REGULAÇÃO E USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA DO BRASIL

REGULATION AND USE OF FACIAL RECOGNITION IN BRAZIL PUBLIC SAFETY

Romulo de Aguiar Araújo
Mestre em Ciências Jurídicas pelo Centro Universitário de Maringá – UniCesumar.
Advogado.
romuloaraujoadv@gmail.com
http://lattes.cnpq.br/1167303453686731
https://orcid.org/0000-0002-3978-9390

Naiara Deperon Cardoso
Especialista em Direito Penal pela Faculdade de Direito Prof. Damásio de Jesus – FDDJ.
Advogada.
naiaradeperon@gmail.com
http://lattes.cnpq.br/7844929103076536
https://orcid.org/0000-0003-4932-7349

Amanda Marcélia de Paula
Especialista em andamento em Direito e Processo Penal pelo Instituto de Direito Constitucional e Cidadania - IDCC.
Pesquisadora independente.
amanda.mdp20@gmail.com
http://lattes.cnpq.br/7090818066927320
https://orcid.org/0000-0003-2891-3437

RESUMO

Com o avanço no desenvolvimento das tecnologias biométricas, o reconhecimento facial vem sendo utilizado em ampla escala na segurança pública e persecução penal no Brasil. O presente trabalho almeja analisar os impactos da expansão de tecnologias dessa natureza em uma sociedade permeada pelo racismo estrutural, diante da incerteza quanto à acuracidade dos novos instrumentos de monitoração e vigilância públicos. Assim, analisa, através de pesquisa bibliográfica e análise de casos noticiados, o enviesamento dos algoritmos e o reflexo de sua utilização em um cenário de proteção de dados pessoais. Por fim, conclui que a ausência de legislação específica no âmbito federal que resguarde os dados tratados pela segurança pública, aliada à utilização de algoritmos submetidos a erros, potencializa o desrespeito à igualdade e coloca em risco garantias e direitos fundamentais constitucionalmente previstos.

» **PALAVRAS-CHAVE:** RECONHECIMENTO FACIAL. SEGURANÇA PÚBLICA. RACISMO. REGULAÇÃO. PROTEÇÃO DE DADOS PESSOAIS.

ABSTRACT

Due to biometric technologies advancement, facial recognition has been widely used in Public security and criminal prosecution in Brazil. This work aims to analyze the impacts of the expansion of technologies of this nature in a society permeated by structural racism, given the uncertainty regarding the accuracy of new monitoring and public surveillance instruments. It analyzes, through bibliographical research and analysis of reported cases, the bias of the algorithms and the reflection of their use in a scenario of personal data protection. Finally, it concludes that the lack of specific legislation at the federal level that protects the data processed by public security, combined with the use of algorithms capable of mistakes, enhances the disrespect for equality and puts in risk the fundamental guarantees and rights that are constitutionally provided.

» ***KEYWORDS:*** *FACIAL RECOGNITION. PUBLIC SAFETY. RACISM. REGULATION. PERSONAL DATA PROTECTION.*

Artigo recebido em 8/3/2021, aprovado em 16/9/2021 e publicado em 30/9/2021.

NOÇÕES INTRODUTÓRIAS

O progressivo uso das tecnologias biométricas e o avanço no desenvolvimento da inteligência artificial tem proporcionado uma crescente conectividade com a captação de grande quantidade de dados, desenvolvimento de sistemas de tratamento desses dados e criação de padrões de identificação, viabilizando maior controle social, tanto no âmbito privado quanto no público, sobre os indivíduos inseridos na sociedade.

Cotidianamente, nos submetemos à colheita de dados biométricos para acessar os mais diversos sistemas e serviços dos quais dispomos, por exemplo, reconhecimento de face e/ou impressão digital no celular, comandos de voz, impressão digital nas operações bancárias, fornecimento de fotografia para identificação civil e impressão digital para cadastros públicos e votação.

