



UNIVERSIDADE DE BRASÍLIA – UnB
FACULDADE DE DIREITO – FD

KAREN MARIA ALVES ALEXANDRE

**A TECNOLOGIA DE RECONHECIMENTO FACIAL COMO MEIO DE
OBTENÇÃO DE PROVA NO ÂMBITO CRIMINAL:**
Uma análise à luz da Suprema Corte dos Estados Unidos

BRASÍLIA
2023

KAREN MARIA ALVES ALEXANDRE

**A TECNOLOGIA DE RECONHECIMENTO FACIAL COMO MEIO DE
OBTENÇÃO DE PROVA NO ÂMBITO CRIMINAL:**

Uma análise à luz da Suprema Corte dos Estados Unidos

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel no Curso de Graduação da Faculdade de Direito da Universidade de Brasília.

Orientador: Prof. Dr. Evandro Charles Piza Duarte

Coorientador: Prof. Me. Pedro Sousa

BRASÍLIA
2023

KAREN MARIA ALVES ALEXANDRE

**A TECNOLOGIA DE RECONHECIMENTO FACIAL COMO MEIO DE
OBTENÇÃO DE PROVA NO ÂMBITO CRIMINAL:**

Uma análise à luz da Suprema Corte dos Estados Unidos

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel no Curso de Graduação da Faculdade de Direito da Universidade de Brasília.

Orientador: Prof. Dr. Evandro Charles Piza Duarte

Coorientador: Prof. Me. Pedro Sousa

Prof. Dr. Evandro Charles Piza Duarte – Orientador
Universidade de Brasília

Prof. Me. Pedro Sousa – Coorientador
Universidade de Brasília

Prof.^a Dr.^a Fernanda de Carvalho Lage – Examinadora
Universidade de Brasília

Prof. Me. Ygor Santos de Santana – Examinador
Universidade de Brasília

Aos **meus pais**, por serem o meu alicerce inabalável;
ao **meu irmão**, por ser minha motivação diária; e ao
meu namorado, por ser meu porto seguro.

Sem vocês, nada disso seria possível.

À **minha avó** – Maria Aparecida – e ao **meu primo** –
Caio – os desafios contados por vocês me despertam
inquietação e motivação no estudo deste tema.

AGRADECIMENTOS

É com lágrimas de alívio, alegria e imensa gratidão que escrevo estes agradecimentos. O desenvolvimento deste trabalho contou com a ajuda de diversas pessoas, dentre as quais agradeço, primeiramente, a Deus por todas as forças inexplicáveis fornecidas nessa batalha.

Aos meus pais – Ricardo e Rosângela – por serem o meu alicerce inabalável ao longo da vida. Seus incentivos e apoios na realização dos meus sonhos, o esforço no fornecimento de um ensino de qualidade, bem como o amor incondicional foram os pilares que sustentaram meu percurso até a conclusão deste trabalho. Graças a tudo isso, agora tenho a oportunidade de me formar na universidade dos meus sonhos e uma das melhores do país. Sou eternamente grata por ser abençoada com pais tão excepcionais.

Ao meu irmão – Kauan Ricardo – por me motivar incessantemente a dar sempre o meu melhor e por ser uma fonte inesgotável de motivação. Cada conquista alcançada é também sua, pois é o seu estímulo que impulsiona minha busca constante pela melhor versão de mim mesma. Tenho imensa gratidão e orgulho por ser sua irmã.

Ao meu amor – Anderson – por toda parceria, paciência e compreensão nesses meses turbulentos de escrita. Por me apoiar, enxugar as minhas lágrimas e me ajudar a ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho. Seu suporte foi fundamental na manutenção do meu equilíbrio emocional e mental ao longo desse desafio. Sou profundamente grata por ter alguém tão incrível ao meu lado.

Ao meu avô Eurípedes e ao meu grande amigo Lucas Mateus, que deixaram o plano terreno no meio dessa minha jornada, mas sempre torceram por meu sucesso. Meu avô que sempre se orgulhou em me chamar de “doutorinha”. E meu amigo Lucas, com quem tive a oportunidade de estudar junto nesses últimos 5 anos, compartilhando risadas, trabalhos, experiências e fofocas. Foi doloroso perdê-los, mas sou muito grata por ter compartilhado diversos momentos maravilhosos com vocês.

À minha psicóloga – Andrea Leastro – por todo o suporte no cuidado e na manutenção da minha saúde mental. Seu compromisso em me ajudar a desenvolver estratégias para lidar com as complexidades da vida foram cruciais para minha evolução.

Aos docentes da Faculdade de Direito da Universidade de Brasília, por todos os ensinamentos. Especialmente ao meu orientador, Evandro Charles Piza Duarte, e ao meu coorientador, Pedro Sousa, por aceitarem conduzir o meu trabalho, pela paciência, pela ajuda e pelos conselhos que guiaram o meu aprendizado e o desenvolvimento deste trabalho.

Aos professores e peritos da matéria de “Perícia: Justiça pela Ciência” – em especial ao Alberto Malta e ao Fábio Esteves –, bem como aos professores Donn Fernando e Evandro Piza, da matéria de “Criminologia e Racismo”, e ao professor Fabiano Hatmann, da matéria de “Inteligência Artificial e Direito”, pois foi a junção dessas matérias que me inspiraram a escrever sobre este tema.

Por fim, agradeço a todos que participaram, direta ou indiretamente, do desenvolvimento deste trabalho – familiares, colegas, professores, fisioterapeutas – seja enriquecendo o meu processo de escrita e aprendizado ou fornecendo apoio físico e mental nessa jornada.

*“O que me preocupa não é o grito dos maus,
mas o silêncio dos bons.”*
(Martin Luther King)

RESUMO

O presente trabalho analisa a utilização da Tecnologia de Reconhecimento Facial como meio de obtenção de prova no âmbito criminal e o debate na Suprema Corte dos Estados Unidos, explorando as implicações jurídicas e sociais geradas pelo uso dessa ferramenta. Para isso, analisa estudos existentes sobre o uso dessa ferramenta no âmbito criminal, bem como a apresentação de casos em que pessoas afrodescendentes foram encarceradas em razão do seu uso. Além disso analisa a jurisprudência atual da Suprema Corte dos Estados Unidos envolvendo possíveis violações da Quarta Emenda em contexto de policiamento, bem com a viabilidade do uso dessa ferramenta como prova de acordo com os fatores de Daubert. A conclusão a que se chega demonstrar que o arcabouço jurídico estadunidense possui diversas lacunas na proteção individual frente ao uso da Tecnologia de Reconhecimento Facial no âmbito criminal. Por fim, é evidente que o racismo estrutural é o principal inimigo existente nesse cenário de diversas violações e discriminações que o uso de uma tecnologia embrionária, enviesada e desregulada está causado em pessoas que sempre estão na mira das forças de segurança.

Palavras-chaves Tecnologia de Reconhecimento Facial; Constitucionalismo Digital; Racismo Algorítmico; Suprema Corte dos Estados Unidos; Forças de Segurança.

ABSTRACT

This work analyzes the use of Facial Recognition Technology as a means of obtaining evidence in the criminal sphere and the debate in the Supreme Court of the United States, exploring the legal and social implications generated using this tool. To do this, it analyzes existing studies on the use of this tool in the criminal context, as well as the presentation of cases in which people of African descent were imprisoned due to its use. Furthermore, it analyzes the current jurisprudence of the Supreme Court of the United States involving possible violations of the Fourth Amendment in the context of policing, as well as the feasibility of using this tool as evidence according to the Daubert Standard. The conclusion reached demonstrates that the North American legal framework has several gaps in individual protection regarding the use of Facial Recognition Technology in the criminal context. Finally, structural racism is the main enemy in this scenario of various violations and discrimination that the use of embryonic, biased, and unregulated technology causes to people who are always in the sights of security forces.

Keywords: Facial Recognition Technology; Digital Constitutionalism; Algorithmic Racism; Supreme Court of the United States; Law enforcement agency.

LISTA DE ILUSTRAÇÕES

Figura 1 – Exemplos de interferências externas à tecnologia de reconhecimento facial.	20
Figura 2 – Relatório de investigação.	35
Figura 3 – Comparação entre o autor do crime (à esquerda) e Michael Oliver (à direita). .	37
Figura 4 – Comparação entre as tatuagens.	37

SUMÁRIO

INTRODUÇÃO	11
1 A TECNOLOGIA DE RECONHECIMENTO FACIAL: FUNDAMENTOS E DESAFIOS.....	13
1.1 A REGULAÇÃO JURÍDICA DO MUNDO DIGITAL.....	14
1.2 DESAFIOS TÉCNICOS E ÉTICOS: PRECONCEITO E DISCRIMINAÇÃO NO RECONHECIMENTO FACIAL	19
1.3 CONCEITO, FUNCIONAMENTO E APLICAÇÕES	27
2 ANALISANDO O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NO ÂMBITO CRIMINAL	31
2.1 TECNOLOGIA E DISCRIMINAÇÃO: CASOS REAIS	33
2.1.1 <i>ROBERT WILLIAMS</i>	33
2.1.2 <i>MICHAEL OLIVER</i>	36
2.1.3 <i>PORCHA WOODRUFF</i>	38
2.2 O DEBATE NA SUPREMA CORTE DOS ESTADOS UNIDOS	39
2.2.1 <i>A SUPREMA CORTE E A QUARTA EMENDA</i>	40
2.2.2 <i>A TECNOLOGIA DE RECONHECIMENTO FACIAL COMO EVIDÊNCIA</i>	47
2.3. A REGULAMENTAÇÃO DA TECNOLOGIA DE RECONHECIMENTO FACIAL.....	52
CONCLUSÃO	57
REFERÊNCIAS BIBLIOGRÁFICAS	59

INTRODUÇÃO

O “Olho de Deus”, este é o nome dado a uma ferramenta capaz de hackear qualquer tipo de dispositivo que contenha uma câmera e, a partir disso, tem a habilidade de rastrear a face de qualquer pessoa, em qualquer lugar do mundo, em tempo real.

Essa é a descrição do *software* retratado no filme “Velozes e Furiosos 7” e, apesar de parecer um cenário existente apenas em filmes de ficção científica, a Inteligência Artificial e mais precisamente a Tecnologia de Reconhecimento Facial estão presentes em nosso cotidiano, sendo utilizada em uma variedade de aplicações, desde o desbloqueio de smartphones até desdobramentos relacionados à segurança pública.

No entanto, apesar dos benefícios, essa inovação tecnológica traz consigo um conjunto de questionamentos e angústias relacionados aos direitos fundamentais na era digital, isso porque estudos apontam que essa ferramenta possui maiores taxas de erro quando utilizadas para identificar indivíduos de cor.¹ Dessa forma, o receio de prisões equivocadas e buscas infundadas sem a ciência de que a evidência que os incriminou tenha sido produzida por uma máquina possivelmente enviesada e com uso não regulamentado são algumas das preocupações que orbitam essa tecnologia.

É nesse cenário de incertezas e ausência de regulação que o presente trabalho se desenvolve, sendo o seu tema a utilização da Tecnologia de Reconhecimento Facial como meio de obtenção de prova no processo penal e o debate na Suprema Corte dos Estados Unidos, explorando as implicações jurídicas e sociais geradas pelo uso dessa ferramenta. Para a realização do presente Trabalho de Conclusão de Curso, será utilizado o método dedutivo, com análise qualitativa, mediante pesquisa bibliográfica e jurisprudencial.

O objetivo inicial do trabalho era analisar se a Suprema Corte dos Estados Unidos já havia se debruçado sobre o tema, no entanto, até o momento presente, não há um precedente na Corte referente à Tecnologia de Reconhecimento Facial e prisões equivocadas, em grande parte devido à dispersão dos casos e não há indícios de que a tecnologia de reconhecimento facial tenha sido apresentada como evidência em algum julgamento (Ferguson, 2021, p. 1193; Haddad, 2021, p. 902)².

¹ Estudos serão mostrados na seção 1.2.

² Segundo Ferguson (2021, p.1193), “os direitos da Quarta Emenda são decididos em situações isoladas onde erros sistêmicos ou estruturais não são apresentados. O resultado é que, em casos criminais, violações constitucionais sistemáticas não são litigadas e, portanto, não são vistas pelos tribunais. Essa prática esconde erros sistêmicos e permite uma compreensão menos holística da má conduta policial.”

Entretanto, com base nos entendimentos já formados pela Suprema Corte em casos envolvendo possíveis violações da Quarta Emenda³ em contexto de policiamento, será possível delinear considerações sobre o que é viável manter ou não em futuros litígios em que a Tecnologia de Reconhecimento Facial seja utilizada como prova em contexto criminal.

Além disso, escolher os Estados Unidos como foco deste estudo oferece uma abordagem estratégica e abrangente. Isso porque o país é conhecido por ser líder em inovação tecnológica, abrigando algumas das principais empresas do setor, sendo pioneiro no desenvolvimento e na implementação de tecnologias de reconhecimento facial em diversos setores. Analisar a adoção e a (des)regulação dessa tecnologia nos Estados Unidos proporciona uma compreensão aprofundada das implicações éticas, legais e sociais associadas ao seu uso.

Diante desse contexto, com o intuito de contribuir para o aprofundamento da discussão, o Capítulo 1 apresentará inicialmente o Constitucionalismo Digital, um campo de estudo cujo objetivo principal é analisar as interações entre as normas constitucionais, os direitos individuais e as tecnologias digitais. Em seguida, apresentará os vieses raciais que cercam essa inovação tecnológica – sendo alvos desse campo de estudo. Por fim, abordará conceitos introdutórios relativos à Tecnologia de Reconhecimento Facial, fornecendo uma síntese do seu funcionamento e suas aplicações no âmbito da segurança pública.

Diante dessa exposição teórica, é necessária a compreensão da real dimensão do impacto do uso desregulado da Tecnologia de Reconhecimento Facial no âmbito criminal. Dessa forma, o Capítulo 2 apresentará 3 (três) casos reais em que pessoas afro-estadunidenses foram encarceradas em decorrência de erro no reconhecimento em razão da existência de vieses raciais no *software* utilizado. Em seguida, apontará a jurisprudência disponível da Suprema Corte dos Estados Unidos sobre o tema e a viabilidade do uso dessa tecnologia como prova de acordo com os Fatores de Daubert⁴.

Por fim, de maneira breve, serão expostas algumas recomendações para produções legislativas, com base nos estudos de Andrew Ferguson (2021) e Gabrielle Haddad (2021) – os quais serão basilares para o desenvolvimento deste trabalho – na tentativa de orientar o uso responsável da Tecnologia de Reconhecimento Facial pelas forças de segurança.

³ Esse preceito constitucional busca proteger os cidadãos estadunidenses contra possíveis abusos em policiamento como será detalhado na seção 2.2.1.

⁴ Entendimento da Corte que visa verificar a possibilidade do uso de determinado método ou teoria como evidência. Será mostrado na seção 2.2.2.

1 A TECNOLOGIA DE RECONHECIMENTO FACIAL: FUNDAMENTOS E DESAFIOS

À medida que o mundo digital se expande e se aperfeiçoa, inúmeras transformações surgem dando origem a uma multiplicidade de desafios e oportunidades para o progresso da sociedade contemporânea e suas instituições jurídicas. Com a Tecnologia de Reconhecimento Facial não é diferente, uma vez que essa inovação vem se tornando cada vez mais presente em nossas vidas sendo utilizada em uma variedade de aplicações, desde o desbloqueio de smartphones até desdobramentos relacionados à segurança pública.

A título de exemplo, estudiosos do Centro de Direito e Tecnologia de Privacidade de Georgetown estimam que mais de 117 milhões de cidadãos estadunidenses são afetados pela Tecnologia de Reconhecimento Facial empregada por forças de segurança, sendo que aproximadamente metade dos adultos têm suas fotografias pesquisadas por meio desse método (Garvie *et al.*, 2016, p. 1).

Além disso,

- Pelo menos um em cada quatro departamentos de polícia estaduais ou locais tem a opção de realizar pesquisas de reconhecimento facial por meio do sistema de sua própria agência ou de outra agência.
- Pelo menos 26 estados (e potencialmente até 30) permitem que as autoridades realizem ou solicitem buscas em seus bancos de dados de carteiras de motorista e fotos de identidade (Garvie *et al.*, 2016, p. 2).⁵

A preocupação se intensifica quando se percebe que não há regulação por parte dos estados estadunidenses acerca do uso desse tipo de ferramenta, que pode ser bem menos precisa para aqueles que possuem maiores chances de serem afetados por ela em contexto investigativo, que são pessoas não-brancas.⁶

Diante desse contexto, com o intuito de contribuir para o aprofundamento da discussão, o presente capítulo apresentará inicialmente o campo de estudo cujo objetivo principal é analisar as complexas interações entre as normas constitucionais, os direitos individuais e as tecnologias digitais. Em seguida, apresentará um dos alvos desse campo de estudo: os vieses raciais que cercam essa inovação tecnológica. Por fim, abordará conceitos introdutórios

⁵ Tradução nossa. No original: “At least one out of four state or local police departments has the option to run face recognition searches through their or another agency’s system. At least 26 states (and potentially as many as 30) allow law enforcement to run or request searches against their databases of driver’s license and ID photos.”

⁶ Este assunto será detalhado de forma mais adequada no tópico 1.2. deste capítulo.

relativos à Tecnologia de Reconhecimento Facial, fornecendo uma síntese do seu funcionamento e suas aplicações no âmbito da segurança pública.

1.1 A REGULAÇÃO JURÍDICA DO MUNDO DIGITAL

Consoante Edoardo Celeste (2019, p. 3-4), a tecnologia vem possibilitando a ampliação do exercício de direitos fundamentais (como os relacionados à informação e à liberdade de expressão) e até mesmo possibilitando a criação de certos direitos (como direito à internet). No entanto, por outro lado, também criou e ampliou ameaças a eles. Além disso, deu poder de intervenção a entes não-estatais, como empresas detentoras e criadoras dessas tecnologias, roubando o papel regulador de entes constitucionais tradicionais, como o próprio Estado.

