ISSN 2447-1097
DIREITO & TI
DIREITO & TI – PORTO ALEGRE / RS
WWW.DIREITOETI.COM.BR

INTELIGÊNCIA ARTIFICIAL NO RECONHECIMENTO FACIAL EM SEGURANÇA PÚBLICA: DADOS SENSÍVEIS E SELETIVIDADE PENAL.

ARTIFICIAL INTELLIGENCE IN FACE RECOGNITION IN PUBLIC SAFETY: SENSITIVE DATA AND CRIMINAL SELECTIVITY.

Janio Konno Junior[1]

Derick Moura Jorge[2]

RESUMO: O presente trabalho tem por objetivo, a partir do uso do método de abordagem lógico-dedutivo, com lastro em pesquisas bibliográficas, analisar a utilização de sistemas de reconhecimento facial, pautados em inteligência artificial, pelos órgãos de segurança pública e as possíveis violações aos direitos humanos e fundamentais na coleta e armazenamento de tais dados sensíveis, de acordo com a Lei Geral de Proteção de Dados, diante da discussão que já restou instalada acerca da utilização do reconhecimento facial como ferramenta da seletividade penal que redunda na exclusão de pessoas indesejáveis, incrementando práticas discriminatórias e desigualdades sociais, raciais e de gênero. Neste norte a pesquisa revela a necessidade de serem adotadas medidas para validação do mecanismo de reconhecimento facial, como a utilização de dados biométricos de todas as pessoas, de forma indistinta, a fim de evitar a seletividade penal, assim como a imperiosidade dos resultados servirem como indícios a serem complementados por outros elementos de informação.

Palavras-chave: Inteligência Artificial; Reconhecimento Facial; Segurança Pública; Seletividade Penal.

ABSTRACT: The present work aims, from the use of the logical-deductive method of approach, with ballast in bibliographical research, to analyze the use of facial recognition

[1] Mestre em Ciência Jurídica pela Universidade Estadual do Norte do Paraná (UENP). Investigador de Polícia Civil de São Paulo. *E-mail:* prof.janiokonnojr@gmail.com. *Lattes:* http://lattes.cnpq.br/0496454489455876.

[2] Mestre em Ciência Jurídica pela Universidade Estadual do Norte do Paraná (UENP/PR). Delegado da Polícia Civil do Paraná. *E-mail:* derickmoura@hotmail.com. *Lattes*: http://lattes.cnpq.br/1550899114585315.

systems, based on artificial intelligence, by public security agencies and the possible violations of human rights. human and fundamental in the collection and storage of such sensitive data, in accordance with the General Data Protection Law, in view of the discussion that has already been installed about the use of facial recognition as a tool of criminal selectivity that results in the exclusion of undesirable people, increasing discriminatory practices and social, racial and gender inequalities. In this north, the research reveals the need to adopt measures to validate the facial recognition mechanism, such as the use of biometric data of all people, indistinctly, in order to avoid criminal selectivity, as well as the imperative of the results to serve as a evidence to be supplemented by other pieces of information.

Keywords: Artificial Intelligence; Facial Recognition; Public Security; Criminal selectivity.

1 INTRODUÇÃO

A utilização de algumas espécies de soluções tecnológicas como forma de individualização e instrumentação à serviço da segurança pública já fez se instalarem várias discussões, sendo a mais recente polêmica resultante do reconhecimento facial por meio de inteligência artificial. Parte da discussão inicia-se com o desconhecimento, até de certa forma preconceituosa, do conceito e utilização da inteligência artificial.

Esta tecnologia emprega dados biométricos previstos na Lei Geral de Proteção de Dados (LGPD), bem como no Decreto nº 10.046/2019, razão pela qual este artigo tem por escopo analisar estas questões técnicas e jurídicas, bem como eventual impacto que decorre de seu emprego, inclusive sob o aspecto de servir como meio para reforçar a seletividade penal e a exclusão dos indesejáveis, promovendo o incremento da discriminação propiciada pelas desigualdades sociais, raciais e de gênero. Para este fim serão analisados aspectos concernentes ao uso da inteligência artificial empregada com o intuito de se obter, no espaço público, principalmente, o reconhecimento facial de pessoas.

Logo, a pesquisam almeja situar o reconhecimento facial como técnica a serviço da investigação, delimitando os seus parâmetros de utilização, estabelecendo quais diretrizes devem ser adotadas com o intuito de possibilitar a identificação da autoria

delitiva, sem serem violados os direitos básicos do ser humano relacionados à sua privacidade, bem como evitando-se práticas discriminatórias e segregacionista.

Quanto à metodologia aplicada, vale-se do processo lógico-dedutivo, com o método de investigação científica pautado em pesquisas bibliográficas em livros, artigos e reportagens, bem como na legislação pátria.

2 RECONHECIMENTO FACIAL E SEGURANÇA PÚBLICA

A biometria é uma das formas de individualização dos sujeitos aplicada pela humanidade há alguns séculos, ainda que as características físicas sempre fossem utilizadas para descrever e identificar pessoas.

Segundo consta, Alphonse Bertillon desenvolveu o primeiro método científico de identificação, em 1879. Tratava-se de um compilado de informações a serem coletadas do indivíduo, tais como descrição de sinais, fotos e impressões digitais (SOUZA, 2020, p.80).