Essas informações e outras colhidas independentemente do nosso conhecimento, como em monitoramento de locais públicos por câmeras, a depender da regulação que norteia o seu uso, podem ter uma infinidade de destinos e, no Brasil, o Poder Público as vem utilizando para a solução de casos forenses mediante a identificação de suspeitos da prática de crimes.

Nesse âmbito, os métodos biométricos mais utilizados atualmente são a biometria da impressão digital, a geometria de mãos e de dedos, da face, de íris e da voz (SOUZA, 2020).

Por biometria entende-se o reconhecimento automatizado de indivíduos com base nas suas características biológicas, como impressões digitais, formato do rosto, voz e íris ou comportamentais como jeito de andar ou falar (LI; JAIN, 2015).

Tais dados referentes às características individuais de cada pessoa, após a sua coleta e armazenamento, precisam de um tratamento para se tornarem algoritmos, possibilitando o refinamento das buscas e a comparação de resultados para encontrar um indivíduo específico, e é à inteligência artificial (IA) que se atribui esse papel.

Quanto à IA, existem inúmeras definições, cada qual ligada à área de conhecimento em que é aplicada. Para fins metodológicos, adotaremos a trazida pela pesquisadora Dora Kaufman, que serve ao nosso propósito, a qual define inteligência artificial como a ciência e a engenharia de fazer máquinas inteligentes, ou seja, de fazer programas de computador inteligentes (KAUFMAN, 2018).

Assim, por meio da colheita de dados e da IA que os transforma em algoritmos, criam-se padrões que viabilizam o reconhecimento automatizado de indivíduos.

Vale ressaltar que o programa que dará tratamento aos dados que culminarão em algoritmos é criado, alimentado e controlado por programadores que são seres humanos e, portanto, têm diferentes

vivências e experiências profissionais e sociais. Além disso, na iniciativa privada há aqueles autônomos e empregados que também possuem suas visões institucionais. *Softwares*, por mais que sejam inteligência artificial, não estão dissociados do contexto social em que se inserem.

Analisar os algoritmos presentes na prática forense traz à tona a indagação sobre serem eles de fato neutros ou permeados de vieses pessoais que possam prejudicar a imparcialidade e colaborar para o cometimento de injustiças, considerando, em especial, o contexto do racismo individual e institucional presentes em nossa sociedade.

No que toca especificamente ao tema da segurança pública, a despeito de serem utilizados vários métodos de identificação criminal no país, escolhemos como objeto do presente estudo a biometria de reconhecimento facial, frente ao seu uso exponencial e à relevância de verificar a sua acuracidade e imparcialidade quando se trata de impor medidas coercitivas e sancionatórias pelo Estado no exercício do *ius puniendi*.

A pesquisa envolveu a apreciação da disciplina legal da proteção de dados pessoais no Brasil, associada à análise de bibliografia, nacional e estrangeira, sobre o estudo de algoritmos, seu desenvolvimento e os impactos de sua utilização.

Isto posto, passaremos a analisar a legislação em vigor que regula a matéria no ordenamento pátrio, a fim de verificar se exaure as hipóteses práticas e se existem ainda lapsos a serem corrigidos para garantir a coexistência da tecnologia do reconhecimento facial com direitos constitucionalmente garantidos, como o da igualdade perante a lei.

1 RECONHECIMENTO FACIAL E REGULAMENTAÇÃO NO BRASIL

A utilização de sistemas de identificação facial em nosso país pelo setor público é reportada, desde 2011, nos setores de educação, transporte, controle de fronteiras e segurança pública (INSTITUTO IGARAPÉ, [entre 2019 e 2021]).

