas falhas do sistema, bem como pela desatualização dos dados. Diante de tantos casos de falhas no reconhecimento facial, urge a necessidade de discutir quais regulações existem para proteger os direitos individuais, demonstrar transparência acerca da utilização e prevenir contra a discriminação algorítmica.

c. A legislação aplicável ao reconhecimento facial

A implementação do reconhecimento facial traz preocupações acerca da transparência, o que enseja a necessidade de o Poder Público apresentar dados sobre a sua implementação, além de regular a temática. Nesse sentido, o Instituto Igarapé

¹⁰² *Ibidem*.

¹⁰³ **Biometria facial, agora, é obrigatória em 100% dos ônibus do DF.** Metrôpoles, Brasília, -2 de maio de 2018. Disponível em: <https://www.metropoles.com/distrito-federal/transporte-df/biometria-facial-agora-e-obrigatoria-em-100-dos-onibus-do-df>. Acesso em: 26 out. 2021.

¹⁰⁴ YOSHIMINE, Rita. **Biometria facial identifica 2,2 mil fraudes em passe livre do DF.** G1, Distrito Federal, 17 de fev. de 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/biometria-facial-identifica-22-mil-fraudes-em-passe-livre-do-df.ghtml>. Acesso em: 26 out. 2021.

e o Data Privacy Brasil¹⁰⁵ elaboraram um estudo comparativo acerca do emprego do reconhecimento facial no Reino Unido, nos Estados Unidos e na França, a partir de cinco princípios: finalidade, necessidade, transparência, segurança e não discriminação.

Consoante evidencia a pesquisa, as câmeras são utilizadas para monitoramento no Reino Unido desde 1953 e o sistema de reconhecimento facial é usado pela polícia do país desde 1998, o que ensejaram a necessidade de uma robusta legislação, haja vista o debate de possíveis violações a direitos a partir do videomonitoramento constante. Destarte, embora o Reino Unido não possua uma legislação específica para a regulamentação do reconhecimento facial que utiliza inteligência artificial, há diversas recomendações que enquadram o RF dentro da legislação pré-existente.

A partir da análise de cinco documentos do Reino Unido, o Instituto Igarapé e o Data Privacy Brasil detalharam o tratamento conferido pela legislação que justifica a regulação dos sistemas de reconhecimento facial para proteger a vida e a propriedade, detectar crimes, verificar ameaças à segurança pública e garantir a segurança nacional. Nesse sentido, os sistemas são utilizados para as seguintes finalidades:

Controle de imigração; investigação, detecção e prevenção de atividades criminosas e terroristas; segurança nacional e segurança pública; bem-estar econômico do país; prevenção de desordem; proteção da saúde ou da moral; proteção de direitos e liberdades.

Os documentos impõem limites ao uso do reconhecimento facial no Reino Unido ao estabelecer que seu uso deve ocorrer somente nas hipóteses que se tratem de uma “demanda urgente, proporcional e efetiva”, quando inexistir outros meios para atingir o objetivo.

Ademais, destaca a proteção dos dados dos indivíduos ao dispor que o consentimento da população deve ser obtido quando se tratar de vigilância em locais públicos, conforme consta no estudo. No entanto, naqueles locais públicos em que não há estabelecido ao certo a privacidade dos indivíduos e, conseqüentemente, não

¹⁰⁵ FRANCISCO, Pedro Augusto P. Francisco; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais.** Brasil: Instituto Igarapé e Data Privacy Brasil Research, 2020. Disponível em: <https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf>. Acesso em: 26 out. 2021.

há necessidade de consentimento, o reconhecimento facial somente poderá ser utilizado se inexistir outro meio capaz de atender o objetivo pretendido¹⁰⁶.

Cumprido destacar que a legislação do Reino Unido ainda não criou um conselho para supervisionar os protocolos de uso do reconhecimento facial, mesmo ressaltando a necessidade de estruturas administrativas para fiscalizar e dispor acerca do emprego da tecnologia. A legislação também prevê a intervenção humana na tomada de decisões baseadas em informações advindas de sistemas de reconhecimento facial, ou seja, embora o RF possa ser utilizado para detectar um rosto, a decisão do que será feito a partir dele deve partir de um humano, sendo vedado integrar outro sistema de inteligência artificial para tomar decisões¹⁰⁷.

A regulação do Reino Unido prevê uma política de transparência ao estabelecer que o aviso aos cidadãos acerca do emprego de câmeras de monitoramento, bem como sua justificativa e o nome da empresa que a opera. Também é conferido a todos os indivíduos o direito de acessar as informações constantes nos sistemas, além de haver um canal para reclamações quando houver lesão pelo emprego das câmeras. Ademais, há o compromisso de algumas autoridades policiais revelarem dados acerca do uso do reconhecimento facial, como a quantidade de prisões realizadas, quantos alertas foram disparados pelo sistemas, quantas identificações foram incorretas e quantas faces foram registradas¹⁰⁸.

A regulação prevê, ainda, a proteção dos dados dos indivíduos gravados pelas câmeras, pois determina que todo o material gravado seja armazenado em segurança para manter a integridade dos dados, além de utilizar os sistemas fechados, ou seja, sem conexão com a *internet*. As imagens de indivíduos detidos são armazenadas pela polícia, no entanto, a regulação prevê a possibilidade de que os indivíduos absolvidos solicitem a remoção de suas imagens. Quanto à não-discriminação, a regulação do Reino Unido prevê a realização de avaliações de impacto à privacidade, bem como avaliação dos dados biométricos por um grupo de ética¹⁰⁹.

A pesquisa realizada pelo Instituto Igarapé em parceria com o Data Privacy Brasil também destaca a regulação do uso do reconhecimento facial nos Estados Unidos, ainda que não haja uma legislação abrangente em todo o território

¹⁰⁶ *Ibidem*, p. 7.

¹⁰⁷ *Ibidem*.

¹⁰⁸ *Ibidem*.

¹⁰⁹ *Ibidem*, p. 8.

estadunidense. Há legislações municipais que têm ganhado notoriedade, especialmente porque o uso do reconhecimento facial é banido em diversas cidades dos Estados Unidos, por considerar que os potenciais benefícios da aplicação do sistema não se sobrepõem ao amplo debate que deve ocorrer para analisar a viabilidade do emprego do RF¹¹⁰.

Nos Estados Unidos, a proibição da utilização dos sistemas de reconhecimento tem como fundamentação a proteção dos direitos individuais e coletivos estabelecidos na Constituição do país. Argumenta-se que o reconhecimento facial afeta o devido processo legal, uma vez que inverte a presunção de inocência para a presunção de que todas as pessoas são potenciais suspeitas. Além disso, pode causar danos à privacidade e à liberdade de expressão, além das diversas falhas do reconhecimento de mulheres e pessoas não-brancas¹¹¹.

As regulações analisadas pelo Instituto Igarapé em parceria com o Data Privacy Brasil proíbem “a aquisição, posse, acesso ou uso de sistemas de reconhecimento facial, ou qualquer outro dado obtido por meio desses sistemas por parte de órgãos ou funcionários públicos das cidades e estados que estejam em vigor”. Desse modo, como mencionado anteriormente, os Estados Unidos possuem uma regulação que proíbe a utilização do reconhecimento facial por agentes públicos¹¹².

Tal proibição é embasada, inclusive, por relatório publicado pelo Comitê de Política de Tecnologia dos EUA da *Association for Computing Machinery*, tida como a maior sociedade de computação educacional do mundo¹¹³. No entanto, cumpre destacar que, no dia 24 de agosto de 2021, o *US Government Accountability Office* divulgou um relatório que detalha o planejamento do uso da tecnologia por agências federais, verificando-se uma tendência do país em utilizar a tecnologia¹¹⁴.