Seguindo no curso da história outro método, que é o mais utilizado até os dias atuais, tem sido a identificação datiloscópica, criada por Juan Vucetich, que catalogou diversos presidiários na Argentina, em 1891. A técnica é relativamente simples e de baixo custo, servindo para a coleta e análise dos padrões, com alto grau de confiabilidade, de modo que isso impulsionou sua utilização, passando a ser adotada em todo o mundo. Recorrem a ela os órgãos públicos para fins de emissão de documentos e, também, empreendimentos privados, como academias de ginástica, portarias de edifícios, guichês de parques de diversão, entre outros.

A biometria evoluiu conforme as tecnologias foram sendo aplicadas e colocadas em prática para esta finalidade, a exemplo do reconhecimento facial. Hoje praticamente todo *smartphone* é dotado de sistema de leitor biométrico de impressão digital, bem como muitos também de reconhecimento facial.

Magno e Bezerra (2020, p.46) trazem o recorte histórico e situam a tecnologia da forma como é aplicada hodiernamente:

> Desenvolvida em 1964 pelo matemático e cientista da computação Woodrow Wilson Bledsoe, considerado o pai do reconhecimento facial, a tecnologia só se tornou mais perceptível nos últimos anos com o uso de aplicativos pessoais de foto e autenticação secundária para dispositivos móveis. O recurso é utilizado, principalmente, para praticidade e segurança, substituindo chaves, códigos numéricos e biometria com impressão digital e leitura da íris. Afora seu uso na indústria do entretenimento, como no Facebook e em jogos como Xbox, e controle ambiental, para proteger animais em risco de extinção, o dispositivo tem sido ferramenta de uso policial para detecção de suspeitos e criminosos. Não obstante, essa utilização é bastante controversa.

No Brasil, o Decreto nº 10.046/2019 insere, dentre os dados biométricos, características a serem utilizadas para fim de reconhecimento facial no seu artigo 2º, inciso II, no sentido de que são considerados:

> II - **atributos biométricos** - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;

Esta forma de fazer a identificação pessoal vem sendo utilizada por instituições bancárias, empresas de certificados digitais e até mesmo por órgãos governamentais, sendo que o Governo Federal, na sua plataforma gov.br, exige a leitura das características faciais para validar o acesso aos serviços digitais[3].

Redes sociais, notadamente o Facebook, utilizam API[4] de reconhecimento facial para identificar usuários em fotos de terceiros, sugerindo que se proceda a vinculação do perfil à imagem, para o fim de ampliar o número de visualizações. Para Margarete Esteves Nunes Crippa, Loryne Viana de Oliveira, Tamires Holanda e Itala Laurente (2021, p. 161-162),

> O reconhecimento facial é ainda visto como uma tecnologia promissora, este interesse se materializa no desenvolvimento de tecnologias e algoritmos de

[3] Atualmente são ofertados 4881 serviços no portal gov.br, sendo 84% totalmente digitais. https://www.gov.br/pt-br

[4] *Applications Protocol Interface* ou interface de programação de aplicações

> modo a permitir a criação de sistemas de reconhecimento facial precisos e robustos.
> A robustez dos sistemas de reconhecimento facial é uma de suas características mais críticas e frequentemente uma das mais problemáticas, e diz respeito aos parâmetros que influenciam a performance do reconhecimento facial em ambientes não controlados, bem como desafios impostos pelo envelhecimento, visibilidade parcial e expressões faciais (Mou 2010). [...] O efeito negativo de parâmetros inadequados pode ser mitigado através da ampliação do banco de dados, cujo limite é crescentemente expandido pelo potencial emprego de big data, definido como conjuntos massivos de dados que precisam ser processados e armazenados. Assim, caso o banco de dados conte com registros fotográficos diferentes — como fotos de identificação, fotos de redes sociais —, e em ambientes variados e puder atualizá-los com registros mais recentes, as técnicas de reconhecimento produzem resultados significativamente robustos (Mou 2010). As vantagens desta tecnologia sobre outras modalidades biométricas — a exemplo da invasividade nula, a tornam uma aliada em potencial para a vigilância e para a segurança pública. Tais vantagens são decorrentes do desenvolvimento e aprimoramento pelos quais vem passando a inteligência artificial.

De acordo com Eduarda Costa Almeida (2022, p. 267-268), o reconhecimento facial pode ser compreendido como:

> [...] um método de identificação de pessoas por meio de rostos capturados em vídeos, fotos ou imagens coletadas em tempo real. Majoritariamente, os sistemas de RF capturam e tratam dados considerados relevantes e únicos, como a distância entre os olhos ou o formato do queixo. Assim, à medida que as pessoas se movimentam por espaços públicos que possuem câmeras de vigilância com RF, a tecnologia isola imagens faciais e extrai dados contidos nelas. Esses dados são tratados e convertidos em representações matemáticas conhecidas como *face template*, uma assinatura facial. Essa assinatura, resultante de tratamento de uma imagem capturada em tempo real, é comparada com outras assinaturas disponíveis em uma base de dados de assinaturas faciais (EFF, 2017). Essa base de dados é uma lista de *templates* de pessoas que podem ser identificadas. No contexto da segurança pública, esse banco de dados é preenchido com assinaturas faciais de sujeitos de interesse.