Desde o ano de 2017, na cidade de São Paulo, são utilizadas câmeras de reconhecimento facial no transporte público para combater fraudes à gratuidade de transporte e uso indevido de cartões por pessoas que não as titulares. Apenas nos dois primeiros anos, houve o bloqueio de mais de 300 mil cartões por suposto uso indevido (GARAY, 2019). O que, em uma cidade da magnitude de São Paulo, onde a maior parte da população utiliza os transportes públicos e percorre grandes distâncias diariamente, representa uma limitação considerável à locomoção de pessoas vulneráveis, considerando que nenhum sistema é isento de falhas.

Também no carnaval do Rio de Janeiro, a tecnologia de vigilância teve a sua implantação iniciada em 2019, com a instalação de câmeras para reconhecimento facial. O sistema foi criado para enviar informações online para o Centro Integrado de Comando e Controle da Polícia Militar do Estado do Rio de Janeiro, cujos operadores avaliam os alertas de correspondência com suspeitos dos ban-

cos de dados (RIO DE JANEIRO, 2019). A princípio, houve a instalação de 34 câmeras, mas o projeto vem se expandindo e atualmente conta com 140 câmeras. Entretanto, juntamente com a expansão, noticiaram, em julho de 2019, ao menos duas pessoas erroneamente identificadas como criminosas (G1 RIO, 2019; ALMEIDA, 2019a).

A despeito da ampla utilização da biometria de face na segurança pública no Brasil, não existe, atualmente, uma norma de âmbito federal que regule os limites dos sistemas de vigilância e tampouco que regule a proteção de dados e da privacidade relacionadas ao reconhecimento facial na segurança pública.

O direito à privacidade, elencado no art. 5º, inciso X, da Constituição Federal, em sentido estrito, de acordo com Gilmar Mendes e Paulo Gustavo Gonet Branco, "conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral" (2017).

A Lei Geral de Proteção de Dados (Lei n. 13.709/2018 – LGPD), vigente desde 2020, apesar de representar um avanço em termos de proteção de dados pessoais e de resguardo da privacidade, não estabeleceu parâmetros para a área de segurança pública, deixando à margem do sistema a proteção dos direitos de suspeitos e investigados.

Em seu artigo 4º, inciso III, alíneas a e d, a LGPD exclui expressamente de seu âmbito de incidência regulatória as atividades de segurança pública, investigação e repressão de infrações penais. O §1º do mesmo artigo dispõe que nesses casos o tratamento de dados pessoais será regido por legislação específica (BRASIL, 2018).

Desse contexto de lacuna legislativa é possível extrair três problemas fundamentais. O primeiro consiste na ausência de uniformidade nacional entre os sistemas de identificação criminal por reconhecimento facial em uso no país. Como cada estado pode escolher adquirir o programa, existirão diversos tipos de *softwares* não regulamentados em utilização, o que pode prejudicar, inclusive, o intercâmbio de informações entre os estados e os próprios órgãos de segurança pública.

Juristas ligados ao sistema legislativo federal apontam que essa carência de uniformidade entre os sistemas obsta também a sua adequação a padrões internacionais de segurança e, consequentemente, inviabiliza o fluxo e tratamento de dados juntamente com órgãos de inteligência internacional, como a Interpol (BRASIL, [entre 2019 e 2021]).

O segundo problema é a ausência de limites e diretrizes aos programadores e empresas privadas que comercializam os *softwares* no tocante a questões éticas, de transparência no tratamento dos dados, de privacidade dos **vigiados**, de limites ao compartilhamento de dados entre os atores da persecução penal e, em especial, a responsabilização por eventuais infrações aos postulados regulatórios.

Por fim, o terceiro e mais grave problema é a proteção deficiente dos cidadãos expostos às tecnologias de reconhecimento, aos quais não é dado saber como as suas informações chegaram até

os bancos de dados, como a ausência de seu consentimento poderá limitar a coleta e uso de dados pessoais, quais as maneiras de se proteger de eventuais discriminações e os mecanismos de reparação em caso de abusos cometidos pelo Estado e pela iniciativa privada (BRASIL, [entre 2019 e 2021]).