Nessa situação, é evidente a eclosão de um conjunto de questionamentos e angústias relacionados aos direitos fundamentais na era digital. A título de ilustração, podemos citar o receio de prisões equivocadas e buscas infundadas, além da condenação de inocentes sem a ciência de que a evidência que os incriminou tenha sido produzida por uma máquina possivelmente enviesada e com uso não regulamentado.

Essa universalidade de embaraços e oportunidades provoca alterações significativas no equilíbrio constitucional vigente. Isso significa uma perturbação no cenário ideal delineado pelas normas constitucionais de um determinado sistema jurídico na garantia da salvaguarda de direitos fundamentais e no equilíbrio dos poderes instituídos, fazendo com que o sistema crie uma série de respostas normativas (Celeste, 2019, p. 3).

A regulação jurídica de novidades tecnológicas não é um objeto de estudo que apareceu recentemente. Nas últimas décadas, termos como “Constitucionalismo Informacional”, de Brian Fitzgerald (1999)⁷, e “Constitucionalismo Constitutivo”, de Paul Berman (2000)⁸, já surgiam na tentativa de fornecer ideais e princípios para orientar a produção de respostas normativas às alterações do equilíbrio constitucional. Seja, segundo Fitzgerald, reconhecendo o poder compartilhado entre atores públicos e privados nesse ciberespaço e utilizando o Direito

⁷ FITZGERALD, Brian. Software as Discourse? A Constitutionalism for Information Society. **Alternative Law Journal**, v. 24, n. 3, p. 144-149, 1999. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/alterlj24&div=37&id=&page=>. Acesso em: 12 out. 2023.

⁸ BERMAN, Paul Schiff. Cyberspace and the State Action Debate: the cultural value of applying constitutional norms to 'private' regulation. **University of Colorado Law Review**, v. 71, n. 4, 2000. Disponível em: <https://ssrn.com/abstract=228466>. Acesso em: 12 out. 2023.

Privado como um freio do poder dos atores privados, ou, de maneira diametralmente oposta, propondo a sujeição de atores privados ao Direito Constitucional, conforme disposto por Berman (Celeste, 2019, p. 6-7).

No entanto, o termo “Constitucionalismo Digital”, o qual será basilar para o desenvolvimento deste trabalho, surge como um campo de estudo que o objetivo principal é analisar as complexas interações entre as normas constitucionais, os direitos individuais e as tecnologias digitais, além de fornecer um conjunto de ideias para a criação de respostas normativas às inovações tecnológicas.

Esse termo foi desenvolvido por Nicolas Suzor em sua tese de doutorado “*Digital constitutionalism and the role of the rule of law in the governance of virtual communities*”⁹. Ao propor um novo quadro conceitual para a regulação de redes sociais e comunidades virtuais, adotou uma posição intermediária entre Fitzgerald e Berman ao reconhecer simultaneamente o papel constitucionalizador desempenhado pelo Direito Privado e a função orientadora e informativa do Direito Constitucional (Celeste, 2019, p. 7-8).

Para autores como Suzor, é inquestionável o papel de agente regulador desempenhado paulatinamente por atores privados em ambientes virtuais – como as plataformas digitais com seus termos de uso. Assim, uma perspectiva constitucional seria importante para a definição de limites necessários e apropriados para os poderes desses agentes privados, cunhando, portanto, o termo “Constitucionalismo Digital”.

Diante disso, o papel constitucionalizador desempenhado pelo Direito Privado pode ser entendido através dos Termos de Uso das Plataformas Digitais, como o Facebook, que são objeto de estudo do trabalho de Suzor¹⁰. Para ele, os Termos de Uso são contratos e, conseqüentemente, as limitações a esse contrato devem ser ditadas pelo Direito Privado. Assim, a autorregulação feita pelas plataformas digitais por meios desses contratos se torna legítima a partir do consentimento do usuário e, para que nenhum excesso seja cometido, o Direito Privado atuará como limitador (Celeste, 2019, p. 7-8).

Já a função orientadora e informativa do Direito Constitucional torna-se importante na determinação de até onde a autorregulação dos atores privados pode chegar sem ferir valores estabelecidos pelo Estado. Além disso, possui o dever de informar e liderar o desenvolvimento

⁹ Disponível em: https://eprints.qut.edu.au/37636/1/Nicolas_Suzor_Thesis.pdf. Acesso em: 12 out. 2023.

¹⁰ SUZOR, Nicolas Pierre. Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms. **Social Media and Society**, v. 4, n. 3, p. 1-11, 2018. Disponível em: <https://eprints.qut.edu.au/120050/1/N.Suzor%20article.pdf>. Acesso em: 12 out. 2023.

do Direito Contratual, devendo os princípios basilares serem observados e adotados na regulação privada (Celeste, 2019, p. 7-8).

Por outro lado, autores como Redeker, Gill e Gasser (2018) entendem que o Constitucionalismo Digital se refere não só à limitação do poder de entes privados, mas também à limitação do poder de entes públicos. Isso porque “na atual economia política da Internet, tanto os estados quanto às empresas privadas podem limitar ou contribuir para a realização dos direitos digitais percebidos” (Redeker, Gill e Gasser, 2018, p. 304 *apud* Celeste, 2019, p. 10)¹¹.

Contudo, considerando o amplo leque conceitual observado, com divergentes definições entre si¹² e a persistência de penumbras sobre certos pontos¹³, Edoardo Celeste (2019)¹⁴, ao revisar a literatura existente, propõe uma abordagem mais abrangente a respeito desse fenômeno, a qual será adotada no presente trabalho, e busca elucidar questões não esclarecidas anteriormente.

Segundo Celeste, o Constitucionalismo Digital é uma nova vertente do Constitucionalismo Contemporâneo, o qual “gira em torno da ideia de limitar o poder do governo e inclui, entre os seus valores fundamentais, a democracia, a proteção dos direitos humanos e o Estado de Direito” (2019, p. 12).¹⁵ Dessa forma, o Constitucionalismo Digital também compartilha esses valores e objetivos, mas os direcionam para o ciberespaço.

Nesse contexto, o Constitucionalismo Digital pode ser interpretado como uma ideologia, ou seja, como sendo um conjunto de ideias, princípios e valores com o propósito de estabelecer e garantir a existência de um conjunto de normas para a proteção dos direitos fundamentais e a manutenção de um equilíbrio de poderes no espaço digital. Tais concepções permeiam, orientam e influenciam o processo de constitucionalização do ambiente digital, servindo como base no desenvolvimento de produção legislativa (Celeste, 2019, p. 12-14).

O uso do termo como ideologia serve para pensarmos no constitucionalismo como um termo puramente teórico, distinguindo-o da sua implementação, ou seja, da

¹¹ Tradução nossa. No original: “[i]n today’s political economy of the Internet, states and private corporations alike can either limit or contribute to the realization of perceived digital rights.”

¹² Os pontos controvertidos são sobre: o alcance do constitucionalismo digital (não há consenso sobre qual ente deve ser regulado, se deve limitar somente o poder privado ou também o poder público); e sobre que ferramenta utilizar para implementar os valores e ideias do constitucionalismo digital (alguns autores entendem pela utilização do Direito Constitucional, outros pelo Direito Privado e outro pela autorregulação dos agentes privados).

¹³ A diferença entre “constitucionalismo” e “constitucionalização” não é bem explicada por autores anteriores.

¹⁴ CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. **International Review of Law, Computers & Technology**, v. 33, n. 1, p. 76-99, 2019. Disponível em: <https://www.tandfonline.com/action/showCitFormats?doi=10.1080%2F13600869.2019.1562604>. Acesso em: 5 set. 2023.

¹⁵ Tradução nossa. No original: “[...] rotates around the idea of limiting the power of government, and includes, among its foundational values, democracy, the protection of human rights and the rule of law.”

constitucionalização, a qual se traduz no processo de criação de normas, que envolve não somente a codificação de normas, mas também o processo de “discussão e elaboração de novos princípios constitucionais em nível social” (Celeste, 2019, p. 17)¹⁶. Na conjuntura atual, pode ser traduzido na produção de diversas respostas normativas na tentativa de enfrentar as perturbações ao equilíbrio constitucional vigente ocasionadas pelo advento da tecnologia digital.

O processo de constitucionalização do ambiente digital pode ocorrer em nível nacional, realizado por institutos tradicionais de elaboração de normas do Estado – a Lei Geral de Proteção de Dados Pessoais (LGPD) é um exemplo – ou mediante outros órgãos – como decisões tomadas pelos tribunais ou instrumentos legislativos hierarquicamente inferiores, como as resoluções. Saindo da dimensão estatal, entidades privadas também podem criar mecanismos de controle, ainda que não possuam caráter vinculativo. Um exemplo, são os “contratos” estudados por Suzor, ou seja, os Termos de Uso e de Serviço das plataformas digitais (Celeste, 2019, p. 14-15).

A título de ilustração, como uma parte do processo de constitucionalização, é possível citar a proibição do uso de suas tecnologias de reconhecimento facial feita pela Amazon, Microsoft e IBM. Tendo em vista a pressão popular resultante do assassinato de George Floyd, em junho de 2020, a Amazon proibiu por um ano o uso de seu *software* de reconhecimento facial pelas forças policiais estadunidenses. A Microsoft também adotou a mesma postura, afirmando que não fornecerá seu *software* à polícia até a criação de uma lei nacional centrada na proteção dos direitos humanos. Enquanto isso, de maneira mais extrema, a IBM saiu completamente do ramo.^{17 18}

¹⁶ Tradução nossa. No original: “Such a process, in contrast to what some scholars affirm, does not exclusively involve a formal institutionalisation or codification of norms in binding legal texts. It is a broader process, which starts from the phase of discussion and elaboration of new constitutional principles at societal level.”

¹⁷ Notícia publicada pela CNBC, em 14 de junho de 2021, com o seguinte título: “Rules around facial recognition and policing remain blurry”. Disponível em: <https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html>. Acesso em: 9 out. 2023.

¹⁸ É importante ressaltar que a Microsoft e a IBM são as empresas em que os sistemas de reconhecimento facial tiveram as piores taxas de precisão na identificação de pessoas não-brancas na pesquisa realizada pelas cientistas Joy Buolamwini e Timnit Gebru (*Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 2018), a qual será exposta na seção seguinte.

Para finalizar, um outro exemplo ocorreu em setembro deste ano (2023) em que o governador da Califórnia assinou uma ordem executiva¹⁹ (*Executive Order N-12-23*)²⁰ com o objetivo de regulamentar o uso da IA. No documento, há diversas determinações no sentido de orientar agências estatais a analisarem possíveis impactos e ameaças a populações mais vulneráveis. Além disso, estabelece prazos definidos até o ano de 2024 com o objetivo de elaborar diretrizes concretas e factíveis que irão guiar o desenvolvimento futuro da IA. Tal iniciativa muito provavelmente impulsionará outros agentes – públicos e privados – a buscarem a normatização do uso dessa tecnologia, gerando, portanto, novos regulamentos e princípios que guiarão a tecnologia na Califórnia e possivelmente em todo território estadunidense.²¹

Providências como essas estão sendo adotadas em razão da aplicação indiscriminada da Tecnologia de Reconhecimento Facial, a qual pode levar a uma intrusão massiva na vida privada dos cidadãos, bem como à possibilidade de discriminação racial, étnica e de gênero. Além disso, a falta de regulamentação pode permitir o uso inadequado da tecnologia por parte de autoridades governamentais e entidades privadas, comprometendo a segurança e a liberdade dos cidadãos.

Portanto, estabelecer diretrizes e regulamentos claros para a utilização do reconhecimento facial é crucial para equilibrar a inovação tecnológica com a proteção dos direitos e liberdades individuais, garantindo transparência e respeito pelas normas éticas na implementação dessa tecnologia. Diante desse contexto, o Constitucionalismo Digital se revela como um pilar fundamental no combate às novas formas de ameaças aos direitos fundamentais como, por exemplo, o racismo algorítmico, o qual vem se mostrando como o principal desafio da Tecnologia de Reconhecimento Facial.

Em consideração ao exposto, como uma maneira de demonstrar a necessidade de respostas normativas eficazes, a seção seguinte cuidará de apresentar fatores externos e internos à Tecnologia de Reconhecimento Facial que possuem o potencial de influenciar os resultados

¹⁹Uma ordem executiva assemelha-se a medida provisória no ordenamento jurídico brasileiro. É uma declaração do presidente ou do governador que tem força de lei e que não necessita de qualquer ação do Congresso. (Cornell Law School, *n.d., n.p.*).

WEX DEFINITIONS TEAM. Cornell Law School. Executive Order. **Legal Information Institute**, 12 jun. 2021. Disponível em: https://www.law.cornell.edu/wex/executive_order#:~:text=An%20executive%20order%20is%20defined,the%20legislature%20cannot%20overturn%20it>. Acesso em: 18 out. 2023.

²⁰ Disponível em: <https://www.gov.ca.gov/wp-content/uploads/2023/09/AI-EO-No.12--GGN-Signed.pdf>. Acesso em: 12 out. 2023.

²¹Notícia publicada por Brookings, em 12 de setembro de 2023, com o seguinte título: “California charts the future of AI.” Disponível em: <https://www.brookings.edu/articles/california-charts-the-future-of-ai/>. Acesso em: 12 out. 2023.

de maneira discriminatória, de modo que o racismo (estrutural) algoritmo é o reflexo de um deles.

1.2 DESAFIOS TÉCNICOS E ÉTICOS: PRECONCEITO E DISCRIMINAÇÃO NO RECONHECIMENTO FACIAL

Conforme salientado por Shang-Hung Lin (2000, p. 3)²², “um rosto humano não é um objeto 3D, e também não é um corpo rígido”. Dessa forma, há fatores externos que podem interferir de maneira significativa no processo de reconhecimento facial, de modo que o autor elenca seis principais.

O primeiro diz respeito à qualidade da câmera de captura de imagem e as interferências que podem ocorrer como distorções e ruídos alterando a qualidade das fotografias geradas. Como segundo fator, temos a complexidade da paisagem de fundo, isto é, quanto mais elementos ao fundo da imagem, maior a possibilidade de o sistema cometer erros. Já o terceiro influenciador é a iluminação, ou seja, caso a fotografia seja feita em drásticas condições de iluminação, pode influenciar nos dados obtidos (Lin, 2020, p. 3-4).

Os demais fatores estão relacionados ao posicionamento do rosto em si, como a variação rotacional e dimensional do rosto, isto é, se o rosto está de lado ou de frente, apontado para cima ou para baixo, ou seja, se há algum elemento que prejudique a visualização completa da face. As expressões faciais também influenciam, isso porque um rosto sorrindo e um triste são completamente diferentes para a máquina. Por fim, maquiagem e estilo de cabelo também são considerados como influenciadores, mas, para o autor, são os que interferem de maneira menos significativa (Lin, 2000, p. 3-4)

A Figura 1 ilustra como alguns desses fatores interferem no funcionamento dessa tecnologia. Na seleção A, encontramos o desafio da variação rotacional do rosto, uma vez que este se encontra de lado. Na seleção B, verificamos problemas relacionados à qualidade da imagem, tendo em vista que o rosto se encontra desfocado. Na seleção C, verificamos a existência de um elemento que prejudica a visualização completa da face. Por fim, identificamos o problema da complexidade da paisagem de fundo na seleção D em que a máquina identifica erroneamente um objeto de fundo como sendo um rosto (Buolamwini *et al*,

²² Tradução nossa. No original: “A human face is not only a 3-D object, it is also a non-rigid body.”

2020, p. 4). Além disso, cabe pontuar que o rosto mais à frente da seleção B e C não foi identificado pelo *software*.

Figura 1 – Exemplos de interferências externas à tecnologia de reconhecimento facial.



Fonte: Facial Recognition Technologies: A Primer (2020).

Perceba que, quando pensamos em um contexto de investigação criminal, as imagens obtidas para identificação ou rastreamento facial²³ de suspeitos muito possivelmente estarão enfrentando a maioria dessas interferências. Isso porque as fotos obtidas não são tiradas nas melhores condições de tempo, espaço e iluminação, além da utilização de artifícios pelos indivíduos para dificultar o reconhecimento como bonés ou máscaras.

Para além desses influenciadores extrínsecos, há também influenciadores intrínsecos a Tecnologia de Reconhecimento Facial, ou seja, aqueles que ocorrem no momento de criação ou treinamento do algoritmo, fazendo com que ele absorva e replique padrões discriminatórios existentes na sociedade como se fossem uma “verdade objetiva” (Mendes e Mattiuzzo, 2019, p. 3).

Segundo Jasmine Wright e Andrej Verity (2020, p. 12), questões como a insuficiência dos bancos de dados, o próprio funcionamento da tecnologia biométrica e o enraizamento da cultura ocidental nos sistemas são fatores que contribuem para que diferentes formas de preconceito ocorram em sistemas de IA. Conforme será explicado melhor na seção seguinte, a Tecnologia de Reconhecimento Facial necessita de um amplo fornecimento de dados para o seu aprendizado. Dessa forma, uma deficiência nesse conjunto pode comprometer

²³ Esses termos serão abordados de maneira mais detalhada na seção 1.3.

significativamente os resultados, fazendo com que os algoritmos repliquem apenas uma parte da sociedade e não a sociedade como um todo. Em outros termos,

[...] os modelos algorítmicos podem ser tendenciosos porque os modelos são representações da realidade, em vez da própria realidade. É como o ser humano que desenvolveu o modelo vê a realidade, portanto, a fonte dos dados, a proporcionalidade dos grupos dentro dos dados e as variáveis escolhidas podem ser influenciadas por preconceitos, mesmo que seja não intencional (Wright e Verity, 2020, p. 16).²⁴.

Diante disso, com o objetivo de analisar a existência de resultados enviesados gerados por algoritmos de reconhecimento facial, Joy Buolamwini e Timnit Gebru (2018), em seu estudo “*Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*”, analisaram três sistemas de reconhecimento facial e classificação de gênero (Microsoft, IBM e Face++). A preocupação por trás da pesquisa consiste no fato de que os *softwares* de reconhecimento facial cada vez mais vêm sendo utilizados por forças policiais estadunidenses na identificação de suspeitos.