Quando os dados faciais são processados por tecnologia de reconhecimento facial, a porcentagem correspondente de características semelhantes entre as duas assinaturas indica a probabilidade de a pessoa ser um dos indivíduos do banco de dados. Essa probabilidade não tem um resultado binário, pois a tecnologia não decide categoricamente se a face apresentada corresponde a um modelo existente ou não, mas numa probabilidade. Nos casos em que a tecnologia de reconhecimento facial não atua com

precisão na identificação de uma pessoa, o resultado é incorreto e ele é classificado como falso negativo ou falso positivo.

Os falsos negativos ocorrem quando o sistema não consegue corresponder um rosto à sua assinatura facial correspondente no banco de dados, ou seja, há um *template* semelhante no banco de dados, porém não é possível a correlação. Falsos positivos, por sua vez, ocorrem quando o sistema de reconhecimento facial erroneamente combina um rosto com uma assinatura facial que não está presente no banco de dados, em outros termos, a pessoa que passou pela câmera de vigilância não é a mesma que o sistema aponta.

Uma polêmica com a utilização de tecnologias de reconhecimento facial ocorreu em 2018 quando a ViaQuatro, concessionária da Linha 4 – Amarela do metrô da cidade de São Paulo instalou "portas interativas digitais" nas estações da Luz, Paulista e Pinheiros, o que redundou numa ação civil pública movida pelo IDEC – Instituto Brasileiro de Defesa do Consumidor[5]:

> Segundo a empresa, a tecnologia implementada nessas portas consiste em uma lente com um sensor que "reconhece a presença humana e identifica a quantidade de pessoas que passam e olham para a tela". O foco da ferramenta é também a identificação de emoção (raiva, alegria, neutralidade), gênero e faixa etária das pessoas posicionadas em frente ao sensor.

No caso concreto, a inteligência artificial aplicada ao reconhecimento facial, sem autorização e consentimento dos usuários do metrô, permitia a publicidade direcionada, bem como a comercialização de dados obtidos a partir das reações dos usuários, se constituindo em atividade diferente da simples publicidade, o que Shoshana Zuboff denomina de "capitalismo de vigilância" (TEÓFILO, KURTZ, PORTO JR, VIEIRA, 2019, p. 28).

A decisão de primeira instância condenou a empresa a se abster da captação destes dados dos usuários, por meio de câmeras ou outros dispositivos, sem prévio

[5] Processo nº 1090663-42.2018.8.26.0100 da 37a Vara Cível do Foro Central Cível da Comarca de São Paulo

consentimento, ratificando a liminar que já tinha sido deferida, e, no caso de continuar com a prática, que as eventuais ferramentas para a captação dos dados que fossem utilizadas, necessitavam de consentimento prévio dos usuários.

Aqui, o conceito de consentimento para tratamento desses dados pessoais, no caso as expressões faciais, encontra respaldo na Lei Geral de Proteção de Dados – Lei nº 13.709/2018, a qual em seu artigo 5º, inciso XII, dispõe ser o consentimento a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", bem como no artigo 7º, inciso I, do mesmo diploma legal, que permite o tratamento de dados "mediante o fornecimento do consentimento pelo titular".

O reconhecimento facial por meio de programas de computador, notadamente com o uso de inteligência artificial, está na pauta de discussão mundial no tema da segurança pública. Em primeiro lugar, por conta da ausência de regulamentação e eventuais abusos ou utilizações indevidas, como se abordará na sequência. Outro ponto importante é o grau de certeza no confronto das imagens e resultados inconclusivos, quando utilizados em pessoas negras, conforme noticiado pela imprensa norte-americana no ano de 2020[6].

3 INTELIGÊNCIA ARTIFICIAL

O tema inteligência artificial é cercado de uma mística, gerando curiosidade carregada com certa dose de exagero por grande parte da indústria do entretenimento. Isso se dá por conta de livros, filmes e seriados que influenciam na percepção do tema. As obras de Isaac Asimov, datadas da década de 50, passando por filmes como "2001: Uma Odisseia no Espaço", "O Exterminador do Futuro", "Eu, Robô" (inclusive baseado

[6] Polícia de Detroit: sistema de reconhecimento facial da cidade erra em 96% dos casos. O índice é pior se comparado ao da polícia de Londres, em que o software erra em 81% dos casos. https://olhardigital.com.br/2020/06/29/seguranca/policia-de-detroit-sistema-de-reconhecimento-facial-da-cidade-erra-em-96-dos-casos/

na obra de Asimov), "Inteligência Artificial" ou séries como "Black Mirror" e "Mr. Robot".

Em grande parte das obras, máquinas dotadas de inteligência artificial são capazes de tomar decisões humanas e ameaçam controlar a sociedade, gerando caos e destruição. Talvez esse viés faça parte do inconsciente humano quando se analisam questões envolvendo a inteligência artificial.

Outros exemplos de aplicação da inteligência artificial que chocou o mundo na década de 1990 foram as partidas de xadrez entre Gary Kasparov e o programa de computador *Deep Blue*, desenvolvido pela IBM. Houve dois duelos transmitidos pela televisão, com massiva cobertura da imprensa. Vale lembrar que Kasparov venceu o primeiro e Deep Blue o segundo confronto.