O Estado de Massachusetts possui um projeto de lei que prevê o uso do reconhecimento facial em casos excepcionais, mediante requisição, que deverá conter informações acerca da autoridade que o utilizará, o propósito, os requisitos,

¹¹⁰ *Ibidem*, p. 9.

¹¹¹ *Ibidem*, p. 10.

¹¹² *Ibidem*.

¹¹³ **Statement on principles and prerequisites for the development, evaluation and use of unbiased facial recognition Technologies.** AMC U.S. Technology Policy Committee (USTPC). Disponível em: <https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf>. Acesso em: 26 out. 2021.

¹¹⁴ HENDLER, James. **Feds are increasing use of facial recognition systems – despite call for a moratorium.** The Conversation. Disponível em: <https://theconversation.com/feds-are-increasing-use-of-facial-recognition-systems-despite-calls-for-a-moratorium-145913>. Acesso em: 26 out. 2021.

bem como os dados obtidos e o período de sua retenção. De acordo com o Instituto Igarapé e com o Data Privacy Brasil, não foram localizadas regulações que discorram acerca da transparência do emprego do reconhecimento facial.

Quanto aos parâmetros antidiscriminatórios, o RF é proibido no país com a fundamentação de que acentua desigualdades pré-existentes. Somente o projeto de lei de Massachusetts estabelece a demonstração de acurácia¹¹⁵ tratando-se de gênero, raça e idade¹¹⁶.

O Instituto Igarapé e o Data Privacy Brasil trazem, ainda, um panorama da utilização do reconhecimento facial na França. O país ainda não possui uma regulação específica, no entanto, o RF vem sendo utilizado por órgãos público e, assim como ocorre no Reino Unido, utiliza-se a legislação existente para aplicar ao uso do RF. Importante destacar que, na França, o emprego dos sistemas tecnológicos de reconhecimento facial estão sendo usados para estudo, a fim de que o Estado compreenda os limites e os impactos da implementação.

Nesse diapasão, os sistemas utilizados são autorizados pelo Conselho de Estado, que analisa cada solicitação. O estudo verificou dois documentos¹¹⁷ da França que permitiram a verificação da regulação do reconhecimento facial quanto ao cinco aspectos mencionados anteriormente. Quanto à finalidade, a França estabelece que o tratamento de dados biométricos somente poderá ocorrer para proteger interesses vitais e que os direitos dos titulares deverão ser preservados. Ademais, recomenda que os dados sejam armazenados em dispositivos pessoais acessíveis para conferir proteção.

No entanto, o tratamento de dados biométricos quando o consentimento do titular não for possível poderá ocorrer, ainda que seja uma exceção. Para tanto, é necessário uma autorização prévia e cada caso tem suas variações, sendo necessário estabelecer limites mais rigorosos em alguns. Quanto à transparência, a regulação vigente limita-se a estabelecer algum modo de informar as pessoas sobre a existência do sistema, bem como de sua consequência para que os indivíduos possam reafirmar seus direitos.

¹¹⁵ Para saber mais sobre esse tema, veja: UCHÔA, Valeska de Sousa. **Aumento de dados para reconhecimento facial com transferência de aprendizado de CNNs**. Dissertação de Mestrado em Ciência da Computação da UFPI, Centro de Ciências da Natureza da Universidade Federal do Piauí, Teresina, 2019.

¹¹⁶ FRANCISCO, Pedro Augusto P. Francisco; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais**. Brasil: Instituto Igarapé e Data Privacy Brasil Research, 2020. Disponível em: <https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf>. Acesso em: 26 out. 2021.

¹¹⁷ CNIL- Facial recognition: for a debate living up the challenges. Parliamentary Office for Scientific and Technological Assessment – Briefing 14 – Facial Recognition – 2019.

No que diz respeito aos parâmetros antidiscriminatórios, a regulação ressalta a identificação de vieses algorítmicos no reconhecimento facial e afirma que eles são levados em consideração, conforme dispõe o estudo. A conclusão da análise da regulação da França é de que ela é insuficiente, de modo que o Estado francês necessita de uma regulação específica para tratar do tema, haja vista a existência de lacunas na legislação vigente.

No Brasil não há legislação federal específica sobre o emprego do reconhecimento facial, no entanto, há espaço para uma futura regulamentação, haja vista a realização de audiências públicas na Câmara dos Deputados e no Ministério Público do Distrito Federal e Territórios, em 2018. Atualmente existem diversas normas que dispõem acerca da proteção dos direitos individuais, a exemplo da Constituição Federal de 1988, do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados (LGPD)¹¹⁸.

Embora a LGPD excetue de suas determinações as atividades de segurança pública, o art. 4º, §1º estabelece que deverá ser criada lei específica para regular tais atividades, seguindo os mesmos princípios da LGPD. No Congresso Nacional há um projeto de lei (PL) que apresenta uma proposta de implementação geral do reconhecimento facial¹¹⁹ e dois que dispõem sobre casos específicos, sendo um sobre controle de fluxo de transporte público e o outro sobre identificação em estabelecimentos penais¹²⁰.

Conforme dispõem o Instituto Igarapé e o Data Privacy Brasil, os projetos de lei em trâmite apenas preveem o emprego dos sistemas de RF, sem discorrer sobre princípios, direitos, transparência, ou demais análises necessárias para garantir acurácia. Apenas o Projeto de Lei nº 4.612/2019 dispõe sobre boas práticas, dentre elas:

¹¹⁸ FRANCISCO, Pedro Augusto P. Francisco; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais**, p. 13. Brasil: Instituto Igarapé e Data Privacy Brasil Research, 2020. Disponível em: <https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf>. Acesso em: 26 out. 2021.

¹¹⁹ BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.612, de 21 de agosto de 2019**. Dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455>. Acesso em: 27 out. 2021.

¹²⁰ BRASIL. Câmara dos Deputados. **Projeto de Lei nº 9.736, de 07 de março de 2018**. Acrescenta dispositivo à Lei nº 7.210, de 11 de julho de 1984, para incluir a previsão de identificação por reconhecimento facial. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011>. Acesso em: 27 out. 2021.

(i) previsão de direitos/preceitos; (ii) definição multissetorial de boas práticas, especialmente em casos nos quais as consequências do uso do reconhecimento facial sejam desconhecidas; (iii) obrigações específicas para desenvolvedores e utilizadores de reconhecimento facial; (iv) restrições ao uso compartilhado de dados provenientes de reconhecimento facial; (v) envolvimento da Autoridade Nacional de Proteção de Dados¹²¹.

Cumprе destacar que o PL 4.612/2019, da Câmara dos Deputados, veda o emprego do reconhecimento facial massivo, ou seja, ininterrupto e indiscriminado que funcione em qualquer local, a qualquer hora. Ademais, incumbe à Autoridade Nacional de Proteção de Dados (ANPD) a elaboração de protocolos para uso do reconhecimento facial, além de estabelecer que os sistemas devem ser supervisionados por seres humanos. Desse modo, esse projeto de lei federal propõe uma regulação que limita o emprego dos sistemas de reconhecimento facial¹²².