No estudo, foram utilizados os termos “masculino” e “feminino” para definir a classe de gênero.²⁵ Não foram utilizados rótulos de raça e etnia, uma vez que essa rotulagem fenotípica pode variar profundamente.²⁶ Em vez disso, foi utilizado o tipo de pele de acordo com o sistema de seis pontos de Fitzpatrick, o mesmo utilizado por dermatologistas na classificação da pele e determinação do risco de câncer de pele (Buolamwini e Gebru, 2018, p. 5).

Diante desses filtros, foram selecionados 1.270 parlamentares de três países africanos (Ruanda, Senegal, África do Sul) e três países europeus (Islândia, Finlândia, Suécia). O resultado obtido mostrou que o grupo com maior taxa de erro no reconhecimento (34,7%) é o de mulheres com pele mais escura e, por outro lado, o grupo com menor taxa de erro (0,8%) é o de homens brancos (Buolamwini e Gebru, 2018, p. 5-8).

Além disso, no geral, os principais resultados obtidos foram:

²⁴ Tradução nossa. No original: “[...] algorithmic models can be biased because models are representations of reality rather than reality itself. It is how the human who developed the model views reality, so the source of the data, the proportionality of groups within the data, and the variables chosen could be influenced by bias, even if it is unintentional.”

²⁵ Tendo em vista que os sistemas de classificação analisados usam rótulos binários, foram utilizados esses termos identificando sujeitos percebidos como homens ou mulheres, respectivamente.

²⁶ Esses etiquetamentos são variáveis dentro da própria categoria racial ou étnica e também a depender da região geográfica, “até mesmo dentro dos países, essas categorias mudam ao longo do tempo” (Buolamwini e Gebru, 2018, p. 4, tradução nossa). Diante dessa instabilidade, as pesquisadoras utilizaram o tipo de pele como rótulo uma vez que “o tipo de pele é um atributo fenotípico que pode ser usado para caracterizar conjuntos de dados de forma mais objetiva, juntamente com formas de olhos e narizes” (*idem, ibidem*, tradução nossa).

- Todos os classificadores têm melhor desempenho em rostos masculinos do que em rostos femininos (diferença de 8,1% a 20,6% na taxa de erro)
- Todos os classificadores têm melhor desempenho em rostos mais claros do que em rostos mais escuros (diferença de 11,8% a 19,2% na taxa de erro)
- Todos os classificadores têm o pior desempenho em rostos femininos mais escuros (taxa de erro de 20,8% a 34,7%)
- Os classificadores da Microsoft e da IBM têm melhor desempenho em rostos masculinos mais claros (taxas de erro de 0,0% e 0,3%, respectivamente)
- Os classificadores da Face++ têm melhor desempenho em rostos masculinos mais escuros (taxa de erro de 0,7%)
- A diferença máxima na taxa de erro entre os grupos mais bem classificados e os piores classificados é de 34,4% (Buolamwini e Gebru, 2018, p. 8).²⁷

Ao final da pesquisa, Buolamwini e Gebru concluíram que:

A pele mais escura por si só pode não ser totalmente responsável pela classificação incorreta. Em vez disso, a pele mais escura pode estar altamente correlacionada com geometrias faciais ou normas de exibição de gênero que foram menos representadas nos dados de treinamento dos classificadores avaliados (2018, p. 10).²⁸

Outro estudo que mostra o enviesamento algorítmico foi o desenvolvido por Augusto Jobim do Amaral, Fernanda Martins e Ana Clara Elesbão (2021), descrito no artigo “Racismo algorítmico: uma análise da branquitude nos bancos de imagens digitais”, o qual buscou analisar como os algoritmos em bancos de imagens têm sido utilizados como métodos de categorização e classificação social e como são capazes de produzir resultados racistas. Para tanto, a pesquisa analisou os resultados obtidos ao buscar a palavra “*family*” em três bancos de imagens (*Getty Images, Shutterstock, e Stock Photos*) para verificar como os resultados obtidos a partir de palavras-chave genéricas são racializados algorítmicamente.

A conclusão foi de que os conteúdos resultantes da busca costumam ser racializados colocando em lugar de destaque famílias brancas, reduzindo a multiplicidade étnica de famílias existentes, traduzindo a branquitude e a ocidentalidade como sinônimo de universalidade. Ainda que alguns bancos de imagens fornecessem filtros étnicos, não houve qualquer alteração significativa, mostrando famílias – ainda que não-brancas – inseridas no padrão ocidental (Amaral, Martins e Elesbão, 2021, p. 16-17).

²⁷ Tradução nossa. No original: “All classifiers perform better on male faces than female faces (8.1% – 20.6% difference in error rate) • All classifiers perform better on lighter faces than darker faces (11.8% – 19.2% difference in error rate) • All classifiers perform worst on darker female faces (20.8% – 34.7% error rate) • Microsoft and IBM classifiers perform best on lighter male faces (error rates of 0.0% and 0.3% respectively) • Face++ classifiers perform best on darker male faces (0.7% error rate) • The maximum difference in error rate between the best and worst classified groups is 34.4%.”

²⁸ Tradução nossa. No original: “[...] darker skin alone may not be fully responsible for misclassification. Instead, darker skin may be highly correlated with facial geometries or gender display norms that were less represented in the training data of the evaluated classifiers.”

Tais ineficiências podem ser atribuídas à falta de diversidade de imagens empregadas no treinamento dos algoritmos, que predominantemente contêm representações de homens brancos, uma figura amplamente dominante no campo dos desenvolvedores de IA (Wright e Verity, 2020, p. 14). Além disso, essas falhas também são produtos de vieses enraizados nos dados de treinamento, provenientes do próprio preconceito humano, perpetuando estereótipos relacionados à raça, gênero e outras formas de discriminação.

Essa problemática ganha outra dimensão pela existência das chamadas "caixas-pretas" nos sistemas de IA, que se caracterizam pela dificuldade em saber como o sistema chegou àquele resultado específico à medida em que o aprendizado do sistema progride (Wright e Verity, 2020, p. 15).

Analisando as caixas-pretas, Frank Pasquale (2015, p. 3) nos mostra que esse termo funciona como uma metáfora pelo seu duplo sentido. De um lado podemos relacionar com as caixas-pretas comumente atribuídas aos dispositivos presentes em aeronaves que servem para guardar gravações, sistemas de monitoramento de dados, registros importantes sobre os voos.

Entretanto, por outro lado,

[...] pode significar um sistema cujo funcionamento é misterioso; podemos observar suas entradas e saídas, mas não podemos dizer como uma se transforma na outra. Enfrentamos esses dois significados diariamente: monitorados cada vez mais de perto pelas empresas e pelo governo, não temos uma ideia clara de até onde essa informação pode viajar, como ela é usada ou suas consequências (Pasquale, 2015, p. 3).²⁹

A obscuridade intrínseca ao processo de reconhecimento facial evoca vividamente a imagem da Máquina de Vidro descrita no conto de Franz Kafka. Segundo os estudiosos Evandro Piza Duarte e Rafael de Deus Garcia (2021), a Máquina de Vidro³⁰, um mecanismo de punição da colônia descrita no conto, apresenta um contraste entre o novo e o antigo, isso porque o vidro (tecnologia nova da época) fornece um ar de transparência, enquanto contrasta com a obscuridade do processo de decisão, visto que a sentença não era enunciada, pois, sob o ponto de vista dos oficiais, seria inútil, já que o condenado iria experimentá-la na própria carne (Duarte e Garcia, 2021, p. 7).

²⁹ Tradução nossa. No original: “can mean a system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other. We face these two meanings daily: tracked ever more closely by firms and government, we have no clear idea of just how far much of this information can travel, how it is used, or its consequences.”

³⁰ A máquina era composta de três partes. Em cima havia um desenhador que movimentava um rastelo de vidro com agulhas fixadas (segunda parte) que escrevia a pena estabelecida nas costas do condenado que se encontra na cama abaixo (terceira parte) (Duarte e Garcia, 2021, p.4).

Pensando no cenário de uso *softwares* de reconhecimento facial, os indivíduos sofrem uma sentença na própria pele ao serem encarcerados em decorrência de erro no reconhecimento, sendo que sequer sabem que uma máquina enviesada e de uso não regulamentado foi o meio de prova utilizado. Temos aqui o contraste do novo – o uso de uma Inteligência Artificial – com o antigo – a obscuridade do processo de decisão. Utilizando as palavras de Duarte e Garcia (2021, p. 7), “muito embora sejam necessárias páginas para construir a metáfora de uma justiça irracional ‘kafkaniana’, bastaria imaginar as sentenças dadas aos indígenas em outra língua, ou as condenações à escravidão no tráfico negreiro”.

Essa deficiência na transparência, resultante de um sistema intrínseco ao próprio funcionamento da máquina, contribui para a perpetuação de vieses presentes nos dados de treinamento dos algoritmos, muitas vezes sem que tenhamos consciência desse fenômeno. Além disso, essa contaminação sistêmica gerada pelo preconceito humano é um traço do racismo estrutural, o qual, segundo Silvio Almeida (2019, *passim*), é o próprio racismo como parte da estrutura da sociedade.

O racismo foi e continua sendo um elemento constitutivo do nacionalismo brasileiro, uma vez que os projetos nacionais, formulados pelas classes dominantes, desde sempre caminharam no sentido de institucionalizá-lo, tornando-o parte do imaginário racional como, por exemplo, a exploração sexual da mulher negra como um produto nacional, incentivando, dessa forma, o “branqueamento da raça” juntamente como o estabelecimento do termo mulato como primeiro degrau na escada da branquificação sistemática do povo, bem como o incentivo a imigração europeia (Nascimento, 1978, *passim*).

Na sociedade estadunidense não é diferente. As chamadas Leis Jim Crow, que institucionalizaram a segregação racial no país, dividiram a maioria dos espaços públicos – escolas e transporte público, por exemplo – com estabelecimentos diferentes para brancos e negros. A decisão tomada pela Suprema Corte dos Estados Unidos sobre o caso *Plessy v. Ferguson* (1896) foi o ponto de partida dessa constitucionalização da segregação sob o argumento *separate but equal*. Esse argumento, à vista da Corte, não violava a constituição, mais especificamente a 14^a Emenda, desde que existisse igual qualidade nos espaços dos negros e dos brancos, dessa forma, a segregação se tornou algo constitucional.³¹

Apesar da Suprema Corte dos Estados Unidos ter declarada posteriormente a inconstitucionalidade da segregação nas escolas, ter exigido a adoção de planos para o combate

³¹ **SEPARADOS**, mas iguais. Direção: George Stevens Jr. Estados Unidos da América: New Liberty Production, 1991. 190 min. Disponível em: <https://www.youtube.com/watch?v=oGMSf87hLbQ>. Acesso em: 31 out. 2023.

da segregação nos sistemas públicos de ensino e, formalmente, não haver mais as Leis Jim Crow, na atualidade, a existência do racismo na sociedade e a segregação ainda persistem.

Na atualidade a segregação racial é facilmente perceptível quando, por exemplo, uma senhora se recusa a viajar ao lado de um negro pelo simples fator cor da pele. Indo para a esfera policial, tal afirmação pode ser confirmada pelo fato de os negros serem mais facilmente detidos e investigados por autoridade policiais estadunidenses do que um homem branco. Os assassinatos de George Floyd e Eric Garner refletem perfeitamente a existência do racismo enraizado na estrutura social estadunidense.

Além disso, de acordo com dados do Departamento de Polícia de Nova York (NYPD), destrinchados por Gisela Aguiar Wanderley (2016, p. 127-128), no período entre janeiro de 2004 e junho de 2012, das 4,4 milhões de pessoas abordadas coercitivamente pelos policiais nova-iorquinos, 52% eram negras, 31% hispânicas e 10% brancas, sendo que a população de Nova York é 23% negra, 29% hispânica e 33% branca.

Para além do racismo presente na própria estrutura social, o preconceito também faz parte da própria estrutura dos algoritmos que podem disseminá-lo ou ampliá-lo. Segundo Duarte e Garcia:

O algoritmo aplicado à segurança pública, inserido no sonho tecnocrata de uma decisão objetiva, neutra e fundamentada, não vem para substituir o tirocínio na tomada de decisão policial, mas para justamente fundamentá-lo, não o corrigir, mas potencializá-lo, seja no momento da abordagem, na definição de suspeição, seja na hora do abate (Duarte e Garcia, 2021, p. 18).

Dessa forma, esse fenômeno é chamado de racismo algorítmico, o qual está intimamente relacionado ao racismo estrutural, podendo até ser chamado de “racismo-estrutural-algorítmico”, nas palavras de Mozart Linhares da Silva e Willian Fernandes Araújo (2020, p. 8). Na perspectiva desses autores, o racismo algoritmo é mais um elemento do racismo estrutural que pode ser definido como “um dispositivo de constituição dos dados e dos arranjos estruturais dessas plataformas” (Da Silva e Araújo, 2020, p. 9). Para eles, uma das duas dimensões do racismo-estrutural-algorítmico se refere justamente a essa contaminação da estrutura do sistema e do seu modo de operação.

Consoante Da Silva e Araújo,

A seleção dos dados usados para treinar uma inteligência artificial até decisões políticas sobre qual conteúdo é “impróprio” ou “ofensivo”, “vieses” do racismo estrutural são inseridos, replicados e potencializados pela ação desses sistemas (Da Silva e Araújo, 2020, p.8).

A segunda dimensão refere-se à maneira como os sistemas aprendem significados. Devido ao fato de que dados são gerados a partir de atividades diárias e as interfaces dos sistemas são tão comuns que muitas vezes nem as notamos, os autores entendem que palavras usadas em mecanismos de busca na internet refletem o que a sociedade pensa sobre raça, muitas vezes de forma inconsciente (Da Silva e Araújo, 2020, pp. 8-9).

Recorrendo ao conceito de Bruna Lima (2022), a palavra algoritmo se torna um adjetivo de uma forma atual em que o racismo é praticado, o qual não está vinculado apenas a preocupações éticas em torno do uso dessas tecnologias, nem é algo que tenha surgido de forma independente a partir dos avanços da IA, em vez disso, “constitui um fenômeno sociotécnico de práticas de violência racial” (Lima, 2022, p. 37).

Além disso, essas maiores taxas de erro no reconhecimento de pessoas não-brancas podem ser consideradas como microagressões, que podem ocorrer tanto de maneira consciente quanto inconsciente muito em razão do racismo sistêmico da sociedade atual. As chamadas microagressões podem ser compreendidas como “ofensas verbais, comportamentais e ambientais comuns, sejam intencionais ou não intencionais, que comunicam desrespeito e insultos hostis, depreciativos ou negativos contra pessoas de cor” (Sue, 2010, p. 29 *apud* Silva, 2020, p. 125).

Esse termo foi cunhado por Chester Pierce (1970), o qual, segundo ele, “são sutis e paralisantes” e só percebemos a potencialidade e a extensão das complicações que causam quando compreendemos que esses pequenos ataques ocorrem de maneira ininterrupta (Pierce, 1970, p. 265-266 *apud* Silva, 2020, p. 124). Dessa forma, o termo “micro” não é, a princípio, para determinar o grau de potencialidade de produzir efeitos graves ou fatais, mas, sim, a capacidade de se espalhar, infiltrar, penetra facilmente na sociedade, além de serem atos perpetuados em níveis individuais – sejam por meio de insultos, invalidações, ou uma “simples” piada (Silva, 2020, p. 125).

Diante disso, observando tudo o que foi discutido anteriormente, torna-se evidente que não é apenas a pigmentação da pele em si que desempenha um papel adverso para os resultados obtidos e que a dificuldade sofrida pela máquina não se restringe exclusivamente ao fato de a pele ser mais escura.

O que se revela é que a questão abrange todos os aspectos que não se encaixam nos padrões predominantes de características faciais associados à etnia branca europeia ocidental. Conforme previamente apontado por Buolamwini e Gebru (2018, p. 10), os sistemas de reconhecimento facial enfrentam maiores obstáculos ao identificar características faciais – como formato dos olhos, narizes e bocas – que não se conformam ao padrão europeu ocidental,

com o qual as máquinas estão mais familiarizadas, devido à carência de dados relativos a essas populações, seja de maneira intencional ou não.

O que se revela é que, ao nos depararmos com essas inquietações, o mito da democracia racial é desmascarado mais uma vez. Ao percebemos que até para uma máquina a branquitude ganha assento privilegiado, é desmantelada a crença de que “pretos e brancos convivem harmoniosamente, desfrutando iguais oportunidades de existência, sem nenhuma interferência, nesse jogo de paridade social, das respectivas origens raciais ou étnicas” (Nascimento, 1978, p. 41).

Dessa forma, diante da constatação de que os sistemas de reconhecimento facial reproduzem e perpetuam vieses raciais, torna-se evidente a existência de lacunas e defeitos na tecnologia. A análise crítica das limitações desses sistemas desmascara não apenas as deficiências tecnológicas, mas também as estruturas sociais arraigadas que marginalizam e subestimam características faciais divergentes do padrão branco-europeu-ocidental, revelando a necessidade urgente de abordagens mais inclusivas e equitativas na tecnologia e na sociedade em geral.

Assim, a compreensão do Constitucionalismo Digital e da constitucionalização do ambiente digital é crucial para confrontar as crescentes ameaças aos direitos fundamentais, como o insidioso fenômeno do racismo algorítmico. Diante desse cenário, torna-se imperativo aprofundar o entendimento sobre a Tecnologia de Reconhecimento Facial em si. Dessa forma, a próxima seção se dedica a apresentar seus conceitos, seu funcionamento e suas aplicações em segurança pública. A análise desses fundamentos busca esclarecer o comportamento peculiar dessa tecnologia, evidenciando a importância da diversificação dos conjuntos de dados utilizados.

1.3 CONCEITO, FUNCIONAMENTO E APLICAÇÕES

De modo simples, a Inteligência Artificial (IA) pode ser definida como sendo a habilidade de um computador de realizar tarefas que normalmente só um humano teria tal competência. Nas palavras de Fabiano Hartmann Peixoto (2020), trata-se de

um ramo da ciência da computação que busca, com interação multidisciplinar com outras áreas do conhecimento, a reprodução de ações cognitivas tipicamente humanas. Para tanto, a IA pode valer-se de diversas técnicas como estratégia de incremento de performance ou simplesmente de delegação de funções enfadonhas, repetitivas ou consideradas delegáveis e roboticamente praticáveis (Peixoto, 2020, p. 17).