Visando corrigir os problemas detectados e atender ao comando legislativo contido no § 1º do art. 4º da LGPD, em 2019, a Câmara dos Deputados instituiu uma comissão composta por 16 juristas, com o apoio técnico de dois consultores legislativos, para elaboração de um anteprojeto de lei para o tratamento de dados no âmbito da segurança pública, investigações penais e repressão de infrações penais (FERREIRA; OLIVEIRA, 2020).

A exposição de motivos do referido anteprojeto foi apresentada e divulgada em 5 de novembro de 2020 (BARRETO; PAULO NETO; MARQUES , 2020) e de sua leitura é possível extrair a motivação e a premente necessidade de dar parâmetros e balizas à matéria, a fim de proteger o titular dos dados pessoais contra mau uso e abusos, compatibilizando a atuação das autoridades com as garantias processuais e os direitos fundamentais do cidadão.

Os pontos mais relevantes trazidos pelo anteprojeto de lei estão inseridos em sua base principiológica que, em síntese, engloba: (i) os princípios da transparência e livre acesso, para garantir aos titulares informações claras, precisas e acessíveis sobre o tratamento de seus dados; (ii) o princípio da responsabilização e prestação de contas direcionado ao Estado e à iniciativa privada; e, em especial destaque, o (iii) princípio da não discriminação, pelo qual é expressamente vedado o uso dos dados sensíveis para fins discriminatórios ilícitos ou abusivos.

Destaca-se que dados sensíveis constituem:

> [...] dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou dado biométrico (BRASIL., [entre 2019 e 2021])

Note-se que os dados biométricos estão definidos no anteprojeto como **sensíveis**, merecedores, portanto, de especial proteção, consistente na vedação expressa a qualquer discriminação, especialmente quanto à origem racial ou étnica daquele que terá a sua biometria disponível perante os órgãos de segurança pública (BRASIL, [entre 2019 e 2021]).

Assim, não havendo no Brasil atual uma normativa específica que garanta a neutralidade dos *softwares* e ofereça diretrizes e limites aos programadores e ao Estado no uso dos dados, bem como que permita aos cidadãos terem acesso às informações claras e precisas sobre o tratamento de seus dados, a utilização do sistema de reconhecimento facial na segurança pública passa a ser permeada de incerteza jurídica, da seletividade de um sistema que segrega e da consequente punição de pessoas vulneráveis e por vezes inocentes, como já se observa atualmente.

2 ALGORITMO E SELETIVIDADE

A aplicação de tecnologias na segurança pública envolve a necessidade de ponderação sobre as heurísticas e os vieses aos quais as decisões humanas estão submetidas. Cabe destacar, ainda que de forma breve, que as heurísticas consistem em mecanismos de reconhecimento de informações que ajudam a encontrar respostas simples para perguntas que demandam maior esforço cognitivo (BOEING, 2019).

Essa construção se dá na medida em que parte das decisões humanas são tomadas de forma automática em hipóteses de situações semelhantes. Nesses casos, o sistema cognitivo caminha em busca de coerência, o que pode acarretar, por exemplo, a familiaridade e o conforto com ilusões de veracidade.

Tais falhas cognitivas podem interferir no Poder Judiciário, na medida em que, em especial pelo excesso de demandas, os sujeitos processuais não têm condições de analisar de forma detalhada as particularidades dos casos que lhes são apresentados. Assim, as heurísticas, ou atalhos, funcionam como mecanismos de decisão pré-pronta (BOEING, 2019).

Esse cenário deixa claro que se os processos cognitivos humanos possuem limitações, também as terão as decisões pautadas em tecnologias advindas da inteligência artificial.

A respeito das decisões tomadas por máquinas, é relevante expor a lição de O'Neil sobre a possibilidade de modelos apresentarem erros. Modelos são aqui entendidos como "a utilização de dados preexistentes para descrever certas regularidades, à medida que tais padrões podem ser aplicados em novas situações" (O'NEIL, 2016).