Quanto à legislação estadual, há duas leis que versam sobre o reconhecimento facial para autenticação, ou seja, para controle de acesso a espaços, são elas: a Lei nº 26.873/2019, do Ceará, e a Lei nº 7.123/2015, do Rio de Janeiro. Há, ainda, duas leis que versam sobre o emprego do reconhecimento facial de modo genérico, podendo ser utilizadas para autenticação ou identificação, o que sugere o uso para identificar um rosto em um local com várias pessoas sob a justificativa de segurança para a sua finalidade. Somente a legislação do Rio de Janeiro menciona proteção aos direitos individuais, o que ratifica a necessidade de se definir parâmetros para a utilização do RF em âmbito nacional¹²³.

Adicionalmente, os estados de Minas Gerais, Paraná e Rio de Janeiro possuem propostas legislativas em trâmite que visam a implantação dos sistemas de reconhecimento facial para identificar criminosos e aumentar a segurança da população, sendo que os PLs de Minas Gerais e do Paraná determinam que o desvio de finalidade ensejará a tomada de “medidas adequadas” de forma totalmente genérica, sem especificar quais atitudes serão adotadas diante de falhas¹²⁴.

Sendo assim, no contexto brasileiro inexistе regulação federal específica para o emprego do reconhecimento facial tecnológico. Ademais, as legislações estaduais

¹²¹ P. 14.

¹²² *Ibidem*.

¹²³ FRANCISCO, Pedro Augusto P. Francisco; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais**, p. 14-15. Brasil: Instituto Igarapé e Data Privacy Brasil Research, 2020. Disponível em: <https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%ABlico.pdf>. Acesso em: 26 out. 2021.

¹²⁴ *Ibidem*.

existentes dividem-se entre dispor somente acerca da autenticação de pessoas e da identificação de pessoas entendidas como potenciais suspeitos para a finalidade segurança. A primeira hipótese serve para adentrar espaços públicos, por exemplo, e a segunda é utilizada para identificar rostos em meio a multidões.

Destarte, urge a necessidade de elaborar uma regulação antidiscriminatória, transparente e que abarque a proteção individual dos indivíduos à privacidade, especialmente porque os sistemas de inteligência artificial utilizados reproduzem os preconceitos dos programadores, que inserem os dados nas máquinas de IA. Adicionalmente, o contexto brasileiro de uso do próprio reconhecimento fotográfico, mesmo sem sistema tecnológico, contribui para a perpetuação do racismo institucional, especialmente diante da quantidade de prisões equivocadas por meio do reconhecimento por foto de indivíduos negros.

III. A necessidade de parâmetros antidiscriminatórios

a. A perpetuação do racismo institucional pela IA

Conforme mencionado anteriormente, a inteligência artificial possui vieses algorítmicos, pois os sistemas funcionam especialmente por meio de *machine learning* e *deep learning*, ou seja, as máquinas aprendem a concluir uma tarefa a partir do treinamento de passo-a-passos inseridos pelos programadores.

No Brasil, o reconhecimento de pessoas é um disseminador de racismo e a utilização do reconhecimento facial tecnológico sem estudos aprofundados contribui para a perpetuação das discriminações existente na sociedade, sobretudo o racismo.

O reconhecimento de pessoas e coisas está previsto no art. 226 do Código de Processo Penal (CPP), que estabelece que:

Art. 226. Quando houver necessidade de fazer-se o reconhecimento de pessoa, proceder-se-á pela seguinte forma:

I - a pessoa que tiver de fazer o reconhecimento será convidada a descrever a pessoa que deva ser reconhecida;

II - a pessoa, cujo reconhecimento se pretender, será colocada, se possível, ao lado de outras que com ela tiverem qualquer semelhança, convidando-se quem tiver de fazer o reconhecimento a apontá-la;

III - se houver razão para recear que a pessoa chamada para o reconhecimento, por efeito de intimidação ou outra influência, não diga a verdade em face da pessoa que deve ser reconhecida, a autoridade providenciará para que esta não veja aquela;

IV - do ato de reconhecimento lavrar-se-á auto pormenorizado, subscrito pela autoridade, pela pessoa chamada para proceder ao reconhecimento e por duas testemunhas presenciais.

Parágrafo único. O disposto no III deste artigo não terá aplicação na fase da instrução criminal ou em plenário de julgamento.

A legislação penal brasileira autoriza o emprego do reconhecimento de pessoas no processo penal. Na prática, o reconhecimento é realizado por meio de foto e contribui para prisões ilegais de pessoas negras.

No dia 08 de setembro de 2021, um motorista de aplicativo denominado Jeferson da Silva compareceu ao seu antigo local de trabalho para receber parcela remanescente de verbas salariais de um contrato findo em 2015. Ao chegar ao local, era aguardado por policiais, que o prenderam. O rapaz, de vinte e nove anos, foi identificado como autor de um crime por meio de uma fotografia 3x4 tirada há mais de quinze anos. Embora Jeferson da Silva não tenha cometido o crime, passou seis dias presos até que conseguir um *habeas corpus*¹²⁵.

¹²⁵ GUIMARÃES, Hellen. **Nos erros do reconhecimento facial, um “caso isolado” atrás do outro**. Piauí, 24 de setembro de 2021. Disponível em: <https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/>. Acesso em: 27 out. 2021.

Em outubro de 2020, a 6ª Turma do Superior Tribunal de Justiça (STJ) firmou o entendimento de que o reconhecimento de suspeitos realizado por fotos como única prova é insuficiente para embasar uma prisão. No julgamento, a turma concedeu *habeas corpus* a um indivíduo cuja condenação pelo crime de roubo foi baseada exclusivamente no reconhecimento fotográfico feito pelas vítimas. A condenação não observou o disposto no art. 226 do CPP, mencionado acima¹²⁶. Muito embora a decisão do STJ tenha sido proferida em outubro de 2020, a prisão de Jeferson da Silva, que ocorreu em setembro de 2021, tinha como embasamento o reconhecimento fotográfico, contrariando não apenas o CPP, mas também o entendimento do Tribunal Superior.

No dia 10 de setembro de 2021, o mototaxista Alexandre dos Reis Pereira Camargo foi solto após uma prisão preventiva indevida que durou 37 (trinta e sete) dias, fruto também de um reconhecimento fotográfico. Ele foi identificado como um dos indivíduos envolvidos em um conflito com policiais em um local que fica a 60 (sessenta) quilômetros de sua residência. Na fotografia utilizada, Alexandre Camargo tinha apenas 12 (doze) anos e tratava-se de imagem da primeira carteira de identidade. A fotografia foi retirada da base dados do Detran e não foi informado a ele quando passou a integrar os registros de suspeitos mantidos pela Polícia Civil¹²⁷, o que indica a falta de transparência na manutenção de dados sensíveis dos indivíduos.

Há, ainda, mais um caso recente e significativo que também ocorreu no Rio de Janeiro, assim como os dois mencionados inicialmente. No dia 17 de agosto de 2021, Raoni Lázaro Rocha Barbosa, cientista de dados, recebeu, em sua residência, policiais civis da Delegacia de Repressão às Ações Criminosas Organizadas às 06 horas da manhã, tendo sido preso sem nenhuma justificativa. Devido à tramitação do processo em segredo de justiça, seu advogado apenas pôde visualizar o motivo da prisão doze dias após o ocorrido. Raoni Barbosa foi confundido com Raoni Ferreira dos Santos, procurado por integrar a milícia de Duque de Caxias. Embora o cientista de dados nunca tenha morado no local, foi preso por ter sido erroneamente reconhecido por uma foto que era do suspeito¹²⁸.

¹²⁶ VITAL, Danilo. **Reconhecimento facial por fotografia não serve para embasar condenação, diz STJ**. Consultor Jurídico, 27 de outubro de 2020. Disponível em: <https://www.conjur.com.br/2020-out-27/reconhecimento-foto-nao-embasar-condenacao-stj>. Acesso em: 27 out. 2021.