Diante desse conceito, é inegável o crescimento extraordinário da IA em diversos âmbitos da sociedade. A sua capacidade de crescimento e sofisticação vem revolucionando o modo que vivemos. A título de exemplo, no âmbito hospitalar, profissionais da saúde a têm como aliada na elaboração de diagnósticos de doenças, facilitando ou aumentando sua precisão, auxiliando em tratamentos e em procedimentos cirúrgicos.³²

Trazendo para o cotidiano de uma sociedade informatizada, diante da crescente necessidade de segurança de dados e de informações, estamos deixando de utilizar senhas alfanuméricas ou PINs para utilizarmos acessos biométricos que, por serem baseados em características biológicas do indivíduo, são mais difíceis de falsificar e fraudar. Isso pode ser facilmente verificado quando desbloqueamos nossos celulares, alteramos senhas em aplicativos de banco ou exercemos nosso direito constitucional ao voto.

Conforme explicado por Shang-Hung Lin (2000, p. 1)³³, essa forma de acesso “é um método automatizado de verificação ou reconhecimento da identidade de uma pessoa viva com base em algumas características fisiológicas”, como, por exemplo, impressão digital, características faciais, leitura de íris e DNA, que são atributos mais estáveis. Há também características comportamentais como estilo de escrita, padrão de voz e modo de andar, que costumam ser mais facilmente alteráveis devido a fatores externos, como doenças, ou aspectos e condições físicas ou fisiológicas, tais como cansaço e estresse.

Um dos mecanismos por trás desse controle de acesso biométrico é a **Tecnologia de Reconhecimento Facial**, a qual pode ser vista como um termo guarda-chuva que engloba “um conjunto de ferramentas digitais utilizadas para realizar tarefas em imagens ou vídeos de rostos humanos” (Buolamwini *et al.*, 2020, p. 2)³⁴. Essas tarefas contam com as habilidades de algoritmos treinados para realizarem automaticamente a correlação entre uma imagem fornecida com imagens constantes em seu banco de dados.

Os algoritmos, por sua vez, nada mais são que “procedimentos codificados que, com base em cálculos específicos, transformam dados em resultados desejados” (Gillespie, 2018, p. 97). O seu treinamento pode ocorrer por meio de um processo de *Machine Learning*

³² DAVENPORT, Thomas; KALAKOTA, Ravi. The potential for artificial intelligence in healthcare. **Future Healthcare Journal**, v. 6, n. 2, p. 94-98, 2019. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6616181/>. Acesso em: 27 set. 2023.

³³ Tradução nossa. No original: “[...] are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics [...]”.

³⁴ Tradução nossa. No original: “[...] a set of digital tools used to perform tasks on images or videos of human faces.”

(Aprendizado de Máquina), que consiste em “um conjunto de técnicas e ferramentas que permitem que os computadores ‘pensem’ criando algoritmos matemáticos com base em dados acumulados”³⁵ (Information Commissioner's Office, n.p.).³⁶

Esse processo normalmente se inicia com a seleção de dados contendo padrões ou semelhanças que se almeja que a máquina aprenda a identificar. Em seguida, esses dados e as respostas dos padrões existentes são entregues para a máquina, que aprenderá a identificá-los e, por fim, gerará um modelo que terá a habilidade de reconhecer padrões de novos dados fornecidos, semelhantes àqueles usados em seu aprendizado.³⁷

A título de exemplificação, são oferecidas diversas fotografias para a máquina com o intuito de ensinar o que seria um rosto. Com isso, gradualmente espera-se que ela aprenda a reconhecer outros rostos além dos originalmente mostrados. Dessa forma, caso haja uma deficiência nesse conjunto, haverá uma deficiência nos resultados gerados pelo *software*.

A depender da finalidade do programa, sua estrutura interna pode variar. No entanto, de modo geral, é dividido internamente em duas funções: (1) um detector facial, que fornece aproximadamente a localização de um rosto, simplesmente fazendo a distinção do que seria um rosto e o que não seria; e (2) um reconhecedor facial, que diz de quem é esse rosto, fornecendo a localização exata, sendo normalmente projetados para encontrar ambos os olhos como forma de auxílio na detecção do restante do rosto (Lin, 2000, p. 2-3).

Assim, nas palavras de Andrew Ferguson (2021, p. 1.100)³⁸, é possível afirmar que se trata de “uma tecnologia digital de correspondência”, uma vez que o algoritmo busca correspondência de características físicas – como olhos, nariz e boca, e as distâncias entre elas – de um rosto com outro constante em seu banco de dados.

Dessa forma, considerando o exposto, pode-se inferir que há uma extensa variedade de aplicações da Tecnologia de Reconhecimento Facial. Segundo Ferguson (2021, p. 1.115-1.126), as mais relevantes aplicações em policiamento e segurança são para: vigilância, identificação, rastreamento e verificação.

³⁵ Tradução nossa. No original: “The set of techniques and tools that allow computers to ‘think’ by creating mathematical algorithms based on accumulated data.”

³⁶ INFORMATION Commissioner's Office. **Glossary**. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/glossary/?q=gradient>. Acesso em: 4 out. 2023.

³⁷ Há também outras técnicas de aprendizado como o *deep learning* – aprendizado profundo – em que o aprendizado se dá através do uso sucessivo de dezenas de camadas de processamento dentro de uma arquitetura de redes neurais, semelhantes ao cérebro humano.

³⁸ Tradução nossa. No original: “Facial recognition is a digital matching technology.”

Nesse ponto, seguindo as aplicações indicadas por Ferguson, a **Vigilância Facial** tem o objetivo de monitorar locais públicos e fazer a identificação em massa de indivíduos, como aeroportos, estações de metrô, estádios esportivos e áreas movimentadas da cidade. Esse método, no qual não há um suspeito específico, pode ser usado para: filtrar gravações de vídeos de segurança e identificar pessoas específicas; monitorar em tempo real locais públicos como forma de segurança ou controle social; ou até mesmo minerar imagens armazenadas em bancos de dados de terceiros (como redes sociais, imagens provenientes da internet e de páginas da web amplamente acessadas) com o objetivo de coletar informações sobre indivíduos de uma sociedade (Ferguson, 2021, p. 1.116-1.119).

Um exemplo de vigilância facial ocorreu durante a pandemia da Covid-19 em diversos países, sendo um deles a China, a qual contou com filmagens de câmeras espalhadas por toda a cidade que capturavam e armazenavam dados obtidos por sistemas automatizados de reconhecimento facial dos cidadãos chineses. O objetivo era observar quem estava respeitando o uso de máscaras e realizar verificações de temperatura corporal em larga escala.³⁹

A **Identificação Facial**, como o termo sugere, almeja determinar a identidade de um rosto específico mediante a correspondência entre uma imagem e um banco de dados. A título de ilustração, quando se dispõe de uma imagem de um indivíduo sob suspeita, obtida por meio de sistemas de vigilância ou fotografias capturadas por testemunhas, e pretende identificar o indivíduo por meio de uma comparação com fotografias presentes em documentos como carteiras de motorista, carteiras de identidade ou equivalentes (Ferguson, 2021, 1.119-1.122).

Por se tratar de uma comparação de um para muitos, erros podem ocorrer e, como exposto anteriormente, alguns fatores podem influenciar significativamente no resultado obtido. Conforme alertado por Ferguson (2021), há sistemas em que o resultado correspondente pode incluir “de vinte a cinquenta impressões digitais faciais semelhantes” (2021, p. 1.111)⁴⁰, isso significa que, por exemplo, na identificação de um suspeito, há grandes chances de “receber de vinte a cinquenta impressões digitais faciais como possíveis correspondências” (2021, p. 1.112)⁴¹.

Por sua vez, o **Rastreamento Facial** busca identificar a localização em tempo real do suspeito a partir da identificação de seu rosto em sistemas de vigilância em massa. Pode ocorrer também por meio de gravações de câmera de vigilância, podendo obter a localização do

³⁹ Notícia publicada pela BBC, em 3 de março de 2020, com o seguinte título: “*Coronavirus: China's tech fights back*”. Disponível em: <https://www.bbc.com/news/technology-51717164>. Acesso em: 4 out. 2023.

⁴⁰ Tradução nossa. No original: “In many systems, returned matches involve more than one image and may involve as many as twenty to fifty similar faceprints.”

⁴¹ Tradução nossa. No original “[...] may receive twenty to fifty faceprints back as possible matches.”

suspeito ao longo do tempo, além de outros dados como dia, hora e o local. Segundo o autor, trata-se de uma junção das técnicas de vigilância e identificação, uma vez que se tem um suspeito específico e é utilizada a vigilância em massa para rastreá-lo (Ferguson, 2021, p. 1.122-1.124).

Por último, a **Verificação Facial** envolve uma verificação um para um, isto é, diferentemente da Identificação Facial – que visa determinar a identidade de um rosto apresentado –, a Verificação Facial busca confirmar se o rosto apresentado corresponde à imagem previamente registrada no sistema de referência (Ferguson, 2021, p. 1.124-1.126). A título de exemplificação, pode-se mencionar o uso dessa técnica no desbloqueio de smartphones, cuja finalidade reside em confirmar se o rosto exibido diante da câmera coincide com o rosto do proprietário previamente registrado.

O uso da Verificação Facial transcende o escopo da investigação criminal, abarcando cenários mais amplos, como sua implementação em aeroportos, eventos, bem como na busca por pessoas desaparecidas. Além disso, essa tecnologia tem sido empregada em processos de controle de fronteiras para autenticar identidades a partir de fotografias presentes em documentos como passaportes e, igualmente, na substituição dos tradicionais cartões de embarque em aeroportos (Ferguson, 2021, p. 1.124-1.126).

Apesar da vasta possibilidade de aplicações dessa tecnologia, diversos fatores podem exercer uma influência adversa sobre os resultados obtidos, resultando em graves violações de direitos fundamentais dos cidadãos, conforme mostrado anteriormente. Dessa forma, o capítulo seguinte apresentará casos reais em que pessoas afro-estadunidenses foram encarceradas em razão de erro no reconhecimento em decorrência de vieses raciais. Em seguida, ficará encarregado de apontar a atuação da Suprema Corte dos Estados Unidos sobre o tema, sua jurisprudência disponível e se, diante disso, a Tecnologia de Reconhecimento Facial pode vir a ser utilizada como prova. Além disso, de maneira breve, serão expostas recomendações feitas por estudiosos sobre o uso dessa tecnologia no âmbito criminal e as tentativas de regulação.

2 ANALISANDO O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NO ÂMBITO CRIMINAL

No capítulo anterior, em sua primeira seção, foram expostos os conceitos de Constitucionalismo Digital e constitucionalização do ambiente digital, que, em síntese, possuem o objetivo de equilibrar as transformações e inovações ocasionadas pelo avanço

tecnológico com a proteção dos direitos fundamentais e a manutenção do equilíbrio dos poderes e das instituições jurídicas preexistentes.

Uma das problemáticas que surgiu com o crescimento extraordinário IA e, como consequência, tornou-se alvo do Constitucionalismo Digital, foi apresentada na segunda seção. Esse novo dilema é o racismo estrutural algorítmico, o qual foi definido como sendo a contaminação da estrutura dos algoritmos pelo próprio preconceito humano, tendo o potencial de disseminá-lo e ampliá-lo. Além disso, ficou demonstrada a sua forma de operação nos *softwares* de reconhecimento facial a partir da demonstração de pesquisas em que foram obtidas maiores taxas de erro no reconhecimento de pessoas não-brancas, sendo estas taxas definidas como microagressões.

Por fim, na terceira seção, foram fornecidos conceitos introdutórios relativos à Tecnologia de Reconhecimento Facial, a qual foi definida como sendo um termo guarda-chuva que abarca todo o tipo de ferramenta digital que possui a finalidade de operar imagens fornecidas de rostos humanos com as constantes em bancos de imagem preexistentes. Além disso, apresentou-se uma síntese do seu funcionamento e suas aplicações no âmbito da segurança pública.

Tendo em vista o funcionamento dessa ferramenta, a qual necessita de uma ampla gama de dados e de condições favoráveis no ambiente em que está sendo utilizada, além dos diversos fatores que possuem o potencial de influenciar os resultados de maneira discriminatória, é necessário compreendermos a real dimensão do impacto do uso desregulado da Tecnologia de Reconhecimento Facial no âmbito criminal. Diante desse contexto, em sua primeira seção, o presente capítulo apresentará casos reais em que pessoas afro-estadunidenses foram encarceradas em decorrência de erro no reconhecimento em razão da existência de vieses raciais no *software* utilizado.

Em seguida, é necessário analisar a reação de entidades estadunidenses e se o arsenal jurídico disponível é eficaz frente às implicações éticas dessa inovação tecnologia. Dessa forma, a segunda seção deste capítulo ficará encarregada de apontar se a Suprema Corte dos Estados Unidos vem atuando sobre o tema, sua jurisprudência disponível e se, diante disso, a Tecnologia de Reconhecimento Facial pode vir a ser utilizada como prova. Além disso, de maneira breve, serão expostas recomendações feitas por estudiosos sobre o uso dessa tecnologia no âmbito criminal e as tentativas de regulação.

2.1 TECNOLOGIA E DISCRIMINAÇÃO: CASOS REAIS

Imagine-se em uma situação em que está a caminho de sua residência ou local de trabalho, quando é abordado por policiais munidos de um mandado de prisão contra você. Sem compreender o motivo da detenção, questiona às autoridades sobre o que está ocorrendo, contudo, é recebido de maneira ríspida e intimidadora.

Após ser detido por dias, ou até mesmo enfrentar meses de julgamento, você descobre que a única evidência utilizada contra você é uma fotografia, sendo que essa imagem foi submetida a um sistema de reconhecimento facial, que apontou erroneamente que você é o responsável por um crime. De maneira mais gravosa, a tecnologia em questão não é regulada, o *software* em questão é conhecido por suas elevadas taxas de erro na identificação de indivíduos não-brancos e, mesmo cientes desse histórico, as autoridades insistiram (e insistem) em utilizar essa ferramenta.

Esse é o cenário angustiante vivenciado por diversas pessoas afrodescendentes nos Estados Unidos, sendo a realidade enfrentada por indivíduos como Robert Williams, Michael Oliver e Porcha Woodruff, que terão seus relatos apresentados respectivamente nas subseções seguintes.

Estes casos foram escolhidos, pois tratam de (1) pessoas negras que foram detidas e encarceradas de maneira equivocada após *softwares* de reconhecimento facial os selecionarem como possíveis autores de crimes, que (2) foram representadas por organizações não governamentais na luta contra a violação de direito com viés de raça, além de (3) compartilharem a localização geográfica dos incidentes – Cidade de Detroit, Michigan – em que o departamento de polícia faz, em média, 125 buscas de reconhecimento facial por ano, sendo a maioria de pessoas negras⁴².

2.1.1 ROBERT WILLIAMS

Segundo a queixa apresentada pela *American Civil Liberties Union* (ACLU) de Michigan⁴³ contra a polícia de Detroit, em 9 de janeiro de 2020, Robert Julian-Borchak Williams, um homem afrodescendente, residente em Farmington Hills – Michigan, recebeu

⁴² Dado apresentado em uma matéria do *The New York Times*. Disponível em: <https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html>. Acesso em: 6 nov. 2023.

⁴³ Queixa apresentada em nome de Robert Williams pela ACLU. Disponível em: <https://www.aclu.org/documents/aclu-michigan-complaint-re-use-facial-recognition>. Acesso em: 1 nov. 2023.

uma ligação do Departamento de Polícia de Detroit obrigando-o a se apresentar a uma delegacia de polícia para sua prisão ser efetuada. O motivo não foi comunicado e, ao pedir mais informações, os policiais ameaçaram efetuar sua prisão em seu local de trabalho. Diante dessa situação, Williams optou por retornar para casa onde poderia conversar com os oficiais que lá estavam.

Chegando ao local, foi detido e algemado imediatamente no quintal de casa na frente de sua esposa e de suas filhas pequenas. A polícia alegou que o sistema de reconhecimento facial identificou a foto de sua carteira de motorista de anos atrás como sendo compatível com o sujeito nas imagens das câmeras de segurança de uma loja de departamentos assaltada.


Na Figura 2 a seguir, podemos observar um relatório de investigação em que contém o resultado da busca feita pelo *software*. A fotografia à esquerda é a do suspeito e à direita é a de Robert Williams. Observe que, logo no início do documento, há a informação de que o resultado obtido não é uma causa provável⁴⁴ para deter o indivíduo, sendo apenas uma ferramenta para o desdobramento da investigação.

Além disso, é necessário pontuar que, como dito na seção 1.2. do capítulo anterior, em um contexto de investigação criminal, as imagens obtidas para identificação de um indivíduo muito possivelmente enfrentarão a maioria dos influenciadores externos. Tal afirmação torna-se evidente na imagem utilizada para identificar o Robert Williams, tendo em vista que a foto do suspeito não foi tirada nas melhores condições de iluminação, além da utilização de artifícios pelo indivíduo para dificultar o reconhecimento, como o boné.


Vejamos a seguir.

⁴⁴ Esse termo será detalhado no tópico 2.2.1.

Figura 2 – Relatório de investigação.





MICHIGAN STATE POLICE
INVESTIGATIVE LEAD REPORT
LAW ENFORCEMENT SENSITIVE



THIS DOCUMENT IS NOT A POSITIVE IDENTIFICATION. IT IS AN INVESTIGATIVE LEAD ONLY AND IS NOT PROBABLE CAUSE TO ARREST. FURTHER INVESTIGATION IS NEEDED TO DEVELOP PROBABLE CAUSE TO ARREST.