Destaca, ainda, a autora que todo modelo é constituído de informações de entrada e de saída, contudo nenhum modelo tem o condão de captar toda a complexidade do mundo real. O objetivo, em verdade, é a constituição de uma simplificação, a qual separe aspectos relevantes e irrelevantes de um determinado processo (O'NEIL, 2016).

Como exemplo, cita-se o sistema de GPS de um veículo terrestre. Este será constituído por informações específicas, tais como estradas, pontes e túneis, mas não terá em sua composição o formato de prédios, o que seria armazenado em um modelo de *software* que guiasse aviões.

Assim sendo, a criação de um modelo pressupõe a seleção de aspectos mais relevantes da realidade, de forma que algumas características são deixadas de lado. É aqui que reside a influência dos criadores do modelo, os quais deixarão de inserir determinadas informações a partir de suas íntimas convicções.

Como consequência, o modelo revelará as convicções e prioridades de seus criadores.

Partindo dessa premissa, é impossível considerar que as tecnologias são dotadas de neutralidade. Pelo contrário, essas revelam os valores e interesses daqueles que influenciam o design e uso, e são fundamentalmente formado a partir das mesmas estruturas desiguais que vigem na sociedade (ACHIUME, 2020).

Exemplo disso é a análise feita pela ProPublica (jornal norte americano) a respeito do COMPAS (Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativas). O algoritmo, desenvolvido pela empresa atualmente denominada *Equivant*, possui o intuito de avaliar riscos sobre pessoas que voltam a praticar crimes e, assim, auxiliar nas decisões de juízes nos tribunais dos Estados Unidos (VIEIRA, 2019).

Nesse sentido, a ferramenta foi utilizada para determinar a probabilidade de reincidência de prisioneiros, mediante avaliação de fatores como histórico criminal, criminalidade da família, abuso de substâncias, dentre outros. Para tanto, foram feitas 137 perguntas a serem respondidas pelos réus.

Entretanto, o citado jornal identificou que as pessoas negras possuem mais chances de serem classificadas como de alto risco, trazendo à tona a presença de enviesamento no citado *software*.

Outra preocupação que cabe relevo é o fato de que a empresa não expunha ao certo como era o funcionamento do algoritmo do COMPAS, de forma que o réu submetido ao *software* não conseguia questionar o resultado, visto que não se sabia sequer como foi calculado o seu risco.

Fato é que os únicos com acesso total aos algoritmos são os próprios programadores. A reflexão disso no contexto em que o racismo estrutural é a regra é, naturalmente, que os modelos desenvolvidos sejam enviesados a partir das concepções racistas de seus criadores.

Não é novidade que no Brasil o racismo permeia a sua história desde o descobrimento, e mesmo sendo maioria dentre a população, os negros são os menos favorecidos na educação, são mais pobres, são minoria no mercado de trabalho e com salários menores, tem menos saneamento básico, são mais dependentes do sistema único de saúde - SUS, e não ocupam, ou se ocupam é de forma irrisória os altos cargos do país, tem baixíssima representatividade política, e são maioria no sistema carcerário, sendo relevante que, pelo que se verifica, o risco destes dados serem transpostos parra os *softwares* de reconhecimento facial é extremamente elevado (LIMA; SILVA; ARAÚJO, 2021).

Paralelamente, como consequência do enviesamento racista, tem-se que, com a utilização do reconhecimento por *software,* não só o direito à privacidade e a proteção de dados ficam na iminência de violação, mas também o direito constitucional de igualdade, tido como signo fundamental da democracia (SILVA, 2005).

Tratar a respeito do racismo impõe expor que o conceito se desdobra em três perspectivas. A primeira delas consiste no racismo sob a concepção individualista, segundo a qual o racismo é uma espécie de anormalidade, um fenômeno ético de caráter individual ou coletivo, mas atribuído a grupos isolados (ALMEIDA, 2019b).