¹²⁷ GUIMARÃES, Hellen. **Nos erros do reconhecimento facial, um “caso isolado” atrás do outro**. Piauí, 24 de setembro de 2021. Disponível em: <https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/>. Acesso em: 27 out. 2021.

¹²⁸ *Ibidem*.

Além de morarem no Rio de Janeiro, os três homens dos casos supramencionados têm um ponto em comum: a negritude. Mesmo exercendo profissões distintas, todos foram reconhecidos equivocadamente como suspeitos de crimes que não cometeram, evidenciando a existência do racismo institucional que persegue a população negra. Ademais, confirma o sistema penal como um instrumento de perpetuação do racismo e da marginalização do povo negro.

As prisões equivocadas embasadas exclusivamente no reconhecimento fotográfico ocorrem com frequência não apenas no Rio de Janeiro, mas em todo o Brasil. De acordo com dois relatórios elaborados pela Defensoria Pública do Estado do Rio de Janeiro em conjunto com o Colégio Nacional de Defensores Públicos Gerais, entre 2012 e 2020 ocorreram pelo menos 90 (noventa) prisões indevidas no país, sendo que 81% (oitenta e um por cento) das pessoas presas eram negras. O primeiro relatório foi produzido em setembro de 2020 e apresentou 58 (cinquenta e oito) erros em reconhecimento fotográfico entre junho de 2019 e março de 2020, tendo todos os casos ocorrido no Rio de Janeiro, e o segundo apresentou 28 (vinte e oito) prisões ocorridas em dez estados.¹²⁹

Insta destacar que, de acordo com o primeiro relatório, o período em que as pessoas ficaram indevidamente presas varia entre 5 (cinco) a 1.116 (um mil, cento e dezesseis) dias, cerca de 3 (três) anos e 21 (vinte e um) dias.

A média indica um período de 9 (nove) meses. No segundo período, o índice de tempo de prisão indevida varia entre 24 (vinte e quatro) a 851 (oitocentos e cinquenta e um) dias, o que corresponde a até 2 (dois) anos e três meses, sendo que a média também é de 9 (nove) meses¹³⁰. Todas as pessoas foram absolvidas, no entanto, essas situações são capazes de gerar traumas, levando a confusões mentais, consoante comenta João Paulo Martinelli¹³¹.

Além do racismo institucional, o estudo comprova a necessidade de seguir o devido processo legal e não realizar prisões que tenham fundamentação

¹²⁹ **Relatório indicam prisões injustas após reconhecimento fotográfico.** Conselho Nacional das Defensoras e Defensores Públicos-Gerais. Disponível em: <http://condege.org.br/2021/04/19/relatorios-indicam-prisoas-injustas-apos-reconhecimento-fotografico/>. Acesso em: 27 out. 2021.

¹³⁰ **Relatório aponta 90 prisões indevidas após reconhecimento fotográfico; Defensoria do CE discute tema ao vivo.** Defensoria Pública Geral do Estado do Ceará. Disponível em: <https://www.defensoria.ce.def.br/noticia/relatorio-aponta-90-prisoas-indevidas-apos-reconhecimento-fotografico-defensoria-do-ce-discute-tema-ao-vivo/>. Acesso em: 27 out. 2021.

¹³¹ MARTINELLI, João Paulo. **O erro no reconhecimento do acusado e as prisões injustas.** Estadão, 21 de setembro de 2021. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/o-erro-no-reconhecimento-do-acusado-e-as-prisoas-injustas/>. Acesso em: 27 out. 2021.

exclusivamente no reconhecimento fotográfico, especialmente porque intensifica a violência na periferia¹³².

Insta destacar, ainda, que cerca de 56% (cinquenta e seis por cento) da população do Brasil se autodeclara negra, sendo que 19,2 milhões de pessoa se assumem como pretas e 89,7% milhões de declaram pardos¹³³. É evidente que os negros são a maior parte da população e, ainda assim, o sistema penal brasileiro contribui para o racismo e, conseqüentemente, para a prisão ilegal. Isso ratifica a necessidade de desenvolver requisitos para que o reconhecimento facial tecnológico não continue a disseminar racismo e a produzir efeitos nefastos, como as prisões ilegais supramencionadas.

Assim como a utilização do reconhecimento de pessoas é problemática, o uso do reconhecimento facial tecnológico também é, embora pareça que uma máquina não faria os mesmos julgamentos dos humanos ao identificar ou ao prender uma pessoa. Consoante explica Pablo Nunes, os algoritmos são produzidos em um contexto da sociedade e o reproduzem, ou seja, inexistente neutralidade na sua utilização¹³⁴. Sendo assim, é necessário não apenas estabelecer parâmetros que a IA deve seguir para ser antidiscriminatória, mas em uma regulação específica que garanta a manutenção dos direitos individuais.

b. Uma luta contra o racismo e discriminações: quais medidas devem ser adotadas?

Consoante fora demonstrado ao longo do trabalho, o emprego do reconhecimento facial tecnológico pelo Estado sem regulação uniformizada apresenta os seguintes problemas: (i) ausência de transparência; (ii) reprodução de discriminação e preconceitos presentes nos seres humanos; e (iii) ausência de proteção aos direitos individuais.

¹³² NAÍSA, Letícia. **Reconhecimento facial: lado bom não compensa efeito perverso, diz sociólogo**. Tilt Uol, 30 de agosto de 2021. Acesso em: 26 out. 2021.

¹³³ AFONSO, Nathália. **Dia da Consciência Negra: números expõem desigualdade racial no Brasil**. Lupa News, Piauí, 20 de novembro de 2019. Disponível em: <https://piaui.folha.uol.com.br/lupa/2019/11/20/consciencia-negra-numeros-brasil/>. Acesso em: 27 out. 2021.

¹³⁴ GUIMARÃES, Hellen. **Nos erros do reconhecimento facial, um “caso isolado” atrás do outro**. Piauí, 24 de setembro de 2021. Disponível em: <https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/>. Acesso em: 27 out. 2021.

Desse modo, é necessário criar medidas que possibilite a existência de uma IA antidiscriminatória e de uma regulação que seja capaz de atender a esses três pontos mencionados. Nesse sentido, os parâmetros para que o reconhecimento facial tecnológico seja transparente e garanta a proteção dos direitos individuais podem ser extraídos do modelo utilizado pelo País de Gales.

O país utiliza o reconhecimento facial ao vivo (*Live Facial Recognition* em inglês), que detecta crimes e auxilia os policiais a localizarem pessoas procuradas pela justiça. O sistema também possui uma lista que contém os criminosos procurados. Quando a população passa pelo local que possui o sistema, ele detecta os rostos e, caso localize um procurado, envia um alerta aos policiais. A partir disso, um policial analisa as imagens e decide se aborda a pessoa ou não¹³⁵.

A página oficial da *Metropolitan Police*, que utiliza o reconhecimento facial ao vivo, ressalta que os policiais sempre explicam às pessoas o motivo da abordagem, além de fornecer um folheto que explica como podem contatá-los para fazer perguntas. As imagens que ensejarem alertas são mantidas por até 31 (trinta e um) dias, ou até que a investigação seja concluída. Quando um rosto é reconhecido e não gera nenhum alerta, os dados biométricos do indivíduo são apagados de modo automático e imediatamente. Além disso, uma pessoa pode escolher não passar pelo reconhecimento facial ao vivo¹³⁶.