BID DIA Identifier: BID-39641-19	Requester: CA Yager, Rathe
Date Searched: 03/11/2019	Requesting Agency: Detroit Police Department
Digital Image Examiner: Jennifer Coulson	Case Number: 1810050167
	File Class/Crime Type: 3000

Probe Image	Investigative Lead
	

Fonte: *WLIW-FM*⁴⁵. Processo disponibilizado na página da ACLU de Michigan.⁴⁶

A acusação baseou-se apenas nessa busca de reconhecimento facial usando as imagens de câmeras de vigilância. Diante do resultado, os investigadores mostraram 6 (seis) fotografias – das quais uma era a foto da carteira de motorista de Williams – a um segurança da loja, mesmo sabendo que ele não havia testemunhado o incidente pessoalmente e que apenas assistiu às mesmas imagens da câmera de segurança que os policiais. Com base na confirmação do segurança, foi emitido um mandado de prisão.

Como resultado, Williams foi acusado injustamente de roubo sendo levado para o Centro de Detenção de Detroit, onde ficou detido durante a noite em uma cela lotada e imunda, sem receber informações sobre o que estava acontecendo com ele ou do que estava sendo acusado. No dia seguinte, foi interrogado e, durante o interrogatório, ficou claro que a sua prisão se baseou em um reconhecimento facial falho. Robert Williams passou cerca de 30 (trinta) horas na prisão antes de ser liberado sob fiança. Durante esse tempo, foi separado de sua família e sujeito a um processo traumático de prisão injusta.

⁴⁵ Disponível em: <https://www.wliw.org/radio/news/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michigan/>. Acesso em: 16 out. 2023.

⁴⁶ Disponível em: <https://www.aclumich.org/en/press-releases/farmington-hills-father-sues-detroit-police-department-wrongful-arrest-based-faulty>. Acesso em: 3 nov. 2023.

Este caso chamou a atenção de todo o território dos Estados Unidos para as preocupações sobre o uso da Tecnologia de Reconhecimento Facial pelas forças de segurança, destacando a possibilidade de violações de direitos com viés racial na tecnologia. Após o ocorrido, Williams fez parte de uma audiência realizada pelo subcomitê de crime, terrorismo e segurança interna da Câmara dos Representantes (*House of Representatives*), que buscou tratar sobre o uso da tecnologia de vigilância pelas forças de segurança.⁴⁷

Atualmente, Williams – juntamente à ACLU – está processando a cidade de Detroit. Após a publicação de sua história, o gabinete da promotoria do Condado de Wayne⁴⁸ enviou um pedido de desculpas a Williams. Além disso, o chefe da polícia de Detroit relatou que a tecnologia tem o potencial de identificar de maneira errada os suspeitos em 96% (noventa e seis por cento) dos casos.⁴⁹

2.1.2 MICHAEL OLIVER

Outro caso diz respeito a Michael Oliver, que, em julho de 2019, foi detido sob acusação de roubo quando se dirigia ao seu local de trabalho em Ferndale – Michigan. Michael teve seu carro apreendido e ficou detido por mais de 2 (dois) dias sem qualquer tipo de informação sobre o motivo de sua prisão, semelhante ao ocorrido com Robert Williams.

De acordo com informações veiculadas pelo jornal *Detroit Free Press*⁵⁰, a tecnologia de reconhecimento facial – desenvolvida pela empresa *Data Works Plus* – identificou Michael como o suposto autor do incidente, no qual um professor teve seu celular arrancado de suas mãos enquanto estava em seu veículo filmando a briga de um grupo de alunos. Com base nesse resultado, os investigadores apresentaram ao referido professor uma relação de fotografias, entre as quais constava uma imagem de Michael, e o docente prontamente identificou-o como o responsável pelo ocorrido. Meses mais tarde, em uma audiência anterior ao julgamento, Michael descobriu que a única evidência existente contra ele consistia em uma captura de tela de um vídeo do incidente, que havia sido gravado pela vítima.

⁴⁷ Disponível em: <https://www.youtube.com/watch?v=KVr7uoEvhsK>. Acesso em: 12 maio 2023.

⁴⁸ Wayne County Prosecutor's Office – Repartição pública municipal em Detroit, Michigan.

⁴⁹ Disponível em: <https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing>. Acesso em: 31 out. 2023.

⁵⁰ Disponível em: <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/>. Acesso em: 7 set. 2023.

Conforme afirmado por Patrick Nyenhuis, advogado de defesa de Michael, em uma entrevista concedida à revista *Motherboard*⁵¹, era evidente que havia algum erro no processo de reconhecimento conduzido na identificação realizada pelo *software*. Tal equívoco tornou-se ainda mais visível em virtude das características distintas de Michael Oliver (Figura 3), que ostenta uma grande quantidade de tatuagens em ambos os braços (Figura 4), notadamente com aspecto envelhecido, compartilhando pouquíssimas características físicas com o suspeito, limitando-se à coincidência na cor da pele.

Figura 3 – Comparação entre o autor do crime (à esquerda) e Michael Oliver (à direita).



Fonte: Detroit Free Press.⁵²

Figura 4 – Comparação entre as tatuagens.



Fonte: Detroit Free Press.⁵³

⁵¹ Disponível em: <https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrest-now-hes-suing>. Acesso em: 31 out. 2023.

⁵² Disponível em: <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/>. Acesso em: 7 set. 2023.

⁵³ Disponível em: <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/>. Acesso em: 7 set. 2023.

Ainda conforme o depoimento do advogado de defesa de Michael à revista *Motherboard*, embora as diferenças entre os dois indivíduos fossem indenes de dúvidas, o promotor encarregado do caso, durante a primeira audiência, permaneceu com suas desconfianças, chegando a sugerir a possibilidade de Michael ter adquirido as tatuagens após a ocorrência do crime, mesmo sendo evidente o fato de possuírem um aspecto antigo. No entanto, posteriormente, a Promotoria do Condado de Wayne retirou as acusações de furto.

Apesar das desculpas subsequentes, os danos causados já haviam se tornado irreparáveis. Em uma entrevista concedida à CBS News⁵⁴, Michael relatou que ainda não havia conseguido se recuperar completamente das consequências de sua injusta prisão. Ele perdeu o emprego e, devido à falta de recursos financeiros, foi forçado a deixar sua residência alugada e perdeu seu veículo.

Posteriormente, Michael entrou com uma ação judicial contra a cidade de Detroit em busca de uma indenização. No processo alega que a Polícia de Detroit tinha ciência de que utilizou uma tecnologia de reconhecimento facial com alta taxa de erro na identificação de pessoas de cor, o que resultou na prisão e encarceramento injustos de indivíduos pertencentes a essa categoria.⁵⁵

2.1.3 PORCHA WOODRUFF

O terceiro e mais recente caso envolve Porcha Woodruff, que, em fevereiro deste ano (2023), foi detida em sua residência enquanto preparava suas duas filhas para irem à escola. De acordo com a ACLU⁵⁶, Porcha é a sexta pessoa a denunciar ter sido presa erroneamente devido ao uso da tecnologia de reconhecimento facial e a primeira mulher a relatar tal incidente.

De acordo com informações veiculadas pelo jornal *The New York Times*⁵⁷, Porcha estava grávida de 8 (oito) meses quando agentes do Departamento de Polícia de Detroit bateram à sua

⁵⁴ Disponível em: <https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/>. Acesso em: 7 set. 2023.

⁵⁵ Disponível em: <https://s3.documentcloud.org/documents/7202332/Draft-of-Michael-Oliver-Complaint-changes932020-1.pdf>. Acesso em: 6 nov. 2023.

⁵⁶ Notícia publicada pela ACLU, em 6 de agosto de 2023, com o seguinte título: “*After Third Wrongful Arrest, ACLU Slams Detroit Police Department for Continuing to Use Faulty Facial Recognition Technology*”. Disponível em: <https://www.aclu.org/press-releases/after-third-wrongful-arrest-aclu-slams-detroit-police-department-for-continuing-to-use-faulty-facial-recognition-technology>. Acesso em: 7 set. 2023.

⁵⁷ Notícia publicada pelo The New York Times, em 6 de agosto de 2023, com o seguinte título: “*Eight Months Pregnant and Arrested After False Facial Recognition Match*”. Disponível em: <https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html>. Acesso em: 6 nov. 2023.

porta com um mandado de prisão em seu nome, com base unicamente na identificação realizada por uma tecnologia de reconhecimento facial desenvolvida pela empresa *Data Works Plus*, que a identificou como sendo a suposta autora de um assalto e um roubo de veículo. Diante desse resultado, os investigadores mostraram seis fotografias à vítima, uma das quais era de Porcha, que acabou apontando-a como autora do crime.

Mesmo em um estágio avançado de sua gravidez, Porcha foi algemada e levada ao Centro de Detenção de Detroit, onde passou horas sendo interrogada sobre um crime que não cometeu. Em seu relato ao jornal, Porcha descreveu ter sentido contrações enquanto estava sob custódia, sofrendo dores intensas e espasmos, provavelmente devido ao ataque de pânico causado por toda a situação. Em razão do estresse que sofreu, ao sair do tribunal mediante pagamento de fiança, foi direto para o hospital, onde foi constatada sua desidratação.

De acordo com o *The New York Times*, posteriormente, o promotor do condado de Wayne retirou as acusações contra ela. No entanto, Porcha Woodruff ingressou com uma ação por detenção indevida contra a Prefeitura de Detroit.

As ações propostas por Williams, Michael e Porcha seguem sem demais atualizações.

2.2 O DEBATE NA SUPREMA CORTE DOS ESTADOS UNIDOS

Considerando todos os desafios discutidos até este ponto, é legítimo questionar se o ordenamento jurídico dos Estados Unidos⁵⁸, que é o foco deste estudo, dispõe de mecanismos eficazes para controlar e lidar com essas questões. Até porque, corroborando os estudos de Celeste (2019) expostos no capítulo anterior, o arcabouço legislativo tradicional – a constituição, por exemplo – demonstra ser insuficiente no enfrentamento dos novos desafios tecnológicos.

Dessa forma, em consideração à problemática, nesta seção, primeiro analisaremos os entendimentos firmados pela Suprema Corte dos Estados Unidos em relação à Quarta Emenda e erros na atividade policial, pois esse preceito constitucional busca proteger os cidadãos estadunidenses contra possíveis abusos em policiamento. Analisar essa jurisprudência servirá de ajuda na hora de pensarmos como a Corte pode vir a julgar em um questionamento quanto ao uso da Tecnologia de Reconhecimento Facial pelas forças de segurança ou se deve seguir outra linha de raciocínio caso a Quarta Emenda seja ineficaz.

⁵⁸ Tanto do governo federal, quanto dos governos estaduais.

Em um segundo momento, serão apresentados os fatores de Daubert, que são cinco critérios a serem identificados pelo juízo na verificação da possibilidade de uso como evidência de um determinado método ou teoria. A partir dessa explanação, será verificado se a Tecnologia de Reconhecimento Facial se encaixa nesses critérios.

Por fim, serão expostas recomendações feitas por estudiosos sobre o uso dessa tecnologia no âmbito criminal e as reações dos estados e tentativas de regulação.

2.2.1 A SUPREMA CORTE E A QUARTA EMENDA

De acordo com as observações de Andrew Ferguson (2021, p. 1.164), a situação nos Estados Unidos em relação à Quarta Emenda da Constituição dos Estados Unidos e sua jurisprudência frente às inovações tecnológicas é motivo de grande preocupação, pois é evidente a ineficiência da Quarta Emenda na regulação das atividades policiais em meio aos avanços tecnológicos.

Segundo a Constituição dos Estados Unidos, a Quarta Emenda prevê que:

O direito do povo de estar seguro em seus corpos, casas, papéis e pertences, contra buscas e apreensões injustificadas, não será violado, e nenhum mandado será emitido, mas mediante causa provável, apoiada por juramento ou afirmação, e descrevendo particularmente o local a ser revistado e as pessoas ou coisas a serem apreendidas (Estados Unidos, 1789, n.p.).⁵⁹

De maneira geral, conforme explicado por Duarte e Silva (2021, p. 218), esse preceito “é essencial à doutrina do devido processo legal, uma vez que institui procedimentos processuais que regulam à inviolabilidade do lar e a proteção da intimidade, que são oponíveis ao Estado Polícia e ao Estado Juiz”, proibindo buscas, prisões e apreensões arbitrárias, as quais devem ocorrer mediante um mandado devidamente fundamentado em uma causa provável, respaldada em fontes confiáveis.

Até o momento presente, não há um precedente na Suprema Corte dos Estados Unidos referente à Tecnologia de Reconhecimento Facial e prisões equivocadas, em grande parte devido à dispersão dos casos e ao receio de muitas pessoas em denunciar (Ferguson, 2021, p.

⁵⁹ Tradução nossa. No original: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Disponível em: <https://constitution.congress.gov/constitution/amendment-4/>. Acesso em: 25 nov. 2023.

1.193; Haddad, 2021, p. 902). Entretanto, com base nos entendimentos já formados pela Suprema Corte dos Estados Unidos em casos envolvendo possíveis violações da Quarta Emenda em contexto de policiamento, é possível delinear considerações sobre o que é viável manter ou não em futuros litígios em que a Tecnologia de Reconhecimento Facial seja utilizada como prova em contexto criminal.

Conforme apontado por Ferguson (2021, pp. 1.174-1.176), um dos entendimentos já formados pela Suprema Corte é a “suspeita razoável” – *Reasonable Suspicion* – cujo propósito é restringir entradas em domicílios, abordagens e apreensões arbitrárias por parte das forças de segurança. Esse *standard* firmado no caso *Terry v. Ohio*⁶⁰ estabelece que o policial deve fornecer argumentos fáticos específicos e plausíveis para justificar de maneira razoável a intromissão na esfera particular do cidadão (Ferguson, 2021, p. 1.174).

Esse entendimento reconhece a condição humana dos policiais e a possibilidade de cometerem equívocos em seus julgamentos durante suas atividades nas ruas. Contudo, ao mesmo tempo, o *standard* da suspeita razoável permite que, caso ocorra um erro cometido dentro de um parâmetro de suspeita razoável, não há violação à Quarta Emenda, sendo que a Corte nunca estabeleceu o limiar de quão errado um policial pode estar (Ferguson, 2021, p. 1.175).

Partindo dessa linha de raciocínio e aplicando-a em uma situação de uso da Tecnologia de Reconhecimento Facial, Ferguson nos mostra que:

[...] essa incerteza significa que a taxa de erro para uma correspondência pode ser significativa (e ainda assim constitucional). Ambos os falsos positivos e falsos negativos podem ocorrer, e dentro das porcentagens existentes, muitos indivíduos podem ser parados incorretamente com base em correspondências errôneas. Se aplicado ao padrão de suspeita razoável, um sistema de reconhecimento facial pode estar mais errado do que certo e ainda ser constitucional (ou pelo menos não violar a Quarta Emenda) (Ferguson, 2021, p. 1.176).⁶¹

⁶⁰ Um policial à paisana observou uma movimentação suspeita de 3 (três) indivíduos que percorriam um trajeto idêntico, indo e voltando. Mesmo sem elementos que embasassem uma causa provável, o agente abordou os suspeitos e, ao realizar uma revista em suas vestimentas, identificou que os suspeitos estavam armados evitando, portanto, um assalto a mão armada. Essa abordagem ficou conhecida como *stop and frisk* (deter e revistar) (Wanderley, 2016, p. 115-116).

⁶¹ Tradução nossa. No original: “[...] this uncertainty means that the error rate for a match could be significant (and yet constitutional). Both false positives and false negatives may occur, and within the existing percentages many individuals could be incorrectly stopped based on erroneous matches. If mapped to the reasonable suspicion standard, a facial recognition system could be more wrong than right and still be constitutional (or at least not violative of the Fourth Amendment).”

Outro entendimento firmado versa sobre a ocorrência de um erro e a existência de uma “causa provável” – *Probable Cause* – (p. 1.176-1.179). Esse preceito tem o propósito de restringir prisões e revistas arbitrárias.

Segundo o Departamento de Justiça dos Estados Unidos (2022, p. 3)⁶², a chamada “causa provável” pode ser entendida como a existência de indícios mínimos de que “um crime tenha sido cometido e que há mais probabilidade de que a evidência de tal crime seja encontrada no local a ser investigado”, fundamentando, portanto, buscas e apreensões de bens. Essa mesma ferramenta pode ser utilizada na detenção e no encarceramento de pessoas, cabendo ao tribunal decidir se “há uma causa provável para acreditar que um crime tenha sido cometido e que há mais probabilidade de que a pessoa a ser detida tenha cometido o crime”.

Partindo desse entendimento e aplicando-o em uma situação de uso da ferramenta aqui estudada, Ferguson (2021, p. 1.176) aponta que “a causa provável de que o rosto de uma pessoa corresponda ao rosto de uma pessoa com um mandado de prisão aberto por um crime grave pode ser suficiente para prendê-la imediatamente”⁶³. Partindo desse pressuposto, as situações enfrentadas por Robert Williams, Michael Oliver e Porcha Woodruff, embora sejam consideradas absurdas, aparentemente não violam a Quarta Emenda.

Um terceiro entendimento diz respeito ao Erro Negligente – *negligente error* – que legitima o uso de provas advindas de erros policiais desde que não sejam “intencionais, imprudentes, grosseiramente negligentes ou resultado de problemas sistêmicos ou recorrentes” (Ferguson, 2021, p. 1.179)⁶⁴. Em outras palavras, um mero erro negligente não implicará a exclusão de provas ilícitas.

Dessa forma, como elucidado por Evandro Piza Duarte e Thales Cassiano Silva (2021), há uma desconstitucionalização do entendimento sobre a exclusão de provas ilícitas – aquelas que foram obtidas de maneira contrária às garantias do devido processo legal previsto pela Quarta Emenda.

Inicialmente, no caso *Weeks v. United States* (1914), a Suprema Corte dos Estados Unidos reconheceu a necessidade de se criar um remédio constitucional para concretizar os direitos constitucionais previstos na Quarta Emenda (Duarte e Silva, 2021, p. 220). No entanto, com o evoluir do entendimento da Corte, houve uma redução da doutrina de exclusão de prova ilícita e, com o caso *Calandra v. United States* (1974), iniciou-se o processo de

⁶² Disponível em: <https://www.justice.gov/criminal-oia/file/1501821/download>. Acesso em: 9 nov. 2023.