Sob esse vértice, não haveria sociedades ou instituições racistas, mas sim indivíduos racistas que agem isoladamente ou em grupo.

Já a concepção institucional, tida como avanço teórico nos estudos sobre a temática, traduz a ideia de que racismo não se resume a comportamentos individuais. É, em verdade, resultado do funcionamento das instituições que atuam de forma a conceder desvantagens e privilégios com base na raça:

> Assim, a principal tese dos que afirmam a existência de racismo institucional é que os conflitos raciais também são parte das instituições. Assim, a desigualdade racial é uma característica da sociedade não apenas por causa da ação isolada de grupos ou de indivíduos racistas, mas fundamentalmente porque as instituições são hegemonizadas por determinados grupos raciais que utilizam mecanismos institucionais para impor seus interesses políticos e econômico (ALMEIDA, 2019b, p. 26).

Consequência disso é que o racismo pode ter sua forma alterada pela ação ou omissão dos poderes institucionais, na medida em que o grupo racial no poder, a fim de assegurar o controle da instituição, se valerá de mecanismos como a produção de consensos sobre a sua dominação.

O conceito de racismo institucional já representou grande avanço ao demonstrar que o racismo transcende o âmbito da ação individual e, também, ao deixar claro que a dimensão do poder é elemento inerente às relações sociais.

Entretanto, partindo do pressuposto que a instituição tem sua atuação condicionada a uma estrutura social previamente existente, o racismo que essa instituição pode expressar é também parte dessa mesma estrutura. Dito de outro modo, "as instituições são racistas porque a sociedade é racista" (ALMEIDA, 2019b).

Assim, é de se passar, então, para o conceito de racismo como estrutural, na medida em que esse é uma decorrência da própria estrutura social, ou seja, do modo **normal** como se constituem as relações sociais, não sendo o racismo uma patologia, tampouco um desarranjo institucional (ALMEIDA, 2019b).

Relevante destacar que considerar o racismo como estrutural não significa que as ações e políticas antirracistas sejam inúteis, nem mesmo que os indivíduos que cometem atos discriminatórios não devem ser devidamente responsabilizados. O que se defende é que "o racismo, como processo histórico e político, cria as condições sociais para que grupos racialmente identificados sejam discriminados de forma sistemática" (ALMEIDA, 2019b).

Feitas essas considerações é que se pode falar, então, em racismo algorítmico, o qual:

> [...]traduz a ideia do modo pelo qual a disposição de tecnologias e imaginários sociotécnicos em um mundo moldado pela supremacia branca fortalece a ordenação racializada de epistemes, recursos espaço e violência em detrimento de grupos racionalizados pela branquitude detentora de epistemologias e capitais hegemônicos que moldam o horizonte de ações da inteligência artificial em sistemas algorítmicos. (SILVA, 2020).

Exemplo dessa perspectiva foi o que revelou o Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA em 2019. Dentre 189 algoritmos de reconhecimento facial analisados, de 99 desenvolvedores diversos, a maioria era, de 10 a 100 vezes, mais propensa a identificar incorretamente pessoas negras e asiática comparadas com uma pessoa branca (GROTHER; NGAN; HANAOKA, 2019).

A identificação incorreta consiste no chamado **falso positivo**, que ocorre quando o algoritmo diz que duas fotos são da mesma pessoa, quando, na realidade, não são. Aqui reside parte da preocupação de utilização do *software* na segurança pública, visto que, diante de um falso reconhecimento, uma pessoa pode ser indevidamente detida pela acusação por um delito.

E foi justamente o que aconteceu no Rio de Janeiro, em julho de 2019, com a instalação das câmeras de vigilância em locais públicos, como já mencionado. Naquela feita, uma mulher foi identificada como uma pessoa acusada do delito de homicídio e de ocultação de cadáver, o que motivou a sua prisão. Todavia, posteriormente, os agentes perceberam que a pessoa procurada, na verdade, já se encontrava presa (ARBULU, 2019).