O modelo adotado pelo País de Gales pode ser utilizado como referência quanto à transparência e manutenção dos direitos individuais porque, além de terem realizado dez testes para verificar a utilidade do sistema, os testes acontecerem em ambientes variados. Adicionalmente, sempre que o reconhecimento facial ao vivo é utilizado, as seguintes medidas de transparência são adotadas: “informação de onde o sistema será implantado; publicação dos resultados de cada uso; disseminação de bilhetes informativos ao público; conscientização do uso; disponibilização de oficiais para explicar ao público o que é e como o sistema funciona”¹³⁷.

Além das medidas supramencionadas, a página oficial apresenta a lista de legislação que ampara o emprego do reconhecimento facial ao vivo no país, além de apresentar documentos que detalham o procedimento operacional, orientações, padrões

¹³⁵ **Live Facial Recognition.** *Metropolitan Police, Advice and Information.* Disponível em: https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/?_cf_chl captcha tk =9hjbJXb9dLgJtrMQqrLKHfL7eEq4quap.lkgTcQknTE-1635515747-0-gaNycGzNCSU. Acesso em: 28 out. 2021.

¹³⁶ *Ibidem.*

¹³⁷ *Ibidem.*

da captura de imagem e a política apropriada. O modelo se destaca, ainda, por disponibilizar avaliação do impacto da proteção de dados, que apresenta a identidade dos controladores de dados, o escopo e os objetivos do procedimento de dados, o período de retenção dos dados¹³⁸.

O modelo apresenta também um relatório de avaliação do impacto da igualdade, que possui três objetivos específicos, são eles¹³⁹:

Remover ou minimizar as desvantagens sofridas pelas pessoas devido às suas características; adotar medidas para proteger as necessidades das minorias quando suas necessidades forem distintas das necessidades de outras pessoas; incentivar as minorias a participarem da vida pública ou de outras atividades em que a participação é desproporcionalmente baixa.

O relatório de impacto da igualdade também apresenta diversos pareceres do Comissário da Informação acerca do uso do reconhecimento facial tecnológico e, dentre eles, um aponta que a proteção de dados se aplica a todo o reconhecimento facial, incluindo os dados biométricos e seu período de retenção. A criação desses documentos é uma das medidas a serem observadas para garantir a proteção individual dos usuários e, por conseguinte, promover a justiça algorítmica.

Sendo assim, é de extrema importância a elaboração de uma regulação capaz de explicar aos usuários onde o reconhecimento facial está implementado, qual é a sua finalidade, bem como os seus limites. Além disso, um modelo de regulação eficiente disponibiliza relatórios de riscos como a avaliação do impacto da proteção de dados e da desigualdade. Ademais, deve afixar placas em locais públicos que informem o uso do reconhecimento facial, além de disponibilizar agentes públicos capazes de explicar à população o funcionamento da tecnologia e, sobretudo, o motivo da detenção de um indivíduo que tenha sido identificado como procurado.

Não obstante seja necessário elaborar uma regulação eficiente, apenas demonstrar dados e disseminar informações acerca do uso do reconhecimento facial não supre todos os parâmetros que devem ser seguidos para o emprego da tecnologia sem discriminação. É necessário treinar as máquinas com diversidade de rostos para

¹³⁸ **Data Protection Impact Assessment (DPIA).** Metropolitan Police. Disponível em: https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/data-protection-impact-assessment.pdf?_cf_chl captcha tk =hnyz6pFaqDmKLg3L9Eiqg8ht78HGdyEX.pMRXt14sC4-1635520658-0-gaNycGzNDRE. Acesso em: 28 out. 2021.

¹³⁹ **Equality Impact Assessment – steps 1 to 7.** Metropolitan Police. Disponível em: <https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/equality-impact-assessment.pdf>. Acesso em: 28 out. 2021.

que seja capaz de identificar adequadamente as faces de pessoas negras, sem enquadrar todas como pertencente ao mesmo rosto negro.

Nesse sentido, Joy Buolamwini, uma cientista de dados e pesquisadora negra, propõe a criação de uma codificação mais inclusiva ao relatar que o *software* que utilizou na elaboração de um projeto no Instituto de Tecnologia de Massachusetts (MIT, sigla em inglês) era incapaz de detectar seu rosto. Ela explica que a informática utiliza técnicas de aprendizagem de máquina para o reconhecimento facial, então, se cria um grupo de formação com exemplos de rostos¹⁴⁰.

Destarte, consoante aborda Buolamwini, as máquinas são alimentadas com rostos para identificar e aprender o que é um rosto, mas se o programador não diversificar as imagens inseridas na máquina, ela não reconhecerá rostos que destoam daquilo que foi inserido nela, contribuindo para a disseminação do racismo. Ela ressalta que os grupos de formação das máquinas são criados por humanos, então, é possível criar grupos que reflitam um retrato mais rico da humanidade, mais diversificado¹⁴¹.

Desse modo, ela propõe a inserção de dados mais semelhantes à realidade. Aplicando a perspectiva ao emprego do reconhecimento facial no Brasil, a IA deveria ser alimentada com diversos de diversas cores e nacionalidades, considerando que se trata da maior parte da população brasileira. Adicionalmente, Joy Buolamwini propõe a criação de plataformas que detectem as falhas cometidas pelos sistemas de reconhecimento facial para coletar depoimentos das pessoas a fim de identificar os erros e auditar os *softwares* que os reproduzem¹⁴².

A cientista de dados sugere, ainda, a criação de uma campanha de fotografias frontais para que as pessoas compartilhem imagens de seus rostos com os desenvolvedores dos sistemas a fim de possibilitar a diversidade na IA¹⁴³. Adicionalmente, é importante a criação de grupos de estudos para reconhecer e combater os erros do reconhecimento facial, especialmente na aplicação da legislação penal. O CNJ anunciou, a criação de Grupo de Trabalho para propor “uma regulamentação de diretrizes e procedimentos para o reconhecimento pessoal em

¹⁴⁰ BUOLAMWINI, Joy. *How I'm fighting bias in algorithms*. Ted Talk, 2016. Disponível em: https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms/up-next?referrer=playlist-the_inherent_bias_in_our_tech&language=en. Acesso em: 28 out. 2021.

¹⁴¹ *Ibidem*.

¹⁴² *Ibidem*.

¹⁴³ *Ibidem*.

processos criminais e a sua aplicação no âmbito do Poder Judiciário, com vistas a evitar condenação de pessoas inocentes”¹⁴⁴.

Embora o grupo de trabalho seja específico para tratar do reconhecimento de pessoas por meio de fotografia, sem a utilização de um sistema de reconhecimento facial para detecção de rostos, a adoção de um grupo de trabalho semelhante para implementar uma regulação a fim de combater as prisões por reconhecimento facial tecnológico também contribuiria para uma IA antidiscriminatória.

Ademais, conforme dispõe Sharona Hoffman¹⁴⁵, professora de Direito Sanitário e Bioética da *Case Western Reserve University*, a judicialização do enviesamento algorítmico é capaz de alertar as autoridades a buscarem uma justiça algorítmica. Por fim, embora não tenha se tornado lei nos Estados Unidos, o *Algorithmic Accountability Act* de 2019 traz medidas relevantes a serem seguidas por sistemas de inteligência artificial, a exemplo da determinação de que haja uma avaliação dos riscos que os sistemas possuem de contribuir para “decisões imprecisas, injustas, tendenciosas ou discriminatórias que afetam os indivíduos”¹⁴⁶.

O relatório de impacto previsto se assemelha ao produzido pelo País de Gales e possibilita a discussão acerca dos riscos de discriminação existentes ao utilizar um sistema de reconhecimento facial e integra uma política de transparência da utilização dos sistemas. Ademais, há outra disposição que prevê uma avaliação do impacto de proteção de dados que se destina a estudar qual proteção o sistema processador consegue conferir aos dados tratados no emprego da IA¹⁴⁷. Essas duas propostas também podem ser adotadas a fim de alcançar uma justiça algorítmica.