⁶³ Tradução nossa. No original: “Probable cause that a person’s face matches the face of a person with an open felony warrant could be sufficient to arrest them on the spot.”

⁶⁴ Tradução nossa. No original: “[...] not intentional, reckless, grossly negligent, or the product of systemic or recurring problems.”

desconstitucionalização das garantias do devido processo legal revistos na Quarta Emenda (Duarte e Silva, 2021, p. 226).

Isso porque a regra da vedação à prova ilícita passou a ser “uma teoria sobre a inibição de condutas dos agentes do estado, que agem em desconformidade com os procedimentos processuais, o que dependeria da valoração da necessidade de sua aplicação em cada caso”, perdendo seu caráter constitucional na garantia de um devido processo legal (Duarte e Silva, 2021, p. 226).

Aliado a isso, no caso *Herring v. United States*, conforme lecionado por Duarte e Silva (2021, p. 231), a Suprema Corte estabeleceu o entendimento de que “a conduta dos policiais deveria ser deliberadamente ilícita e suficientemente culpável para que se pudesse acionar o gatilho da regra de exclusão das provas”, invertendo o entendimento existente sobre a necessidade e possibilidade de exclusão da prova ilícita. Dessa forma,

a ilegalidade ensejaria exclusão de evidências quando “independentemente de um policial razoavelmente bem treinado, diante de todas as circunstâncias, pudesse ter reconhecido a ilegalidade da busca”. A conduta só seria passível de excluir as provas se, no caso concreto, o policial potencialmente soubesse da ilicitude da busca” (Duarte e Silva, 2021, p. 231).

Pensando no funcionamento da Tecnologia de Reconhecimento Facial, Ferguson aponta que a jurisprudência da Suprema Corte

[...] solidifica a realidade de que erros negligentes na aplicação não minarão a constitucionalidade do sistema. Apenas casos intencionais, imprudentes ou sistêmicos de erro justificarão um remédio pela regra da exclusão. Embora direitos e remédios sejam certamente diferentes, esse perdão para erros permite uma maior liberdade para cometer equívocos. Se for apenas negligente, um erro em uma correspondência de reconhecimento facial não terá consequências para a investigação policial (Ferguson, 2021, p. 1.180).⁶⁵

Seguindo essa linha de raciocínio, ao analisarmos os três casos expostos anteriormente, caso a Suprema Corte entenda que o uso da Tecnologia de Reconhecimento Facial pelo Departamento de Polícia de Detroit, mesmo cientes das altas taxas de erro, é um ato sistemático e reiterado, é possível considerá-lo como uma violação à Quarta Emenda e, portanto, inconstitucional. Contudo, caso considere como um mero erro, a prisão equivocada e a

⁶⁵ Tradução nossa. No original: “[...] solidifies the reality that negligent errors in application will not undermine the constitutionality of the system. Only intentional or reckless or systemic instances of error will warrant an exclusionary rule remedy. While rights and remedies are certainly different, this forgiving of error allows a greater freedom for mistakes. If merely negligent, an error in a facial recognition match will have no consequence for police investigation.”

humilhação sofrida por Robert, Michael e Porcha, ou até mesmo por outros afrodescendente em outros estados, serão consideradas constitucionais.

Além desses três *standards*, questões como vieses raciais – intencionais ou não – e ausência de transparência e de tratamento igualitário não são levadas em consideração pela Suprema Corte na avaliação de constitucionalidade de uma abordagem policial. Isso significa que, diante de todos os problemas apontados que cercam a tecnologia – maiores taxas de erros em pessoas não-brancas e dificuldade na transparência em razão da existência de caixas-pretas inerentes ao aprendizado de máquina –, não serão levados em consideração.

Em relação aos vieses, Ferguson (2021, pp. 1.181-1.185) aponta que a Suprema Corte possui o entendimento de que a Quarta Emenda, apesar de cuidar de questões policiais, não é o local adequado para tratar de viés racial do policial como indivíduo. Isso significa que uma abordagem intencionalmente discriminatória não será considerada inconstitucional perante a Corte.

Segundo Gisela Wanderley (2016, p. 118-119), no caso *Terry v. Ohio*, apesar de ter sido suscitada a possibilidade de abuso do poder policial em face das minorias raciais, a Suprema Corte optou por não analisar a adequação da abordagem policial, restringindo-se apenas a admissibilidade das provas obtidas. Na ocasião, a Corte decidiu que, mesmo a abordagem tendo sido realizada de maneira desarrazoada, a exclusão dessas provas seria uma medida ineficaz na luta contra as diversas violações sistemáticas dos direitos de pessoas negras pelas forças policiais (Wanderley, 2016, p.118-119). Isso porque

[...] a simples declaração da ilegalidade da busca, com a conseqüente exclusão das provas obtidas no âmbito do processo penal, seria ineficiente para combater a discriminação racial pelo aparato policial, que se manifesta de variadas maneiras e em abordagens com finalidades múltiplas (Wanderley, 2016, p. 118-119).

Essa decisão abriu portas para flexibilização das abordagens policiais, ignorando as questões de discriminação racial que poderiam (e vieram) a ser agravadas por essa decisão. O assassinato constate de negros em abordagens policiais é um reflexo disso.

Pensando nas estruturas dos algoritmos,

[...] isso significaria que um sistema programado para incentivar paradas baseadas em raça não necessariamente enfrentaria problemas da Quarta Emenda. Além disso,

seria permitido incluir proxies para viés racial sobre certos grupos ou áreas no modelo de correspondência (Ferguson, 2021, p. 1.183).⁶⁶

Em relação à transparência, conforme relatado por Ferguson (2021, pp. 1.188-1.191), a polícia nos Estados Unidos, de maneira tradicional, não tem adotado práticas transparentes em questões relacionadas à formação, treinamento ou táticas de sua corporação, chegando inclusive a se autodenominar como secreta. Além disso, os governos locais têm evitado e, por vezes, resistido a diversas iniciativas de transparência.

A situação agrava ao percebermos que a Quarta Emenda não impõe a exigência de transparência por parte da polícia nem busca compreender o verdadeiro motivo que impulsionou a abordagem, desde que haja uma justificativa – como causa provável ou suspeita razoável (Ferguson, 2021, p. 1.188-1.191).

Atualmente, com o grande fluxo de informações, percebemos que, conforme explicado por Duarte e Garcia (2021, p. 13), as atividades de policiamento são “cada vez mais marcadas pelo emprego de portarias de acesso restrito, de funções de investigação não definidas em lei e pelo uso maleável da ideia de ‘atividade de inteligência’”, sendo que o que importa é o resultado e não como se chegou lá.

Dessa forma, um *software* de reconhecimento facial – que já possui embaraços com transparência por sua própria natureza – construído de acordo com os parâmetros de uma polícia dita secreta pode se tornar “uma verdadeira ‘caixa preta’ e ainda assim ser constitucional sob esta lógica”⁶⁷ (Ferguson, 2021, p. 1190).

Por fim, em relação à falta de tratamento igualitário, é evidente que a legislação deve ser aplicada de maneira igualitária, sem distinção de raça, classe social, idade ou gênero. Contudo, casos como os assassinatos de George Floyd e Eric Garner demonstram o racismo sistêmico impregnado na estrutura da polícia estadunidense, fazendo com que atue de maneira desigual e discriminatória. Infelizmente, diante dessa questão, Ferguson (2021, p. 1.185-1.188) aponta que a igualdade no tratamento dos cidadãos prevista na Quarta Emenda nunca foi uma exigência constitucional.

Referindo-se à tecnologia de reconhecimento facial e em seu funcionamento, o autor afirma que:

⁶⁶ Tradução nossa. No original: “[...] this would mean that a system programmed to encourage pretextual race-based stops would not necessarily run into Fourth Amendment problems. In addition, proxies for racial bias about certain groups or in certain areas would be permissible to include in the matching model.”

⁶⁷ Tradução nossa. No original: “[...] can be a true ‘black box’ and still be constitutional under this thinking.”

[...] qualquer desigualdade não será uma preocupação da Quarta Emenda. Reclamações de que os sistemas de correspondência de reconhecimento facial não funcionam igualmente bem em diferentes raças ou gêneros porque são treinados em conjuntos de dados sem diversidade suficiente não receberão atenção da Quarta Emenda (Ferguson, 2021, p. 1.188).⁶⁸

Diante das considerações apresentadas, é possível concluir que o arcabouço jurídico relacionado ao uso da Tecnologia de Reconhecimento Facial nos Estados Unidos está longe de ser claro e definitivo. Andrew Ferguson (2021, p. 1.191) busca nos tranquilizar ao destacar que a Corte possui a tendência de não relevar erros recorrentes ou decisões sistematicamente tendenciosas. Segundo ele:

Quanto mais programaticamente projetada e sistematizada se torna uma prática policial, maior deve ser o nível de exame e detalhamento da Quarta Emenda que ela recebe do tribunal. Como a tecnologia de reconhecimento facial é literalmente uma construção de engenharia programática e design de computador, ela receberia um exame minucioso mais rigoroso da Quarta Emenda (2021, p. 1.191).⁶⁹

No entanto, ao mesmo tempo, a constatação de que a Suprema Corte tende a relevar erros isolados e vieses raciais subjetivos dos policiais sugere uma lacuna preocupante na proteção dos direitos individuais diante do uso da Tecnologia de Reconhecimento Facial no âmbito criminal. Dessa maneira, a legislação e a jurisprudência atuais mostram-se ineficazes diante das inovações tecnológicas, deixando margem para abusos e violações de direitos, sendo necessária a elaboração de inovações legislativas caso essa ferramenta continue a ser utilizada pelas forças de segurança.

Dessa forma, diante da análise da Quarta Emenda e da jurisprudência da Suprema Corte sobre o assunto e, ainda pensando em futuros litígios em que a Tecnologia de Reconhecimento Facial possa vir a ser utilizada como prova, é necessário também analisar a viabilidade do uso dessa ferramenta como evidência sob a lente do *Daubert Standard*, gerado no caso *Daubert vs. Merrell Dow Pharmaceuticals*, julgado em junho de 1993, pela Suprema Corte.

⁶⁸ Tradução nossa. No original: “[...] any unfairness in effect will not be a Fourth Amendment concern. Complaints, then, that facial recognition matching systems do not work equally well on different races or genders because they are trained on datasets without sufficient diversity will not merit Fourth Amendment attention.”

⁶⁹ Tradução nossa. No original: “[...] the more programmatically designed and systematized a policing practice becomes, the higher level of Fourth Amendment scrutiny it should receive from the Court. As facial recognition technology is literally a construct of programmatic engineering and computer design, it would receive higher Fourth Amendment scrutiny.”

2.2.2 A TECNOLOGIA DE RECONHECIMENTO FACIAL COMO EVIDÊNCIA

No caso *Daubert vs. Merrell Dow Pharmaceuticals*, Jason Daubert e Eric Schuller, que nasceram com graves doenças congênitas, representados por seus pais, propuseram uma ação contra a Terreal Dow Pharmaceuticals Inc. sob a alegação de que o medicamento Bendectin, comercializado pela ré, teria a aptidão de causar anomalia ou doença congênitas quando usados no pré-natal (Cornell Law School, n.p.).⁷⁰

A empresa farmacêutica, por intermédio de seu perito particular, apresentou estudos publicados e aceitos pela comunidade acadêmica que comprovavam a inexistência de ligação entre o uso do medicamento no pré-natal e defeitos congênitos em humanos. Por outro lado, os autores apresentaram estudos novos realizados em animais *in vitro* e *in vivo* que evidenciavam a má-formação congênita em decorrência do uso do medicamento. Ocorre que os estudos apresentados pelos autores, apesar de amparados por 8 (oito) especialistas, não foram considerados válidos pela Suprema Corte pelo fato de a metodologia aplicada ainda não ter aceitação dentro da comunidade científica em geral (Cornell Law School, n.p.).⁷¹

Diante de toda a discussão sobre a validade dos estudos que embasaram a prova apresentada pelos requerentes, uma lista de verificação não taxativa foi criada para que o juízo de primeira instância verifique se o método utilizado por um perito – *expert witness testimony* – pode ser considerada como válido e, por consequência, pode ser usado como prova (Robinson, 2023, n.p.).⁷²

Os itens que devem ser observados são: (1) **testabilidade** – se esse método pode ser testado e, caso tenha sido, se possui a aptidão de atender a uma série de critérios exigidos na simulação de teste de maneira eficiente (Tofanini e Teixeira, 2011, p. 51); (2) **revisão e publicação** – se esse método está sendo estudado e sendo submetido a publicação e revisão por pares, o que confirma a validade da ciência relatada; (3) **taxa de erro** – se a taxa de erro desse método é conhecida, tanto taxa de erro atual quanto potencial; (4) **existência de parâmetros** que guiem o seu funcionamento; e (5) **aceitação** dentro da comunidade científica (Robinson, 2023, n.p.).⁷³

⁷⁰ Disponível em: <https://www.law.cornell.edu/supct/html/92-102.ZS.html>. Acesso em: 14 nov. 2023.

⁷¹ *Idem*.

⁷² Disponível em: https://www.law.cornell.edu/wex/daubert_standard. Acesso em: 13 nov. 2023.

⁷³ Disponível em: https://www.law.cornell.edu/wex/daubert_standard. Acesso em: 13 nov. 2023.

Com base nesses critérios e nos estudos realizados por Gabrielle Haddad (2021)⁷⁴, passemos para a análise da possibilidade de a Tecnologia de Reconhecimento Facial ser utilizada como evidência no âmbito criminal.

De início, é inequívoca a possibilidade de a Tecnologia de Reconhecimento Facial ser testada, dado que se trata de uma construção de engenharia, um produto do campo das ciências exatas, suscetível a avaliações objetivas. Os testes apresentados no capítulo anterior corroboram essa afirmação. Entretanto, conforme bem pontuado por Haddad (2021, p. 904-905), não há testes obrigatórios às empresas privadas para verificar a confiabilidade dessa tecnologia. Esse fator crucial fica a critério das próprias empresas privadas, que podem decidir se conduzem ou não esses testes e, caso realizem, têm a prerrogativa de determinar quais critérios serão analisados e se divulgam ou não os resultados para o público em geral.

Além disso, mesmo com a existência do programa de testes *Face Recognition Vendor Test* (FRVT), do *National Institute of Standards and Technology* (NIST), é comum que os algoritmos submetidos a avaliação não sejam os produtos finais em si, mas apenas protótipos, minando, dessa forma, o propósito do programa de testar a confiabilidade dos *softwares* disponíveis no mercado (Haddad, 2021, p. 905). De acordo com Haddad (2021, p. 905), essa manobra enfraquece a possibilidade de que esse tipo de tecnologia seja admitido como evidência, tendo em vista que “os relatórios mais abrangentes sobre a tecnologia de reconhecimento facial e sua precisão testam protótipos, não produtos finais”.⁷⁵

Além disso, o racismo algoritmo vem cada vez mais sendo uma preocupação que aparece em uma das fases do programa realizado pelo NIST. Como dito no capítulo anterior, estudos apontam que a Tecnologia de Reconhecimento Facial tem maiores taxas de erros em pessoas não-brancas, muito em razão do fenômeno chamado racismo algoritmo. Sobre isso, a autora aponta que, apesar da possibilidade de a tecnologia melhorar suas taxas de precisão com o tempo, “o viés atual desses sistemas é preocupante e enfraquece a alegação de que ela deve ser permitida em julgamento como evidência” (Haddad, 2021, p. 906).⁷⁶

Indo para o segundo critério – **publicação e revisão por pares** –, também é inequívoca a vasta existência de estudos publicados e revisados sobre a Tecnologia de Reconhecimento Facial. No entanto, há um fator que mina a viabilidade do uso dessa ferramenta como evidência.

⁷⁴ Em seu texto “Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom”.

⁷⁵ Tradução nossa. No original: “[...] the most comprehensive reports on facial recognition technology and its accuracy test prototypes, not final products.”

⁷⁶ Tradução nossa. No original: “[...] the current bias in these systems is concerning and weakens the claim that it should be allowed into trial as evidence.”

Segundo Haddad, os *softwares* utilizados pelos departamentos de polícia são de empresas privadas contratadas e, em razão disso, é ínfima a possibilidade de a comunidade científica avaliar e analisar o funcionamento de cada *software* de cada empresa, isso porque, para analisar a confiabilidade dessa ferramenta, é necessário ter acesso ao código-fonte do *software*, algo muito dificilmente divulgado pelas empresas privadas em razão de competitividade no mercado (Haddad, 2021, p. 906).

Em relação ao terceiro critério, a autora nos alerta sobre a existência de dois tipos de **taxas de erro** que devem ser observados. O primeiro é definido com taxa de erro originária, relacionada aos vieses embutidos na tecnologia em razão dos dados de treinamentos.

O segundo tipo de taxa de erro é o mais preocupante por ser o mais difícil de se estabelecer, tendo em vista que se refere à precisão, ou falta dela, do algoritmo quando exposto a dados diferentes dos utilizados em seu treinamento. Em outras palavras, enquanto a taxa de erro originária é calculada em um ambiente controlado, como um laboratório, a taxa de erro potencial refere-se à performance do *software* quando confrontado com o mundo real (Haddad, 2021, p. 906-907).

Como mostrado no capítulo anterior, fatores externos ao algoritmo como condições da câmera e do ambiente podem interferir de maneira significativa nos resultados obtidos pela máquina. Além disso, fatores internos com a insuficiência de dados em razão de vieses raciais interferem no desempenho da máquina quando aplicada no mundo real. Diante disso, determinar a taxa de erro de maneira precisa é uma tarefa árdua, tendo em vista a variedade de porcentagens de erro que podem aparecer tanto em razão do ambiente, tanto em razão das características únicas de cada indivíduo.