De maneira clara e sucinta Hoffmann-Riem (2020, p. 14) traça limites ao conceito de inteligência artificial e sua forma de utilização:

> Atualmente, as capacidades computacionais e de análise dos computadores estão sendo expandidas e as possibilidades de aplicação e desempenho dos algoritmos estão crescendo e mudando rapidamente. A chamada inteligência artificial é particularmente importante para isso. Esse termo refere-se em particular ao esforço de reproduzir digitalmente estruturas de decisão semelhantes às humanas, ou seja, de projetar um computador de tal forma e, em particular, de programá-lo usando as chamadas redes neurais de tal forma que possa processar os problemas da maneira mais independente possível e, se necessário, desenvolver ainda mais os programas utilizados.

Portanto, a inteligência artificial, em resumo, trata-se da programação de um computador para que este realize tarefas humanas, ou seja, a nomenclatura tem sido utilizada de forma incorreta, segundo alguns doutrinadores, e já era questionado por Alan Turing em outubro 1950 em seu célebre artigo "Computing Machinery and Intelligence"[7].

[7] "I PROPOSE to consider the question, 'Can machines think?' This should begin with definitions of the meaning of the terms 'machine' and 'think'. The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous. If the meaning of the words 'machine' and 'think' are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, 'Can machines think?' is to be sought in a statistical survey such as a Gallup poll. But this is absurd. Instead of attempting such a definition I shall

Em verdade, a inteligência artificial nada mais é do que um "aprendizado de máquina", que possui duas técnicas principais de abordagem: aprendizado supervisionado e não supervisionado.

Na abordagem por aprendizado supervisionado, uma grande quantidade de dados é fornecida, porém rotulados pelo programador. Nesta situação o resultado já está previsto pelo profissional que projeta a inteligência artificial, bastando que a aplicação chegue a um dos resultados. (ASHLEY, 2017, p. 427).

A inteligência artificial pressupõe uma forma de fazer o treinamento do sistema a ser alimentado, sendo que desta forma, ele se torna apto a reconhecer situações que são difíceis até os para especialistas mais habilitados, porém, a qualidade dos dados ali inseridos influencia no comportamento do sistema. Este modelo é o adotado nos casos de reconhecimento facial, como se verá adiante.

De modo singelo, o aprendizado não supervisionado não traz resultados predeterminados pelo programador, bastando que a tecnologia possa analisar a questão e agrupá-las para posterior análise do programador (ASHLEY, 2017, p.247). Para Raphael M. O. Cóbe, Luiza G. Nonato, Sérgio F. Novaes e José A. Ziebarth (2020, p. 39):

> [...] atualmente compreende diferentes áreas que incluem aprendizado de máquina, visão computacional, processamento de linguagem natural, reconhecimento de padrões em imagens, robótica, entre outras. Os avanços recentes em IA têm viabilizado a criação e o aperfeiçoamento de aplicações que vão desde veículos autônomos, diagnóstico médico, assistência física a eficientes e idosos, à segurança pública e indústria de entretenimento. As técnicas de IA, associadas à abundante quantidade de dados digitais e ao onipresente poder de processamento paralelo entregue pela computação na nuvem, deverão, sem dúvida, suprir a alta demanda pública por serviços digitais inovadores.
> O caráter transversal da IA possibilita construir soluções que permitam lidar com uma ampla variedade de problemas, trazendo melhorias socioeconômicas significativas para a sociedade. Dada essa importância, devemos estar preparados para induzir políticas públicas eficientes que contemplem aspectos técnicos, éticos e de formação de recursos humanos para permitir que acompanhemos de perto o ritmo de países que atualmente lideram os desenvolvimentos das áreas.

replace the question by another, which is closely related to it and is expressed in relatively unambiguous words" (TURING, 1950, p. 433)

Em 2016 nos Estados Unidos a rede ProPublica de jornalismo trouxe elementos concretos que apontavam para o viés discriminatório que a compilação destes dados pode provocar. Neste estudo, ficou demonstrado que os dados inseridos, no tópico que avaliava a reincidência criminal indicava terem as pessoas negras o dobro de propensão em relação às pessoas brancas (CORTIZ, 2020, p.2).

A utilização da tecnologia da informação e das novas técnicas gerenciais modificaram a atuação policial que migrou das práticas repressivas convencionais para técnicas de policiamento dirigido, comunitário e proativo, cujo objetivo foi o de corresponder aos novos tempos, visando dotar os órgãos de melhores instrumentos com vistas a melhorar a qualidade do trabalho e da vida das pessoas, contribuindo para a prevenção dos delitos (GARLAND, 2008, p. 367-368).

Constatados estes fatos, a discussão centra-se então num aspecto que tem alimentado o debate entre os pesquisadores da inteligência artificial: o fato do algoritmo[8] poder apresentar uma inclinação que seja discriminatória ou preconceituosa nos resultados que ele auxilia a construir, portanto, um aprendizado de máquina supervisionado.

Além disso tudo, ou seja, destes questionamentos já elencados, há outro ponto que necessita de ponderação: como ficam as imagens coletadas frente à Lei Geral de Proteção de Dados?