Em suma, as seguintes medidas podem ser adotadas a fim de combater a reprodução de racismo e discriminações pela inteligência artificial no emprego do reconhecimento facial: a criação de uma regulação eficiente que seja capaz de apresentar transparência aos indivíduos, bem como proteger os direitos individuais; a diversificação de rostos inseridos nas máquinas de IA para treinarem a detecção de rostos com faces de

¹⁴⁴ **Grupo vai aprimorar reconhecimento pessoal em processos criminais.** Agência CNJ de Notícias. Disponível em: <https://www.cnj.jus.br/grupo-vai-aprimorar-reconhecimento-pessoal-em-processos-criminais/>. Acesso em: 28 out. 2021.

¹⁴⁵ HOFFMAN, Sharona. **Biased AI can be bad for your health – here’s how to promote algorithmic fairness.** TheConversation, 9 de março de 2021. Disponível em: <https://theconversation.com/biased-ai-can-be-bad-for-your-health-heres-how-to-promote-algorithmic-fairness-153088>. Acesso em: 28 out. 2021.

¹⁴⁶ Algorithmic Accountability Act of 2019. Disponível em: < <https://www.congress.gov/bill/116th-congress/house-bill/2231/text>>. Acesso em: 28 out. 2021.

¹⁴⁷ *Ibidem*.

diversas etnias e gêneros; a existência de um fórum para que as pessoas relatem as falhas e discriminações dos sistemas; a criação de um grupo de estudo para pesquisar constantemente regulações para se propor sistemas mais justos; a divulgação de relatórios de impacto sobre os vieses algorítmicos e a proteção dos dados dos usuários. Cumpre destacar, por fim, que o combate ao racismo algorítmico deve ter a participação ativa do governo

V. Conclusão

A implementação da inteligência artificial na esfera jurídica é capaz de contribuir para a celeridade da elaboração de contratos, a uniformização de jurisprudência, a criação de controvérsias, a identificação de matérias relevantes, a comparação de processos que versam sobre a mesma temática, dentre outros. Destarte, a fusão de inteligência artificial e direito pode produzir resultados favoráveis, contribuindo para a celeridade processual.

A inteligência artificial também está presente no reconhecimento facial, que tem gerado discussões, conforme fora demonstrado, diante do emprego dos sistemas de RF no âmbito público, tanto para autenticação, a exemplo da entrada em locais públicos, como para identificação de indivíduos com a finalidade de segurança, a exemplo das prisões realizadas a partir da detecção de pessoas procuradas enquanto caminham pelas ruas.

A implementação do RF é problemática em que pese a existência de vieses algorítmicos na inteligência artificial, que é treinada com dados inseridos por humanos, reproduzindo discriminação de gênero, raça e classe, conforme fora demonstrado nos capítulos 1 e 2. Portanto, a discriminação humana é refletida nos algoritmos, o que enseja a necessidade de se pensar em parâmetros antidiscriminatórios.

Tratando-se do reconhecimento facial de mulheres de peles mais escuras, a IA possui taxa de erro de 34,4%, o que ratifica a discriminação contra este grupo da população. Além disso, a estrutura da sociedade brasileira já contribui para práticas racistas por meio do reconhecimento fotográfico, que é utilizado para embasar prisões, ainda que seja a única prova, contrariando o Código de Processo Penal, bem como o entendimento do Superior Tribunal de Justiça. Destarte, o emprego do reconhecimento facial tecnológico contribui para a institucionalização do racismo, que já ocorre pelo sistema penal.

Os efeitos são nefastos, tais como a prisão equivocada de pessoas negras, o não-reconhecimento de pessoas negras pelo RF, a identificação de rostos distintos como sendo o mesmo ou, até mesmo, a não-identificação do mesmo rosto em fotografias distintas. Desse modo, urge a necessidade de elaborar uma regulação específica sobre reconhecimento facial que seja capaz de evitar padrões discriminatórios, além de demonstrar transparência para a população com a divulgação de quais locais possuem videomonitoramento, qual é a finalidade do uso,

quais são as situações em que o RF está autorizado, quais são as medidas de proteção aos direitos individuais, especialmente ao de privacidade.

Nesse sentido, algumas medidas podem ser adotadas para a promoção de uma justiça algorítmica, a exemplo da diversificação de rostos ao treinar as máquinas de reconhecimento facial por meio de *deep learning*. Ademais, a criação de um canal de atendimento para receber depoimentos de violações de direitos ou de falhas cometidas pela IA podem contribuir para verificar quais sistemas necessitam de reparos para melhorar a acurácia. Além disso, a criação de leis que disciplinem a matéria e determinam transparência na implementação e no tratamento de dados são fundamentais. Desse modo, há medidas para implementar o reconhecimento facial de modo seguro para os usuários, sem que haja a necessidade de banir seu uso.

Referências bibliográficas

Addressing the problem of algorithmic bias. Technical Paper. Australian Human Rights Commission, 2020. Disponível em: <https://humanrights.gov.au/our-work/rights-and-freedoms/publications/using-artificial-intelligence-make-decisions-addressing>. Acesso em: 24 out. 2021.

AFONSO, Nathália. **Dia da Consciência Negra: números expõem desigualdade racial no Brasil.** Lupa News, Piauí, 20 de novembro de 2019. Disponível em: <https://piaui.folha.uol.com.br/lupa/2019/11/20/consciencia-negra-numeros-brasil/>. Acesso em: 27 out. 2021.

ANGWIN, Julia. LARSON, Jeff. MATTU Surya. KIRCHNER, Lauren. Machine Bias: there's software used across the country to predict future criminals. And it's biased against blacks. ProPublica, 23 de maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 24 out. 2021.

ASSIS, Alexandre Alfaix de. **Inteligência artificial chegou ao STF com o robô Victor.** TCE-GO, Goiás, 27 de jun. de 2019. Disponível em: <https://portal.tce.go.gov.br/-/inteligencia-artificial-chegou-ao-stf-com-victor>. Acesso em: 23 out. 2021.

Biometria facial, agora, é obrigatória em 100% dos ônibus do DF. Metrôpoles, Brasília, -2 de maio de 2018. Disponível em: <https://www.metropoles.com/distrito-federal/transporte-df/biometria-facial-agora-e-obrigatoria-em-100-dos-onibus-do-df>. Acesso em: 26 out. 2021.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 21, de 03 de fevereiro de 2020. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da inteligência artificial no Brasil, e dá outras providências. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2236340>, Acesso: 19 out. 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.612, de 21 de agosto de 2019.** Dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455>. Acesso em: 27 out. 2021.

BRASIL, Conselho Nacional de Justiça (CNJ). Resolução CNJ nº 332, de 21 de agosto de 2020. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 23 out. 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 9.736, de 07 de março de 2018.** Acrescenta dispositivo à Lei nº 7.210, de 11 de julho de 1984, para incluir a previsão de identificação por reconhecimento facial. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011>. Acesso em: 27 out. 2021.

BRASIL. Conselho Nacional de Justiça (CNJ). Portaria nº 271, de 4 de dezembro de 2021. Disponível em: <<https://atos.cnj.jus.br/atos/detalhar/3613>>. Acesso em: 23 out. 2021.

BUOLAMWINI, Joy. **How I'm fighting bias in algorithms**. Ted Talk, 2016. Disponível em:

https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms/up-next?referrer=playlist-the_inherent_bias_in_our_tech&language=en. Acesso em: 28 out. 2021.