Em relação ao quarto critério, deve-se analisar a **existência de parâmetros** que guiam o funcionamento da tecnologia. Nesse ponto, voltamos à problemática das empresas desenvolvedoras dessa tecnologia e a competitividade no mercado, pois “as empresas desenvolvem sua própria tecnologia de reconhecimento facial e mantêm suas informações para si mesmas” (Haddad, 2021, p. 907).⁷⁷ Dessa maneira, torna-se dificultosa a tarefa de estabelecer padrões de funcionamento, de desenvolvimento e até mesmo de regulação da Tecnologia de Reconhecimento Facial, para que funcionem de maneira semelhante e previsível.

Por fim, sobre a **aceitabilidade da tecnologia**, de modo geral, a Inteligência Artificial e as técnicas de aprendizado de máquina são aceitas pela comunidade científica, bem como a

⁷⁷ Tradução nossa. No original: “Companies develop their own facial recognition technology and keep their information to themselves.”

Tecnologia de Reconhecimento Facial e uma variedade de testes realizados (Haddad, 2021, p. 907-908). No entanto, o seu pelas forças de segurança é bastante discutido e atacado, tendo em vista todas as problemáticas apresentadas até este ponto.

Contudo, a Tecnologia de Reconhecimento Facial, apesar de ser passível de testes, ter revisões e publicações sobre o assunto e ter uma taxa de erro conhecida, enfrenta uma série de desafios que comprometem sua viabilidade como evidência. A complexidade e especificidade dessa ferramenta revelam que, embora seja uma ferramenta aceita no âmbito acadêmico, sua aplicação como prova é suscetível a inúmeros obstáculos.

Como dito anteriormente, esses cinco fatores não são taxativos e, ainda que um deles esteja ausente, o juízo pode aceitar a prova e, caso reportem necessário, sua decisão poderá ser revista por um tribunal superior. Contudo, ainda que a prova seja admitida, é necessário observar outros fatores para determinar a potencialidade da Tecnologia de Reconhecimento Facial ser usada como prova.

Um termo que encapsula a essência dessas considerações é "transparência", ou a falta dela. A título de exemplificação, toda prova deve possuir a capacidade de ser contestada, e quando se trata de uma ferramenta algorítmica, o acesso ao seu código-fonte é fundamental. Isso porque o código-fonte tem o papel de fornecer todas as instruções, expressas em linguagem de computação, para um programa de computador sobre quais tarefas deverão ser executadas como deverão ser executadas e como deverão ser apresentadas. Dessa forma, a forma mais eficaz para o réu poder contestar uma prova obtida por um *software* de reconhecimento facial é ter acesso ao código-fonte, pois é por meio dele que se tem acesso ao funcionamento interno do algoritmo (Haddad, 2021, p. 910).

Observar o código-fonte, segundo a analogia feita pela autora, seria como “olhar debaixo do capô” de um carro (Haddad, 2021, p. 910). Essa correlação serve para ilustrar a diferença entre simplesmente observar o resultado de uma ação e compreender os mecanismos internos que a impulsionam.

Poder olhar “embaixo do capô” de um *software* de reconhecimento facial possibilita avaliar o cumprimento dos fatores de Daubert, ou seja, o réu tem a possibilidade de comprovar a (im)precisão da ferramenta utilizada para condená-lo, como também verificar a confiabilidade, a validade e a eficiência da ferramenta bem com os testes utilizados para treiná-la e também verificar quais testes deveriam ter sido feitos e não foram.

Contudo, esse requisito colide novamente com questões de privacidade e competitividade de mercado, especialmente no contexto das empresas privadas que desenvolvem essas tecnologias. Isso porque as empresas privadas possuem o privilégio de

segredo comercial dos desenvolvedores, tendo a prerrogativa de não divulgarem detalhes de sua tecnologia em razão do fato de estarem competindo em um mercado com outras empresas, tornando um obstáculo considerável para os réus que possuem condições de recorrer e exigir tal medida.

Essa ausência de regulamentação e transparência pode ser interpretada como um reflexo da influência e do poder exercidos pelos detentores e criadores dessa tecnologia, deixando o Estado à margem da discussão. Além disso, é um reflexo das hierarquias coloniais, em especial, da raça e da branquidade (Duarte e Garcia, 2021, p. 3), revelando que:

as tecnologias punitivas nascem da imaginação colonial, nas relações de poder inscritas na modernidade ocidental. Elas não são nem europeias ou estadunidenses, nem locais ou estrangeiras, são coloniais, ou seja, são concebidas na experimentação e nas disputas dos processos de dominação, e produzidas por meio da sua circulação e justaposição (Duarte e Garcia, 2021, p. 19).

Não é incomum ver as empresas desenvolvedoras de tecnologias invocarem o privilégio de segredo comercial quando o réu tenta exercer seu direito de confrontar as provas apresentadas contra si. A título de exemplo, no Estado da Califórnia, a Corte de Apelações cassou decisão proferida em primeiro grau que havia determinado que o desenvolvedor de software forense de análise de DNA oportunizasse o acesso do código-fonte ao réu, que estava sendo acusado de cometer um homicídio. A Corte de Apelações entendeu que o privilégio de segredo comercial deveria ser assegurado, em detrimento ao direito de defesa do réu, o qual seria exercido mediante acesso ao código-fonte para confrontar e interrogar uma testemunha (Haddad, 2021, p. 911-913).

Conforme brilhantemente pontuado por Evandro Piza Duarte (2021):

A Suprema Corte Americana, ao longo de sua história, decidiu inúmeras vezes sobre casos nos quais o racismo era o tema central, sem jamais tocar no assunto e, quando o fez, construiu o belo conceito de diversidade das instituições sem questionar o próprio poder da branquidade (WARE, 2007) resultante do colonialismo e da escravidão (Duarte, Queiroz, 2017) (Duarte, 2021, p. 37).

Além desses fatores externos, a própria estrutura da ferramenta é misteriosa pela existência das chamadas “caixas-pretas”, como discutido no capítulo anterior. Esses elementos adicionam camadas de complexidade à utilização da Tecnologia de Reconhecimento Facial como prova, destacando a importância da transparência na sua aplicação jurídica.

Diante de todo o exposto, restou evidenciado a complexidade e especificidade do uso da Tecnologia de Reconhecimento Facial como meio de prova no âmbito da jurisdição criminal.

Em razão disso, como já ressaltado anteriormente, essas transformações tecnológicas causam uma perturbação no equilíbrio constitucional vigente, fazendo com que atores políticos reajam por meio de respostas normativas para equilibrar essas transformações e inovações com a proteção dos direitos fundamentais e a manutenção do equilíbrio dos poderes e das instituições jurídicas preexistentes.

Dessa forma, na próxima seção, serão expostas as reações embrionárias já existentes e as recomendações de estudiosos sobre o tema, de modo a guiar e assistir a constitucionalização do ambiente digital.

2.3. A REGULAMENTAÇÃO DA TECNOLOGIA DE RECONHECIMENTO FACIAL

Inicialmente, ficou evidente que a atual posição da Suprema Corte em relação à Quarta Emenda é insuficiente quando se trata de potenciais equívocos em abordagens policiais. Isso significa que, diante de todas as questões destacadas em torno da tecnologia, estas novas questões não serão levadas em consideração. Além disso, as experiências humilhantes vivenciadas por Robert, Michael e Porcha podem ser consideradas constitucionais caso uma mudança jurisprudencial não ocorra.

Em seguida, a análise dos fatores de Daubert apontou diversos fatores que dificultam o uso do reconhecimento facial como evidência. A falta de transparência por parte de empresas desenvolvedoras na realização de testes do dispositivo; a dificuldade em estabelecer as taxas de erros potências da máquina quando confrontada com o mundo real; a inexistência de parâmetros que guiem seu funcionamento; e a dificuldade em poder contestar esse tipo de prova foram alguns dos elementos que possuem o potencial de minar a viabilidade do uso dessa tecnologia como prova caso não haja regulação.

Neste contexto, serão apresentadas algumas recomendações para produções legislativas, com base nos estudos de Andrew Ferguson (2021) e Gabrielle Haddad (2021), na tentativa de orientar o uso responsável da Tecnologia de Reconhecimento Facial pelas forças de segurança.

De início, é possível sugerir a limitação do uso dessa tecnologia na modalidade de vigilância facial⁷⁸, como forma de evitar buscas generalizadas por meio do reconhecimento facial sem qualquer fundamentação. Restrições devem ser estabelecidas para evitar a vigilância

⁷⁸ A **Vigilância Facial** tem o objetivo de monitorar locais públicos e fazer a identificação em massa de indivíduos. Nesse método não há um suspeito específico.

indiscriminada ou o uso da tecnologia para monitoramento constante de cidadãos. Isso significa vetar o monitoramento de locais públicos sem qualquer fundamentação específica por meio dessa ferramenta, além de proibir a coleta de informações pessoais dos cidadãos como localização e hábitos diários, salvo em situações de emergência (Ferguson, 2021, p. 1.197-1.199).

Nos Estados Unidos, 17 cidades⁷⁹ já proibiram o uso governamental de reconhecimento facial.

Em seguida, há considerações a serem feitas que devem ser observadas na fase pré-processual, em que se busca esclarecer os fatos ocorridos e formar uma *opinio delicti*. De início se faz necessária a exigência de um mandado baseado em uma fundada suspeita – causa provável – para que buscas de identificação facial⁸⁰ sejam realizadas. Esse requisito tem o objetivo de evitar que a identificação facial sem mandado se torne uma medida do cotidiano policial, guardando essa ferramenta para crimes específicos de maior ofensividade (Ferguson, 2021, p. 1.199-1.202).

Adotar essa medida traria benefícios adicionais, pois, segundo Ferguson,

o processo de mandado gerará um registro escrito que permitirá uma medida de transparência, responsabilidade e prevenção de abusos. Os mandados de causa provável não servem apenas para justificar uma intrusão na privacidade pessoal, mas também para documentar o uso após o fato (2021, p. 1.201).⁸¹

Com esse documento escrito, espera-se que seja documentado também as possíveis correspondências à foto buscada. Ou seja, se em uma busca foram identificados 20 outros suspeitos, que essas 20 outras possibilidades sejam documentadas e armazenadas para uma possível contestação pelo réu (Ferguson, 2021, p. 1.209).

Infelizmente, é necessário pontuar que, além das medidas de banimento local da tecnologia por algumas cidades, o congresso estadunidense vem tentando implementar legislações federais que regulem o assunto, mas acabam não sendo aprovadas por conflito de interesses. Uma delas foi o *Facial Recognition Technology Warrant Act*, que almejava

⁷⁹ A título de curiosidade, são eles: Berkeley (CA); Boston (MA); Brookline (MA); Cambridge (MA); Condado de King (WA); Madison (WI); Minneapolis (MN); Nova Orleans (LA); Northampton (MA); Oakland (CA); Pittsburgh (PA); Portland (ME); Portland (OR); São Francisco (CA); Santa Cruz (CA); Somerville (MA); e Springfield (MA). Disponível em: <https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition>. Acesso em: 20 nov. 2023.

⁸⁰ A **Identificação Facial** tem o objetivo de determinar a identidade de um rosto específico mediante a correspondência entre uma imagem e um banco de dados. Foi o que ocorreu com Robert, Michal e Porcha.

⁸¹ Tradução nossa. No original: “[...] the warrant process will generate a written record allowing for a measure of transparency, accountability, and avoidance of abuse. Probable cause warrants are not simply about justifying an intrusion into personal privacy but also about documenting the use after the fact.”

justamente isso, a expedição de um mandado baseado em uma fundada suspeita para o uso dessa ferramenta em situação de vigilância facial (Haddad, 2021, p. 900-901).

Além disso, outra recomendação a ser feita diz respeito à necessidade de realizar investigações mais aprofundadas após a obtenção de um resultado de identificação. A Tecnologia de Reconhecimento Facial pode ser uma ferramenta útil para impulsionar a investigação, servindo como ponto de partida para romper a inércia. No entanto, é crucial compreender que não deve ser considerada como uma verdade absoluta, até por ser uma ferramenta passível de muitos erros.

Em relação ao rastreamento facial,⁸² há defensores da proibição total desse tipo de mecanismo, muito em razão da desconfiança na possibilidade de uso dessa ferramenta pelas forças de segurança, devido ao estado embrionário da tecnologia que muito tem a evoluir e à falta de preparo dos policiais que podem usar de maneira indevida contra minorias (Ferguson, 2021, p. 1.202-1.205).

No entanto, é possível limitar o uso do rastreamento facial para crimes específicos. Pegando de exemplo a nossa Lei de Interceptação Telefônica – Lei nº 9.296, de 24 de julho de 1996 –, o rastreamento facial só deve vir a ser utilizado como a última ferramenta possível, ou seja, caso a prova não seja possível ser obtida por outros meios disponíveis. Além disso, é imprescindível haver indícios mínimos de autoria ou participação em infração penal, além do delito ser de maior ofensividade ou até mesmo restringindo aos hediondos.

Indo para a ação penal, outros requisitos devem ser estabelecidos. Inicialmente, o uso da Tecnologia de Reconhecimento Facial como meio de obtenção de prova deve ser evitado até que padrões de funcionamento ou protocolos de testes sejam estipulados ou um mecanismo de impugnação da prova obtida por essa ferramenta seja fornecido (Haddad, 2021, p. 915-916).

Ainda nessa linha de raciocínio, é necessário estabelecer ferramentas de impugnação para o réu confrontar as provas contra si – como fornecendo o código-fonte –, mas que equilibrem com o direito de proteção dos desenvolvedores dos softwares sem que mine o incentivo a inovação (Haddad, 2021, p. 916-917).

Gabrielle Haddad (2021) cita como exemplo o fornecimento do acesso ao código-fonte, mas com a sujeição de certos termos.

Por exemplo, os tribunais exigiram a divulgação sujeita a medidas cautelares com restrições diversas: os peritos com acesso concedido estão sujeitos a verificação; os peritos assinam uma declaração reconhecendo a sua obrigação de não divulgar a

⁸² **Rastreamento Facial** busca identificar a localização em tempo real do suspeito a partir da identificação de seu rosto em sistemas de vigilância em massa.

informação protegida; os peritos estão autorizados a estudar a informação exclusivamente em áreas seguras; e os especialistas têm de realizar as suas análises em computadores protegidos (2021, p. 917).⁸³

Isso porque o congresso também já propôs a criação do chamado *Justice in Forensic Algorithms Act* em que visava fornecer amplamente o acesso aos réus sem nenhuma garantia aos desenvolvedores. No entanto, esse projeto de lei proposto não foi aprovado por desincentivar a inovação tecnológica (Haddad, 2021, p. 916-917).

No geral, implementar um sistema de “auditoria algorítmica” pode ser uma alternativa para verificar questões envolvendo preconceitos, segurança e transparência. Com um órgão responsável por esse tipo de regulação, espera-se que mecanismos de prestação de contas sejam implementados para garantir maior transparência e responsabilidade das agências em relação ao uso adequado da tecnologia.

Ainda como possíveis atribuições a este órgão, avaliações regulares do impacto da ferramenta na sociedade, incluindo análises de seus efeitos sobre as comunidades mais vulneráveis, são atividades que devem ser realizadas. Bem como o incentivo de testes dos *softwares* utilizados pelos departamentos de polícia, mas de maneira que assegure o sigilo comercial, incentivando a competitividade e inovação tecnológica.

Além do mais, caso não seja viável a criação de um novo órgão específico, Pedro Sousa (2022, p. 103) no orienta o aproveitamento de uma “estrutura de um órgão já existente, como a Autoridade Nacional de Proteção de Dados, que possui vocação tecnológica desde seu nascimento”.

Ademais, é imperativo o treinamento adequado dos agentes que irão utilizar essas ferramentas nas ruas ou em uma investigação criminal. É necessário terem o conhecimento básico do funcionamento da tecnologia bem como os desafios que enfrentam – com os fatores extrínsecos e intrínsecos que influenciam os resultados obtidos. A conscientização sobre os limites da tecnologia e suas possíveis consequências devem ser amplamente promovidas entre os profissionais da área. Aliado a esse treinamento, é primordial a colaboração das forças de segurança com especialistas sobre o assunto para que a implementação e o aprimoramento contínuo do uso da Tecnologia de Reconhecimento Facial.

⁸³ Tradução nossa. No original: “For example, courts have required disclosure subject to protective orders with varying constraints: the experts granted access are subject to vetting; the experts sign a declaration to acknowledge their obligation not to circulate the protected information; the experts are allowed to study the information exclusively in secure areas; and the experts have to conduct their analysis on protected computers.”

Antes de finalizar, cabe mencionar, como forma de enriquecer as recomendações aqui delineadas, o *Artificial Intelligence Act* da Comissão Europeia que apresenta uma “limitação e controle de determinadas aplicações críticas de algoritmos” (Sousa, 2022, p. 102). Esse regramento é uma inovação regulatória por abordar os riscos inerente ao uso da IA apresentando um conjunto de obrigações e requisitos no objetivo de salvaguardar os direitos fundamentais dos cidadãos da União Europeia (Hoffmann, 2023, n.p.).⁸⁴

Por fim, a Tecnologia de Reconhecimento Facial deve ser utilizada de maneira específica e proporcional. É inegável a utilidade dessa ferramenta em buscas de pessoas desaparecidas, soluções de assassinatos e outras situações em que somente os olhos humanos ou o focinho de um cão não seriam capazes de solucionar. No entanto, é necessário olhar as diversas violações e discriminações que o uso de uma tecnologia embrionária, enviesada e desregulada está causando em pessoas que sempre estão na mira das forças de segurança.

⁸⁴ Disponível em: <https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/#:~:text=The%20AI%20Act%20is%20a,systems%20across%20EU%20member%20states>. Acesso em: 22 nov. 2023.

CONCLUSÃO

O presente trabalho apresentou, em seu primeiro capítulo, os conceitos de Constitucionalismo Digital e constitucionalização do ambiente digital, que, em síntese, possuem o objetivo de equilibrar as transformações ocasionadas pelo avanço tecnológico com a proteção dos direitos fundamentais e a manutenção do equilíbrio dos poderes preexistentes.