O artigo 5º, inciso II, da Lei no 13.709/2018 (a Lei Geral de Proteção de Dados – LGPD) dentre os dados pessoais sensíveis, prevê de forma expressa o "dado biométrico". Entretanto o artigo 4º, inciso III, desta mesma lei, prescreve que estas limitações não se aplicam ao tratamento de dados pessoais para fins exclusivos de segurança pública e atividades de investigação e repressão de infrações penais.

Desta feita, a utilização de reconhecimento facial para os fins de segurança pública não se encontra acobertada pela regulamentação, o que contribui para incertezas e um

[8] "A set of computational steps for solving a problem" (ASHLEY 2017, p. 391) ou conjunto de etapas computacionais com o escopo de solucionar um problema.

campo aberto para debates jurídicos quanto a validade ou não de tais técnicas. Impende citar o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, apelidada de "LGPD Penal". Extrai-se de seu texto os artigos 42 e 43, abaixo colacionados:

> Art. 42. A utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados por autoridades competentes dependerá de previsão legal específica, que estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de vigilância.
> [...]
> Art. 43. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.

O fulcro do anteprojeto é balancear a já mencionada proteção de dados pessoais, inclusive elevada à direito fundamental pela Emenda Constitucional 115/2022 (artigo 5º, inciso LXXIX, da Constituição da República Federativa do Brasil de 1988). Observe-se que a preocupação do legislador repousa sobre duas situações distintas: a primeira é coleta de dados biométricos de forma indiscriminada, ou seja, aplicações de reconhecimento facial em câmeras colocadas em locais públicos para identificação de indivíduos com mandados de prisão em aberto, por exemplo. A segunda é a formação de um banco de dados sem consentimento do usuário, onde seus dados biométricos são utilizados como paradigma de pesquisa.

4 SELETIVIDADE PENAL

A seletividade penal é apresentada pela doutrina como uma característica do sistema de justiça criminal, baseada na hierarquia racial, acontecendo em todos os lugares, mas sendo estudada sobremaneira nos Estados Unidos, sendo que lá, principalmente, negros e latinos são classificados como incivilizados e propensos às práticas criminosas,

comparativamente aos da raça branca, denominada "casta racial" (ALEXANDER, 2017, p. 413).

Este fenômeno pode ser observado também pela participação diminuta dos que não são da raça branca tanto na política como no sistema de justiça, fato já anteriormente mencionado, que pode influenciar no *Machine Learning*[9] da inteligência artificial, transformando o algoritmo em um meio para fornecer informações de cunho racista ou excludente.

Aliado a isso, Baratta (2002, p. 162) aponta quais são as características do direito penal que seriam utilizadas contra os indesejáveis, na tutela dos interesses da classe dominante, que se valeria do sistema criminal:

> a) O direito penal não defende todos e somente os bens essenciais, nos quais estão igualmente interessados todos os cidadãos, e quando pune as ofensas aos bens essenciais o faz com intensidade desigual e de modo fragmentário;
> b) A lei penal não é igual para todos, o status de criminoso é distribuído de modo desigual entre os indivíduos;
> c) O grau efetivo de tutela e distribuição do status de criminoso é independente da danosidade social das ações de da gravidade das infrações à lei, no sentido de que estas não constituem a variável principal da reação criminalizante e da sua intensidade

Combinando as duas premissas de seletividade penal, quais sejam o racismo com a exclusão dos indesejáveis, Magno e Bezerra (2020, p. 46) apresentam dados numéricos sobre a utilização do reconhecimento facial:

> A tecnologia ainda não apresenta eficiência sincrética no reconhecimento de pessoas negras de pele mais escura, principalmente mulheres, possibilitando que populações socialmente vulneráveis estejam sujeitas à automatização de constrangimentos e violências. Um estudo da Rede de Observatório da Segurança (NUNES, 2019) revela que 90% das 151 pessoas detidas, em 2019, com base no dispositivo, são negras. De acordo com o Departamento Penitenciário Nacional, de janeiro a junho de 2019, na Bahia, no Rio de Janeiro, em Santa Catarina e na Paraíba – estados em que o dispositivo foi testado e base de análise da Rede –, foram detidas 108.395 pessoas, das quais

[9] *Machine learning* é o termo em inglês para a tecnologia conhecida no Brasil como aprendizado de máquina e significa a capacidade dos computadores aprenderem de acordo com as respostas esperadas, por meio associações de diferentes dados, os quais podem ser imagens, números e tudo que essa tecnologia possa identificar. https://www.ibm.com/br-pt/analytics/machine-learning (acesso em 05 mar. 2023).

> 66.419 são negras ou pardas, um total de 61,27%. "O reconhecimento facial tem se mostrado uma atualização high-tech para o velho e conhecido racismo que está na base do sistema de justiça criminal e tem guiado o trabalho policial há décadas" (NUNES, 2019: 69-70). Há um dispositivo de segurança que, com a face da neutralidade, aplica um algoritmo racista capaz de legalizar e culpabilizar robôs por práticas humanas.