BURTON-HARRIS, Victoria. MAYOR, Philip. **Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart**. American Civil Liberties Union, 24 de junho de 2020. Disponível em: <https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart/>. Acesso em: 24 out. 2021.

Câmara aprova projeto que regulamenta uso da inteligência artificial. Câmara dos Deputados, Brasília, 29 de set. de 2021. Disponível em:

<<https://www.camara.leg.br/noticias/811702-camara-aprova-projeto-que-regulamenta-uso-da-inteligencia-artificial/>>. Acesso em 19 out. 2021.

CENCI, Gabrielle Casagrande. A fundamentação da decisão e a inteligência artificial no Direito Penal. Conjur, 05 de jun. de 2021. Disponível em:

<<https://www.conjur.com.br/2021-jun-05/cenci-fundamentacao-decisao-ia-direito-penal>>. Acesso em 19 out. 2021.

CNJ, Pesquisa revela que 47 tribunais já investem em inteligência artificial. Agência de notícias, publicada em 2 de março de 2021. Disponível em:

<https://www.cnj.jus.br/pesquisa-revela-que-47-tribunais-ja-investem-em-inteligencia-artificial/>. Acesso em: 19 out. 2021.

COELHO, João Victor de Assis Brasil Ribeiro Coelho. **Aplicações e Implicações da Inteligência Artificial no Direito**. Monografia (Graduação em Direito), Faculdade de Direito, Universidade de Brasília. Brasília, p. 11. 2017. Disponível em:

<https://bdm.unb.br/bitstream/10483/18844/1/2017_JoaoVictordeAssisBrasilRibeiroCoelho.pdf>. Acesso em: 18 out. 2021.

DABASS, Joti. **Scope of Artificial Intelligence in Law**. The Northcap University, 2018.

Data Protection Impact Assessment (DPIA). Metropolitan Police. Disponível em:

<https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/data-protection-impact-assessment.pdf?cfchlcaptcha tk =hnyz6pFaqDmKLg3L9Eiqg8ht78HGdyEX.pMRXt14sC4-1635520658-0-gaNycGzNDRE>. Acesso em: 28 out. 2021.

ELIAS, Paulo Sá. **Algoritmos, Inteligência Artificial e Direito**. Conjur. Disponível em: <https://www.conjur.com.br/dl/algoritmos-inteligencia-artificial.pdf>. Acesso em: 18 out. 2021.

Equality Impact Assessment – steps 1 to 7. Metropolitan Police. Disponível em: <https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/data-protection-impact-assessment.pdf>

[g-information/facial-recognition/equality-impact-assessment.pdf](https://www.facial-recognition-equality-impact-assessment.pdf). Acesso em: 28 out. 2021.

FERRARO, Andres; SERRA Xavier; BAUER Christine. **Break the loop: gender imbalance in music recommenders**. CHIIR. Publicado em 14 de março de 2019, Canberra, Austrália. Disponível em: <https://dl.acm.org/doi/10.1145/3406522.3446033>>. Acesso em: 24 out. 2021.

Gender Shades, resultados. Disponível em: <http://gendershades.org/overview.html>. Acesso em 27 out. 2021.

GENERAL, John. SARLIN, Jon. **A false facial recognition match sent this innocent black man to jail**. Cnn Business, 29 de abril de 2021. Disponível em: <https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html>. Acesso em: 24 out. 2021.

Grupo vai aprimorar reconhecimento pessoal em processos criminais. Agência CNJ de Notícias. Disponível em: <https://www.cnj.jus.br/grupo-vai-aprimorar-reconhecimento-pessoal-em-processos-criminais/>. Acesso em: 28 out. 2021.

GUIMARÃES, Hellen. **Nos erros do reconhecimento facial, um “caso isolado” atrás do outro**. Piauí, 24 de setembro de 2021. Disponível em: <https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/>. Acesso em: 27 out. 2021.

FRANCISCO, Pedro Augusto; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais**. Brasil: Instituto Igarapé e Data Privacy Brasil Research, 2020. Disponível em: <https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf>. Acesso em: 26 out. 2021.

FRAZÃO, Ana de Oliveira. **Algoritmos e inteligência artificial. Direito Antitruste 4.0: fronteiras entre concorrência e inovação**. Juliana Oliveira Domingues et al, organizadores. São Paulo: Singular, 2019.

FRAZÃO, Ana. **Discriminação algorítmica: compreendendo o que são os julgamentos algorítmicos e o seu alcance na atualidade**. Conjur, 26 de jun. de 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-16062021>. Acesso em: 23 out. 2021.

FREIRE, Victor. **Reconhecimento facial intensifica segurança nos aeroportos**. Serpro. Disponível em: http://intra.serpro.gov.br/tema/noticias-tema/reconhecimento-facial-intensifica-seguranca-nos-aeroportos/nitf_galleria. Acesso em: 24 out. 2021.

HARWELL, Frew. **Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use**. The Washington Post, 19 de dezembro de 2019. Disponível em: <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>. Acesso em: 24 out. 2021.

HENDLER, James. **Feds are increasing use of facial recognition systems – despite call for a moratorium.** The Conversation. Disponível em: <https://theconversation.com/feds-are-increasing-use-of-facial-recognition-systems-despite-calls-for-a-moratorium-145913>. Acesso em: 26 out. 2021.

HERNANDES, Raphael. **Reconhecimento facial salva vidas, mas cerceia liberdades.** Folha de S. Paulo, São Paulo, 19 de fevereiro de 2020. Disponível em: <https://temas.folha.uol.com.br/inteligencia-artificial/ia-no-mundo-real/reconhecimento-facial-salva-vidas-mas-cerceia-liberdades.shtml>. Acesso em: 26 out. 2021.

HOFFMANN, Alexandra Felipe. **Direito e Tecnologia: a utilização de inteligências artificiais no processo decisório.** Monografia, (Graduação em Direito), Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina (UFSC), Florianópolis, p. 31. 2018. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/192574/TCC_Final.pdf?sequence=1&isAllowed=y. Acesso em: 18 out. 2021.

INFOGRAPHIC: historical bias in AI systems. Australian Human Rights Commission. Disponível em: <https://humanrights.gov.au/about/news/media-releases/infographic-historical-bias-ai-systems>. Acesso em: 24 out. 2021.

Instituto Igarapé. **Reconhecimento Facial no Brasil.** Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 25 out. 2021.

Inteligência Artificial do Facebook rotulou homem negro como primata. Folha de S. Paulo, São Paulo, 4 de setembro de 2021. Disponível em: <https://www1.folha.uol.com.br/mercado/2021/09/inteligencia-artificial-do-facebook-rotulou-homem-negro-como-primata.shtml>. Acesso em: 24 out. 2021.

Inteligência Artificial: tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário Brasileiro. Disponível em: https://ciapi.fgv.br/sites/ciapi.fgv.br/files/estudos_e_pesquisas_ia_1afase.pdf. Acesso em: 23 out. 2021.

JEE, Charlotte. **A biased medical algorithm favored White people for health-care programs.** MIT Technology Review. Disponível em: <https://www.technologyreview.com/2019/10/25/132184/a-biased-medical-algorithm-favored-white-people-for-healthcare-programs/>. Acesso em: 24 out. 2021.

KLOSOWSKI, Thorin. **Facial Recognition Is Everywhere. Here's what we can do about it.** Wirecutter, 15 de julho de 2020. Disponível em: <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>. Acesso em: 24 out. 2021.