Em seguida, expôs o conceito de racismo estrutural algorítmico, o qual foi definido como sendo a contaminação da estrutura dos algoritmos pelo próprio preconceito humano, tendo o potencial de disseminá-lo e ampliá-lo. Além disso, demonstrou a sua forma de operação nos *softwares* de reconhecimento facial, a partir da apresentação de pesquisas em que foram obtidas maiores taxas de erro no reconhecimento de pessoas não-brancas, sendo estas taxas definidas como microagressões.

Posteriormente, foram fornecidos conceitos introdutórios relativos à Tecnologia de Reconhecimento Facial, a qual foi definida como sendo um termo guarda-chuva que abarca todo o tipo de ferramenta digital que possui a finalidade de operar imagens fornecidas de rostos humanos com as constantes em bancos de imagem preexistentes. Além disso, apresentou-se uma síntese do seu funcionamento e suas aplicações no âmbito da segurança pública.

Em seu segundo capítulo, foram apresentados os casos de Robert Williams, Michael Oliver e Porcha Woodruff, 3 (três) pessoas negras que foram detidas e encarceradas de maneira equivocada após serem selecionados como possíveis autores de crimes pelo *software* de reconhecimento da *Data Works Plus* usado pelo Departamento de Polícia de Detroit – Michigan.

Em seguida, diante da análise do posicionamento jurisprudencial atual da Suprema Corte em relação à Quarta Emenda, ficou evidente a sua insuficiência frente a potenciais equívocos em abordagens policiais. Isso nos mostrou que todas as questões destacadas em torno da tecnologia – como maiores taxas de erros em pessoas de cor; a falta de transparência diante da existência das caixas-pretas; e o próprio racismo estrutural algorítmico – não serão levadas em consideração. Além disso, as experiências humilhantes vivenciadas por Robert, Michael e Porcha podem ser consideradas constitucionais caso uma mudança jurisprudencial não ocorra.

Em seguida, a análise dos fatores de Daubert apontou diversos fatores que dificultam o seu uso como evidência. A falta de transparência por parte de empresas desenvolvedoras na realização de testes do dispositivo; a dificuldade em estabelecer as taxas de erros potências da máquina quando confrontada com o mundo real; a inexistência de parâmetros que guiem seu funcionamento; e a dificuldade em poder contestar esse tipo de prova foram alguns dos

elementos que possuem o potencial de minar a viabilidade do uso dessa tecnologia como prova caso não haja regulação.

Nesse contexto, foram apresentadas algumas recomendações para produções legislativas na tentativa de orientar o uso responsável da Tecnologia de Reconhecimento Facial pelas forças de segurança, como: (1) a limitação do uso dessa tecnologia na modalidade de vigilância facial (Ferguson, 2021, p. 1.197-1.199); (2) a exigência de um mandado baseado em uma fundada suspeita para que buscas de identificação facial sejam realizadas (Ferguson, 2021, p. 1.201); (3) a necessidade de realizar investigações mais aprofundadas após a obtenção de um resultado de identificação; (4) a limitação do uso do rastreamento facial para crimes específicos; (5) a criação de padrões de funcionamento ou protocolos de testes (Haddad, 2021, p. 915-916); (6) o fornecimento de mecanismo de impugnação da prova obtida por essa ferramenta (Haddad, 2021, p. 916-917); e (7) eventualmente a criação de um sistema de “auditoria algorítmica” para verificar questões envolvendo preconceitos, segurança e transparência.

Por último, tendo em vista a relevância do tema, mostra-se imperioso o conhecimento dos limites e problemáticas que essa ferramenta apresenta por parte dos profissionais que irão utilizá-la em locais de crime, busca e apreensão e demais abordagens policiais. Ademais, é recomendável aos magistrados cautela ao excluírem ou admitirem uma prova obtida por meio da Tecnologia de Reconhecimento Facial, até porque, devido ao estado inicial dessa tecnologia e de legislações que busquem regulá-la, pode contribuir para que injustiças e insegurança jurídica ocorram.

REFERÊNCIAS BIBLIOGRÁFICAS

ACLU of Michigan Complaint re Use of Facial Recognition. **ACLU**, 24 jun. 2020. Disponível em: <https://wp.api.aclu.org/documents/aclu-michigan-complaint-re-use-facial-recognition>. Acesso em: 1 nov. 2023.

AFTER Third Wrongful Arrest, ACLU Slams Detroit Police Department for Continuing to Use Faulty Facial Recognition Technology. **ACLU**, 6 ago. 2023. Disponível em: <https://www.aclu.org/press-releases/after-third-wrongful-arrest-aclu-slams-detroit-police-department-for-continuing-to-use-faulty-facial-recognition-technology>. Acesso em: 7 set. 2023.

ALLYN, Bobby. ‘The Computer Got It Wrong’: how facial recognition led to false arrest of black man, **WLIW-FM**, 24 jun. 2020. Disponível em: <https://www.wliw.org/radio/news/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michigan/>. Acesso em: 16 out. 2023.

ALMEIDA, Silvio Luiz de. **Racismo estrutural**. São Paulo: Pólen, 2019.

AMARAL, Augusto Jobim do; MARTINS, Fernanda; ELESBÃO, Ana Clara. Racismo algorítmico: Uma análise da branquitude nos bancos de imagens digitais. **Pensar: Revista de Ciências Jurídicas**, v. 26, n. 4, p. 1-9, 2021. Disponível em: <https://ojs.unifor.br/rpen/article/view/11806/6702>. Acesso em: 5 set. 2023.

ANDERSON, Elisha. Controversial Detroit facial recognition got him arrested for a crime he didn’t commit. **Detroit Free Press**, 10 jul. 2020. Disponível em: <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/>. Acesso em: 7 set. 2023.

BERMAN, Paul Schiff. Cyberspace and the State Action Debate: the cultural value of applying constitutional norms to ‘private’ regulation. **University of Colorado Law Review**, v. 71, n. 4, 2000. Disponível em: <https://ssrn.com/abstract=228466>. Acesso em: 12 out. 2023.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. **Proceedings of Machine Learning Research**, v. 81, p. 1–15, 2018. Disponível em: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em: 5 set. 2023.

BUOLAMWINI, Joy; ORDONEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. **Facial Recognition Technologies: A Primer**. University of Massachusetts, 2020. Disponível em: <https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf>. Acesso em: 28 set. 2023.

CALIFORNIA. **Executive Order 12-23, 06 de setembro de 2023**. Disponível em: <https://www.gov.ca.gov/wp-content/uploads/2023/09/AI-EO-No.12--GGN-Signed.pdf>. Acesso em: 18 out. 2023.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. **International Review of Law, Computers & Technology**, v. 33, n. 1, p. 76-99, 2019. Disponível em: <https://www.tandfonline.com/action/showCitFormats?doi=10.1080%2F13600869.2019.1562604>. Acesso em: 5 set. 2023.

CHICKLAS, Dana. Farmington Hills Father Sues Detroit Police Department For Wrongful Arrest Based On Faulty Facial Recognition Technology, **ACLU**, 13 abr. 2021. Disponível em: <https://www.aclumich.org/en/press-releases/farmington-hills-father-sues-detroit-police-department-wrongful-arrest-based-faulty>. Acesso em: 3 nov. 2023.

CORNELL LAW SCHOOL. DAUBERT et ux., individually and as guardians and litem for DAUBERT, et al. v. MERRELL DOW PHARMACEUTICALS, INC. **Legal Information Institute**, [s.d.]. Disponível em: <https://www.law.cornell.edu/supct/html/92-102.ZS.html>. Acesso em: 14 nov. 2023.

DA SILVA, Mozart Linhares; ARAÚJO, Willian Fernandes. Biopolítica, racismo estrutural-algorítmico e subjetividade, **Educação Unisinos**, v. 24, 2020. Disponível em: <https://revistas.unisinos.br/index.php/educacao/article/view/edu.2020.241.40/60748039>. Acesso em: 5 set. 2023.

DATATILSYNET. **Artificial intelligence and privacy**. Oslo, Noruega: Norwegian Data Protection Authority, 2018. Disponível em: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Acesso em: 19 out. 2020.

DAVENPORT, Thomas; KALAKOTA, Ravi. The potential for artificial intelligence in healthcare. **Future Healthcare Journal**, v. 6, n. 2, p. 94-98, 2019. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6616181/>. Acesso em: 27 set. 2023.

DUARTE, Evandro Piza. Diálogos com o “realismo marginal” e a crítica à branquidade: por que a dogmática processual penal “não vê” o racismo institucional da gestão policial nas cidades brasileiras? In: DUARTE, Evandro Piza; SANTOS, Fernando Nascimento dos; MAGALHÃES, Camilla (coords.). **Lições de Dogmática Crítica: direitos fundamentais dos identificados como suspeitos na atividade policial**. São Paulo: Dialética, 2021.

DUARTE, Evandro Piza; SILVA, Thales Cassiano. A Interpretação da Prova Ilícita como Garantia Processual Penal na Suprema Corte dos Estados Unidos, De Weeks (1914) A Hering (2013): Breves Apontamentos Sobre a Convergência Axiológica, ou não, com a Prova Ilícita no Brasil. **Revista de Direito Brasileira**, v. 27, n. 10, p. 216-240, 2021. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/3937>. Acesso em: 25 nov. 2023.

DUARTE, Evandro; GARCIA, Rafael Deus. Novos Regimes de Visibilidade da Vigilância e Inteligência Artificial na Segurança Pública? Um diálogo sobre Tecnologias de Controle Social desde a Criminologia Decolonial. In: PINHO, Ana Carolina (coord.). **Discussões sobre Direito na Era Digital**. Rio de Janeiro: GZ, 2021.

ESTADOS UNIDOS DA AMÉRICA. Constituição. **Emenda Constitucional n. 4, 1789**. Disponível em: <https://constitution.congress.gov/constitution/amendment-4/>. Acesso em: 25 nov. 2023.

ESTADOS UNIDOS DA AMÉRICA. Departamento de Justiça dos EUA. **Uma breve explicação da causa provável para as autoridades estrangeiras**. Abr. 2022. Disponível em: <https://www.justice.gov/criminal-oia/file/1501821/download> . Acesso em: 9 nov. 2023.

ESTADOS UNIDOS DA AMÉRICA. Estado do Michigan. Wayne County Circuit Court. **MICHAEL OLIVER, Plaintiff v. DONALD BUSSA, in his individual and official capacity, STEPHEN CASSINI, an individual and CITY OF DETROIT**. Disponível em: <https://s3.documentcloud.org/documents/7202332/Draft-of-Michael-Oliver-Complaint-changes932020-1.pdf>. Acesso em: 6 nov. 2023.

FEINER, Lauren; PALMER, Annie. Rules around facial recognition and policing remain blurry. **CNBC**, 12 jun. 2021. Disponível em: <https://www.cnn.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html>. Acesso em: 9 out. 2023.

FERGUSON, Andrew. Facial Recognition and the Fourth Amendment. **Minnesota Law Review**, v. 105, p. 1105-1210, 2021. Disponível em: https://digitalcommons.wcl.american.edu/facsch_lawrev/742 Acesso em: 12 maio 2023.

FITZGERALD, Brian. Software as Discourse? A Constitutionalism for Information Society. **Alternative Law Journal**, v. 24, n. 3, p. 144-149, 1999. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/alterlj24&div=37&id=&page=>. Acesso em: 12 out. 2023.

GARVIE, Clare; BEDOYA, Alvaro M.; FRANKLE, Jonathan. The Perpetual Line-Up: Unregulated Police Face Recognition In America. **Center on Privacy & Technology at Georgetown Law**, 18 out. 2016. Disponível em: <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf>. Acesso em: 18 out. 2023.

GILLESPIE, Tarleton. A relevância dos algoritmos. **Parágrafo**, v. 6, n. 1, 2018. Disponível em: <https://revistaseletronicas.fiamfaam.br/index.php/recicofi/article/view/722> Acesso em: 20 set. 2023.

HADDAD, Gabrielle M. Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom. **Vanderbilt Journal of Entertainment and Technology Law**, v. 23, n. 4, 2021. Disponível em: <https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss4/5>. Acesso em: 9 nov. 2023.

HILL, Kashmir. Eight Months Pregnant and Arrested After False Facial Recognition Match. **The New York Times**, 6 ago. 2023. Disponível em: <https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html>. Acesso em: 6 nov. 2023.

HOFFMANN, Mia. The EU AI Act: A Primer. **Center for Security and Emerging Technology**, 26 set. 2023. Disponível em: <https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/#:~:text=The%20AI%20Act%20is%20a,systems%20across%20EU%20member%20states> . Acesso em: 22 nov. 2023.

HOUSE Committee on the Judiciary. Facial Recognition Technology: Examining Its Use by Law Enforcement. (3h 28min). **YouTube**, 2021. Disponível em: <https://www.youtube.com/watch?v=KVr7uoEvhsK>. Acesso em: 12 maio 2023.

INFORMATION Commissioner's Office. **Glossary**. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/glossary/?q=gradient>. Acesso em: 4 out. 2023.

JAKHAR, Pratik. Coronavirus: China's tech fights back. **BBC**, 3 mar. 2020. Disponível em: <https://www.bbc.com/news/technology-51717164>. Acesso em: 4 out. 2023.

LIMA, Bruna Dias Fernandes. **Racismo algorítmico**: o enviesamento tecnológico e o impacto aos direitos fundamentais no Brasil. 2022. 127 f. Dissertação (Mestrado em Direito) – Universidade Federal de Sergipe, São Cristóvão, 2022.

LIN, Shang-Hung. An Introduction to Face Recognition Technology. **Informing Science**, v. 3, n. 1, 2000. Disponível em: https://www.researchgate.net/publication/26388489_An_Introduction_to_Face_Recognition_Technology. Acesso em: 18 set. 2023.

NASCIMENTO, Abdias do. **O genocídio do negro brasileiro**: processo de um racismo mascarado. São Paulo: Perspectiva, 1978.

O' NEILL, Natalie. Faulty Facial Recognition Led to His Arrest – Now He's Suing, **Motherboard**, 4 set. 2020. Disponível em: <https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing>. Acesso em: 31 out. 2023.

PASQUALE, Frank. **The Black Box Society**. Cambridge: Harvard University Press, 2015.

PEIXOTO, Fabiano Hartmann. **Direito e Inteligência Artificial**. Vol. 2. Brasília: DR.IA, 2020. Disponível em: www.dria.unb.br. Acesso em: 11 nov. 2023.

ROBINSON, Jim. Cornell Law School. Daubert Standart. **Legal Information Institute**, 2023. Disponível em: https://www.law.cornell.edu/wex/daubert_standard. Acesso em: 13 nov. 2023.

SCHERTEL MENDES, Laura; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Acesso em: 5 set. 2023.

SEPARADOS, mas iguais. Direção: George Stevens Jr. Estados Unidos da América: New Liberty Production, 1991. 190 min. Disponível em: <https://www.youtube.com/watch?v=oGMSf87hLbQ>. Acesso em: 31 out. 2023.

SHEARD, Nathan; SCHWARTZ, Adam. The Movement to Ban Government Use of Face Recognition. **Electronic Frontier Foundation**, 5 maio 2022. Disponível em: <https://www EFF.org/deeplinks/2022/05/movement-ban-government-use-face-recognition>. Acesso em: 20 nov. 2023.

SILVA, Tarcízio. Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. In: SILVA, Tarcízio (org.). **Comunidades, algoritmos e ativismos digitais: Olhares afrodiaspóricos**. São Paulo: LiteraRUA, 2020.

SOUSA, Pedro. **Direito penal nos tempos da inteligência artificial: uma análise da responsabilidade dos agentes envolvidos no desenvolvimento e na operação de algoritmos de seleção e recrutamento em relação ao crime de racismo previsto no art. 4º da lei 7.716/1989**. 2023. 123 f. Dissertação (Mestrado em Direito Constitucional) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022.

STOKES, Elaisha. Wrongful arrest exposes racial bias in facial recognition technology. **CBS News**, 19 nov. 2020. Disponível em: <https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/>. Acesso em: 7 set. 2023.

SUZOR, Nicolas Pierre. **Digital constitutionalism and the role of the rule of law in the governance of virtual communities**. Thesis (PhD in Philosophy) – Queensland University of Technology, Brisbane, Australia, 2010. Disponível em: https://eprints.qut.edu.au/37636/1/Nicolas_Suzor_Thesis.pdf. Acesso em: 12 out. 2023.

SUZOR, Nicolas Pierre. Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms. **Social Media and Society**, v. 4, n. 3, p. 1-11, 2018. Disponível em: <https://eprints.qut.edu.au/120050/1/N.Suzor%20article.pdf>. Acesso em: 12 out. 2023.

TOFANINI, César Tegani; TEIXEIRA, Fábio Vieira. Testabilidade de Software: Visão Geral. **Engenho**, v. 3, p. 50-69, 2011. Disponível em: <https://revistas.anchieta.br/index.php/RevistaEngenho/article/view/806/701>. Acesso em: 13 nov. 2023.

WANDERLEY, Gisela Aguiar. Abordagem Policial Sob Suspeita: Filtragem Racial Na “StopAnd Frisk” e Controle Judicial Das Práticas Policiais A Partir Dos Casos Terry V. Ohio E Floyd V. City Of New York, **Revista de Criminologia e Políticas Criminais**, v. 2, n. 1, 2016. Disponível em: <https://indexlaw.org/index.php/revistacpc/article/view/291>. Acesso em: 25 nov. 2023.

WEST, Darrell M. California charts the future of AI. **Brookings**, 12 set. 2023. Disponível em: <https://www.brookings.edu/articles/california-charts-the-future-of-ai/>. Acesso em: 15 out. 2023.

WEX DEFINITIONS TEAM. Cornell Law School. Executive Order. **Legal Information Institute**, 12 jun. 2021. Disponível em: https://www.law.cornell.edu/wex/executive_order#:~:text=An%20executive%20order%20is%20defined,the%20legislature%20cannot%20overturn%20it. Acesso em: 18 out. 2023.

WRIGHT, Jasmine; VERITY, Andrej. Artificial Intelligence Principles For Vulnerable Populations in Humanitarian Contexts. **DH Network**, 2020. Disponível em: <https://www.digitalhumanitarians.com/artificial-intelligence-principles-for-vulnerable-populations-in-humanitarian-contexts/>. Acesso em: 9 set. 2020.