Neste ponto, Rosane Leal da Silva e Fernanda dos Santos Rodrigues da Silva (2019, p. 14-15), destacam que:

> [...] se não observadas algumas medidas de precaução, o uso de tecnologias de reconhecimento facial automatizado pode colaborar profundamente para o enraizamento do racismo nas estruturas sociais do Brasil. Em razão disso, é necessário, em primeiro lugar, transparência nos sistemas de auditora dos algoritmos de aprendizagem, a fim de identificar possíveis vieses de discriminação e soluções para essa hipótese. Outrossim, faz-se essencial também uma alteração na política de segurança pública, em especial, na forma de distribuição do orçamento para fins de investimento na área de tecnologia e aprimoramento do aparato tecnológico das polícias federal e civil. De fato, conforme o exposto, o uso de câmeras com boa resolução e qualidade podem ser fundamentais para um menor índice de imprecisão no momento do uso do reconhecimento facial automatizado.

A questão acima pontuada merece preocupação quanto ao emprego da tecnologia de reconhecimento facial, em especial para fins da alimentação dos bancos de dados, pois, caso as fotos e dados que são inseridos sejam apenas de condenados e/ou indivíduos que tenham sido identificados para fins investigatórios, por determinados tipos de delitos, a possibilidade de se considerar um resultado seletivo é muito grande. Neste ponto, Eugenio Raul Zaffaroni (1991, p. 67) destaca que:

> A carga estigmática produzida por qualquer contato do sistema penal, principalmente com pessoas carentes, faz com que alguns círculos alheios ao sistema penal aos quais se proíbe a coalizão com estigmatizados, sob pena de considerá-los contaminados, comportem-se como continuação do sistema penal. Cabe registrar que a carga estigmática não é provocada pela condenação formal, mas pelo simples contato com o sistema penal. Os meios de comunicação de massa contribuem para isso em alta medida, ao difundirem fotografias e adiantarem-se às sentenças com qualificações como "vagabundos", "chacais".

Outro ponto relevante é que o Brasil, tendo em vista sua miscigenação, possui uma população com diversas características físicas distintas e as tecnologias de

reconhecimento facial advém de empresas situadas nos Estados Unidos, Europa e Ásia, realidade totalmente discrepante daquela aqui observada. Isto pode gerar um problema com resultados imprecisos e enviesados (LEMOS *et al*, 2021, p. 6).

Quanto à ferramenta da reconhecimento facial usada pela Polícia Federal[10] e pela Polícia Civil do Estado de São Paulo[11], não há, em princípio, elementos que indiquem a propensão para resultados seletivos, ao menos quanto ao banco de dados e imagens paradigmas, posto que as imagens são obtidas das Carteiras Nacionais de Habilitação (CNH) para a Polícia Federal, e dos Registros Gerais (RGs) no caso da Polícia Civil, ou seja, são compilados dados dos que possuem os referidos documentos e são os que integram os bancos para fins de reconhecimento facial.

Outro ponto importante é que a ferramenta deve ser utilizada para fins de diligência em sede investigatória, sempre associada a outras práticas que acontecem no curso de um inquérito policial, não devendo constituir na única diligência realizada, de modo que, como afirmou o Delegado-Geral da Polícia Civil Ruy Ferraz Fontes ao Portal do Governo do Estado de São Paulo em entrevista de 28 de janeiro de 2020:

> O reconhecimento facial não vai ser utilizado isoladamente como meio de prova. Nós vamos 'linkar' a outros procedimentos da Polícia Civil e formar um conjunto que vai determinar se um sujeito, que é o suspeito, praticou um delito ou não.

Neste ponto Eduarda Costa Almeida (2022, p. 278) alerta que:

> [...] uso dessa tecnologia expõe as pessoas a riscos elevados e peculiares, podendo ser identificadas mesmo sem aviso ou consentimento prévio. Esses riscos são ainda mais manifestos quando a tecnologia é utilizada para finalidades similares à segurança pública, já que essencialmente o direito penal é intrusivo, excepcional e possui papel de balizar e limitar o poder punitivo do Estado. Porém, se não houver regulamento adequado e direcionado para a proteção de dados, existe o risco iminente de a regra ser a vigilância digital, o controle e a penalização dos cidadãos. Não obstante o RF já estar sendo utilizado pelas forças policiais brasileiras, é fundamental a promulgação de

[10] *Vide* https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica (acesso em 05 mar. 2023).

[11] *Vide* https://www.saopaulo.sp.gov.br/spnoticias/governo-inaugura-laboratorio-de-reconhecimento-facial-e-digital-da-policia-civil/ (acesso em 05 mar. 2023).

> uma legislação que proíba o uso da tecnologia nesse contexto ou, ao menos, que coíba o uso abusivo.
> [...]
> Como consequência, se uma lei autorizar o uso dos sistemas de RF na segurança pública, ela deve explicitar balizas de aplicação dos princípios de proteção de dados. Com isso, seria possível que a tecnologia fosse utilizada apenas para uma finalidade específica em um caso concreto determinado, nunca para atender uma motivação vaga ou imprecisa. Assim, a autoridade que utilizasse a tecnologia apenas faria tratamento de dados pessoais de pessoas de interesse por tempo em que houvesse necessidade, e nada além disso. Ainda, todo esse processo de utilização da tecnologia pelas autoridades policiais seria seguida de ampla transparência com todos os cidadãos para que pudesse haver escrutínio público sobre a proporcionalidade e a utilidade da tecnologia de reconhecimento facial.