LAGE, Fernanda. **Manual de Inteligência Artificial no Direito Brasileiro**, p. 26.1ª ed. Brasília: Juspodivm, 2020.

LawGeex, startup especializada na revisão automática de contratos. Disponível em: https://www.lawgeex.com/?utm_source=google&utm_medium=cpc&utm_campaign=Global_sch_brand&utm_adgroup=27388619163&device=c&placement&utm_term=

[awgeex&qclid=CjwKCAjwsIbpBRBNEiwAZF8-z8l3hvf_jSeNHWPzLnXHX0TqvXRal2ebW8l6BRWZ00Gkiw8Nt8kBoCLg4QAvD_BwE](https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/?_cf_chl_captcha_tk__=9hjbJXb9dLgJtrMQqrLKHfL7eEq4quap.lkgTcQknTE-1635515747-0-gaNycGzNCSU)> Acesso em: 19 out. 2021.

Live Facial Recognition. Metropolitan Police, Advice and Information.

Disponível em: https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/?_cf_chl_captcha_tk__=9hjbJXb9dLgJtrMQqrLKHfL7eEq4quap.lkgTcQknTE-1635515747-0-gaNycGzNCSU. Acesso em: 28 out. 2021.

Machine learning e Deeping learning: aprenda as diferenças. Disponível em:

<<https://www.salesforce.com/br/blog/2018/4/Machine-Learning-e-Deep-Learning-aprenda-as-diferencas.html>>. Acesso em: 18 out. 2021.

MARTINELLI, João Paulo. O erro no reconhecimento do acusado e as prisões injustas. Estadão, 21 de setembro de 2021. Disponível em:

<https://politica.estadao.com.br/blogs/fausto-macedo/o-erro-no-reconhecimento-do-acusado-e-as-prisoas-injustas/>. Acesso em: 27 out. 2021.

MAYBIN, Simon. Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA. BBC News, 31 de outubro de 2016. Disponível em:

<https://www.bbc.com/portuguese/brasil-37677421>. Acesso em: 23 out. 2021.

NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. Revista de Processo, v. 285, pp. 421-447, 2018. Disponível em:

<https://bit.ly/3jsJjwH>. Acesso em: 23 out. 2021.

O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016. p. 27, *apud* Nunes, Dierle; Marques, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. Revista de Processo, v. 285, pp. 421-447, 2018. Disponível em: <https://bit.ly/3jsJjwH>. Acesso em: 23 out. 2021.

PF compra sistema que cruzará dados biométricos de 50 milhões de brasileiros.

Folha de S.Paulo, São Paulo, 7 de julho de 2021. Disponível em: <https://www1.folha.uol.com.br/tec/2021/07/pf-compra-sistema-que-cruzara-dados-biometricos-de-50-milhoes-de-brasileiros.shtml>. Acesso em: 26 out. 2021.

RAVACHE, Guilherme. Algoritmo do Spotify privilegia músicos homens, diz pesquisa. Uol, 06 de maio de 2021. Disponível em:

<https://www.uol.com.br/splash/colunas/guilherme-ravache/2021/05/06/algoritmodo-spotify-privilegia-musicos-homens-diz-pesquisa.htm?cmpid=copiaecola>. Acesso em: 24 out. 2021.

Receita Federal utilizará tecnologia de identificação facial da NEC em 14 aeroportos internacionais do País. NEC. Disponível em:

https://br.nec.com/pt_BR/press/PR/20160409060302_11186.html. Acesso em: 25 out. 2021.

Reconhecimento facial ajuda criança sequestrada a encontrar família após 32 anos. CNN Brasil, 21 de maio de 2021. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/reconhecimento-facial-ajuda-crianca-sequestrada-a-encontrar-familia-apos-32-anos/>. Acesso em: 26 out. 2021.

Reconhecimento facial resolve em segundos enigma que durava 15 anos. Folha de S. Paulo, São Paulo, 23 de junho de 2021. Disponível em: <https://f5.folha.uol.com.br/voceviu/2021/06/pimeyes-resolve-em-segundos-um-enigma-que-durava-15-anos.shtml>. Acesso em: 26 out. 2021

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. Disponível em: <https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/>. Acesso em: 25 out. 2021.

Relatório aponta 90 prisões indevidas após reconhecimento fotográfico; Defensoria do CE discute tema ao vivo. Defensoria Pública Geral do Estado do Ceará. Disponível em: <https://www.defensoria.ce.def.br/noticia/relatorio-aponta-90-prisoos-indevidas-apos-reconhecimento-fotografico-defensoria-do-ce-discute-tema-ao-vivo/>. Acesso em: 27 out. 2021.

Relatório indicam prisões injustas após reconhecimento fotográfico. Conselho Nacional das Defensoras e Defensores Públicos-Gerais. Disponível em: <http://condege.org.br/2021/04/19/relatorios-indicam-prisoos-injustas-apos-reconhecimento-fotografico/>. Acesso em: 27 out. 2021.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: A Modern Approach.** 3ª ed. Berkeley: Universidade da Califórnia, 2017.

Sistema de Reconhecimento facial da PM do RJ falha e mulher é detida por engano. G1, Rio de Janeiro, 11 de julho de 2020. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 24 out. 2021.

SILVA, Tarcízio. **Linha do Tempo do Racismo Algorítmico.** Blog do Tarcízio Silva, 2020. Disponível em: <http://https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo>. Acesso em: 24 out. 2021.

Startup LawGeex. **IA VS. LAWYERS: THE ULTIMATE SHOWDOWN.** Disponível em: <https://www.lawgeex.com/resources/whitepapers/aivslawyer/>. Acesso em: 19 out. 2021.

Statement on principles and prerequisites for the development, evaluation and use of unbiased facial recognition Technologies. AMC U.S. Technology Policy Committee (USTPC). Disponível em: <https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf>. Acesso em: 26 out. 2021.

TEIXEIRA, Isadora. **Biometria facial nos ônibus não reconhece mudança visual de alunos**. Metrôpoles, Brasília, 12 de maio de 2018. Disponível em: <<https://www.metropoles.com/distrito-federal/transporte-df/biometria-facial-nos-onibus-nao-reconhece-mudanca-visual-de-alunos>>. Acesso em: 24 out. 2021.

VALENTINI, Rômulo Soares. **Julgamento por computadores? As novas possibilidades da juscibernética no século XX e suas implicações para o futuro do direito e do trabalho dos juristas**. Tese de doutorado, Faculdade de Direito da Universidade Federal de Minas Gerais, Universidade Federal de Minas Gerais. Belo Horizonte, p. 43. 2017. Disponível em: <<https://repositorio.ufmg.br/handle/1843/BUOS-B5DPSA>>. Acesso em: 18 out. 2021.

VIEIRA, Leonardo Marques. A problemática da inteligência artificial e dos vieses algorítmicos: caso Compas. Brazilian Technology Symposium, 2019. Disponível em: <https://www.lcv.fee.unicamp.br/images/BTSym-19/Papers/090.pdf>. Acesso em: 23 out. 2021.

VITAL, Danilo. **Reconhecimento facial por fotografia não serve para embasar condenação, diz STJ**. Consultor Jurídico, 27 de outubro de 2020. Disponível em: <https://www.conjur.com.br/2020-out-27/reconhecimento-foto-nao-embasar-condenacao-stj>. Acesso em: 27 out. 2021.

YOSHIMINE, Rita. **Biometria facial identifica 2,2 mil fraudes em passe livre do DF**. G1, Distrito Federal, 17 de fev. de 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/biometria-facial-identifica-22-mil-fraudes-em-passe-livre-do-df.ghtml>. Acesso em: 26 out. 2021.