A ferramenta é realmente um importante avanço tecnológico à disposição dos órgãos de segurança pública, porém tem suas limitações quando utilizada de maneira isolada, podendo ser dado um exemplo disso: imagine-se um fato criminoso cuja imagem do autor é registrada em câmeras de segurança e nenhum outro indício há, até então, que possa vinculá-lo como autor, o reconhecimento facial se torna apenas um indício, para apontar suspeitos, sendo que a partir disso, devem ser realizadas diligências que possam ou não indicar a quem será ou não possível vincular a autoria do ilícito penal.

5 CONSIDERAÇÕES FINAIS

Abordou-se no presente trabalho aspectos técnicos e a evolução histórica das formas de identificação biométrica, partindo de características físicas, passando pela identificação datiloscópica até a atual temática do reconhecimento facial, em especial o realizado por programas de computador dotados de inteligência artificial e qual o impacto na sociedade moderna e na segurança pública.

A Lei Geral de Proteção de Dados (LGPD), bem como no Decreto 10.046/2019, regulamentam o tema, porém excluem a proteção desses dados quando utilizados em segurança pública e/ou investigação de delitos.

A inteligência artificial empregada nestes programas de reconhecimento facial é normalmente realizada por abordagem por aprendizado supervisionado, ou seja, depende

de uma programação alimentada por uma pessoa, que pode "ensinar" a máquina sob influência de suas convicções, preconceitos e visões discriminatórias, não sendo algo neutro, em princípio, sendo razoável esta preocupação.

A ausência de neutralidade pode tornar o reconhecimento facial uma ferramenta que contribui para seletividade penal e exclusão dos indesejáveis, podendo servir como reforço às discriminações decorrentes das desigualdades sociais, raciais e de gênero.

Por fim, apontaram-se medidas a serem utilizadas para validação da ferramenta, como a utilização de dados biométricos de todas as pessoas, de forma indistinta (RG e CNH), bem como que o reconhecimento fotográfico seja utilizado em sede de investigação criminal sempre com um indício que deve ser complementado por outros elementos a serem colhidos a partir da primeira evidência, para fim de apontar, por exemplo, o autor de um crime.

A problemática também está relacionada com a inteligência artificial e a questão da abordagem por aprendizado supervisionado, ou seja, a tarefa é "ensinada" a uma máquina por um ser humano que é dotado de convicções, preferências, vivências e experiências que podem influenciar na neutralidade de suas inclinações quanto aos direcionamentos realizados para orientar a alimentação do sistema.

REFERÊNCIAS

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal . **Revista Brasileira de Segurança Pública**, v. 16, n. 2, p. 264–283, 2022. Disponível em: https://revista.forumseguranca.org.br/index.php/rbsp/article/view/1377. Acesso em: 8 set. 2022.

ASHLEY, Kevin D. **Artificial Intelligence and Legal Analytics**. New Tools For Law Pratice in the Digital Age. Cambridge: Cambridge University Press, 2017.

BARATTA, Alessandro. **Criminologia Crítica e Crítica do Direito Penal**: introdução à sociologia do direito penal. Tradução: Juarez Cirino dos Santos.3° ed. Rio de Janeiro: Revan: Instituto Carioca de Criminologia, 2002.

BRASIL. Câmara dos Deputados. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. Brasília: Comissão da Câmara dos Deputados, 2020. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 01 mar. 2022.

BRASIL. **Constituição da República Federativa do Brasil** de 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 20 jan. 2022.

BRASIL. Decreto n° 10.046 de 9 de outubro 2019. **Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados**. In: Diário Oficial da República Federativa do Brasil, Brasília, DF, 9 out. 2019. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 20 jan. 2022.

BRASIL. Lei n° 13.709 de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. In: Diário Oficial da República Federativa do Brasil, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 jan. 2022.

CÓBE, Raphael M. O.; NONATO, Luiza G.; NOVAES, Sérgio F.; ZIEBARTH, José A. Rumo a uma política de Estado para inteligência artificial. **Revista USP**, n. 124, p. 37-48, 2020. Disponível em: https://www.revistas.usp.br/revusp/article/view/167914. Acesso em: 8 set. 2022.

CORTIZ, Diogo. **Inteligência Artificial**: equidade, justiça e consequências. Internet Sectoral Overview. Year XII - N. 1, 2020. Disponível em https://www.cetic.br/media/docs/publicacoes/6/20200626161010/panorama_setorial_ano-xii_n_1_inteligencia_artificial_equidade_justi%C3%A7a.pdf Acesso em: 20 jan. 2022.

CRIPPA, Margarete Esteves Nunes; DE OLIVEIRA, Loryne Viana; HOLANDA, Tamires; LAURENTE, Itala. Uso de reconocimiento facial aplicado a la seguridad pública en Brasil. **Controversias y Concurrencias Latinoamericanas**, v. 12, n. 22, p. 159-173, 1 abr. 2021. Disponível em: http://ojs.sociologia-alas.org/index.php/CyC/article/view/248. Acesso em: 02 set. 2022.

DA SILVA, Rosane Leal; DA SILVA, Fernanda dos Santos Rodrigues. **Reconhecimento Facial e segurança pública**: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. In: 5 Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede. 2019. Disponível em https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf. Acesso em: 21 jan. 2022

DA SILVA, Lorena Abbas; FRANQUEIRA, Bruna Diniz; HARTMANN, Ivar A**. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina**. Revista Digital de Direito Administrativo, v. 8, n. 1, p. 171-204, 2021. Disponível em https://www.revistas.usp.br/rdda/article/view/173903. Acesso em: 22 jan. 2022.

DUARTE, Renata et al. **Aplicação dos Sistemas Biométricos de Reconhecimento Facial na Segurança Pública**. Brazilian Journal of Forensic Sciences, Medical Law and Bioethics, v. 11, n. 1, p. 1-21, 2021. Disponível em https://www.ipebj.com.br/bjfs/index.php/bjfs/article/view/848. Acesso em: 22 jan. 2022.

FELDENS, Luciano. **Direitos fundamentais e direito penal** – A Constituição Penal. 2 ed. Porto Alegre: Livraria do Advogado, 2012.

GARLAND, David. **A cultura do controle**: crime e ordem social na sociedade contemporânea. Rio de Janeiro: F.Bastos, 2001, Revan, 2008, 1ª reimpressão, janeiro de 2014.

Governo inaugura laboratório de reconhecimento facial e digital da Polícia Civil. **saopaulo.sp.gov.br**, São Paulo, 28 jan. 2020. Disponível em https://www.saopaulo.sp.gov.br/spnoticias/governo-inaugura-laboratorio-de-reconhecimento-facial-e-digital-da-policia-civil/. Acesso em: 20 jan. 2022.

JACQUET, Maëlig; CHAMPOD, Christophe. **Automated face recognition in forensic science**: Review and perspectives. Forensic science international, v. 307, p. 110124, 2020. Disponível em https://www.sciencedirect.com/science/article/abs/pii/S0379073819305365. Acesso em: 22 jan. 2022.

LEMOS, Alessandra; FERNANDES, Elora; MEDEIROS, Juliana; GUEDES, Paula. **Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública**: Tecnologia de Reconhecimento Facial. Rio de Janeiro. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2021. Disponível em https://itsrio.org/pt/publicacoes/comentarios-ao-anteprojeto-de-lei-de-protecao-de-dados-para-a-seguranca-publica/. Acesso em: 10 mar 2022.

MAGNO, M. E. da S. P.; BEZERRA, J. S. **Vigilância negra**: O dispositivo de reconhecimento facial e a disciplinaridade dos corpos. Novos Olhares, São Paulo, v. 9, n. 2, p. 45-52, 2020. ISSN: 2238-7714. DOI: https://doi.org/10.11606/issn.2238-7714.no.2020.165698. Disponível em: https://www.revistas.usp.br/novosolhares/article/view/165698. Acesso em: 22 jan. 2022.

NUNES JÚNIOR, Vidal Serrano**. A Cidadania Social na Constituição de 1988 Estratégia de Positivação e Exigibilidade judicial dos Direitos Sociais**. São Paulo: Verbatim, 2009.

Polícia de Detroit: sistema de reconhecimento facial da cidade erra em 96% dos casos. **Olhar digital**. 29 jun. 2020. https://olhardigital.com.br/2020/06/29/seguranca/policia-de-detroit-sistema-de-reconhecimento-facial-da-cidade-erra-em-96-dos-casos/ Acesso em: 20 jan 2022.

Polícia Federal implementa nova Solução Automatizada de Identificação Biométrica. **gov.br**, Brasília, 06 jul. 2021. Disponível em https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica Acesso em: 20 jan 2022.

PREUSSLER, Gustavo. Resenha: ALEXANDER, Michelle. **A nova segregação: racismo e encarceramento em massa**. São Paulo: Boitempo,2018,376p. Argumenta Journal Law, Jacarezinho–PR, Brasil, n.29,2018, p.411-414. Disponível em http://seer.uenp.edu.br/index.php/argumenta/article/view/1425/pdf. Acesso em: 15 set. 2021.

SOUZA, Marco Antonio de. **A biometria e suas aplicações**. Revista Brasileira de Ciências Policiais. ISSN 2178-0013, ISSN Eletrônico 2318-6917. Brasília, v. 11, n. 2, p. 79-102, mai/ago 2020. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/710 Acesso em: 17 set. 2021.

TEOFILO, Davi; KURTZ, Lahis; PORTO JR, Odélio; VIEIRA, Victor Barbieri Rodrigues**. Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro. Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo**, objeto do processo no 1090663-42.2018.8.26.0100 da 37a Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A. (ViaQuatro). Setembro de 2019. Belo Horizonte: IRIS, 2019. Disponível em: http://bit.ly/340ZN53. Acesso em: 20 jan. 2022.

TURING, Alan. **Computing Machinery and Intelligence**. Mind, LIX (236): 433–460, DOI:10.1093/mind/LIX.236.433, 1950.

WACQUANT, Loïc. **Punir os pobres: a nova gestão da miséria nos Estados Unidos**. Rio de Janeiro: F.Bastos, 2001, Revan, 2003.

ZAFFARONI, Eugenio Raul. **Em Busca das Penas Perdidas**: a perda de legitimidade do sistema penal. Rio de Janeiro: Editora Revan, 1991.