No Brasil, um marco do reconhecimento fácil na segurança pública ocorreu em 2019, quando, no estado da Bahia, mais de cem pessoas foram presas mediante uso da tecnologia. Atualmente, mais de vinte estados brasileiros já tiveram ou estão em processo de licitação para a compra de tecnologia dessa natureza (NUNES, 2020).

Soma-se a isso o fato de que, em 2019, o então ministro da segurança pública assinou a Portaria nº 793, a qual previa o fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, mediante financiamento do Fundo Nacional de Segurança Pública (BRASIL, 2019).

Isto posto, fica evidente que a análise a respeito da viabilidade de utilização do reconhecimento facial é urgente, pois já há registos de sua implementação e até mesmo de prisões realizadas através dele.

Dentre as circunstâncias que chamam atenção a respeito da tecnologia está o enviesamento racista que pode permear algoritmos. O cenário sobre o tema não é diferente na realidade brasileira.

Em um levantamento feito nos estados da Bahia, Ceará, Pernambuco e Rio de Janeiro, entre cento e oitenta pessoas presas com o uso de reconhecimento, noventa por cento eram negras (NUNES, 2020).

Além do mais, não se pode ignorar que o reconhecimento facial é altamente utilizado no Brasil como elemento investigativo no processo penal e até mesmo como meio de prova. É de se questionar, então, se o aumento da utilização do reconhecimento por algoritmo alcançará também a seara processual.

Certo que uma das problemáticas do reconhecimento fotográfico é a falibilidade da memória humana, a qual está sujeita a distorções oriundas de influências externas e internas (FRAGA, 2020).

Outrossim, é inegável a possibilidade de criação de falsas memórias fotográficas a partir da imagem do suspeito retirada dos álbuns de fotografia e mostrada à vítima na fase investigativa, antes mesmo da realização do reconhecimento pessoal.

Há, então, um comprometimento da memória em virtude de um juízo prévio criado, e a consequente indução em erro para realização do ato (LOPES JR., 2019).

Transpondo a questão para o reconhecimento algorítmico, chama atenção o modo que um falso positivo na fase investigativa pode gerar o comprometimento da memória do reconhecedor, que poderá reproduzir o erro na fase judicial e contribuir para formação de uma condenação injusta.

A despeito das circunstâncias aqui levantadas, o que se tem é que a tecnologia de reconhecimento facial por meio da IA tende a crescer no país. Diante disso, a manutenção do respeito aos limites constitucionais do Estado democrático impõe uma regulamentação precisa da matéria, que estabeleça parâmetros mínimos de prestação de contas por parte dos desenvolvedores e propulsores dos *softwares*.

CONCLUSÃO

A inteligência artificial e os mecanismos a ela relacionados são partes indissociáveis da atual vida em sociedade. Desde os modelos presentes no smartphone até a utilização desses pelo Estado, a realidade é permeada pelo digital.

Diferente não é o âmbito da segurança pública, o qual, como dito, conta com utilização da tecnologia de reconhecimento facial no Brasil desde 2011.

Indaga-se, então, quais as medidas a serem tomadas a fim de que a já utilizada tecnologia de reconhecimento facial se afaste dos vieses arbitrários e discriminatórios e seja compatível com o Estado democrático.

Dito isso, importante destacar que não se defende aqui um rechaço completo à combinação de tecnologia e persecução penal. Trata-se, em verdade, de alerta sobre o que há por trás dos bancos de dados que alimentam os sistemas de reconhecimento, assim como acerca da necessidade de respeito aos direitos individuais quando da utilização dessa tecnologia.

Constata-se, em uma primeira análise, que a utilização do reconhecimento facial pressupõe regulamentação em âmbito federal, tendo em vista que, apesar da já em vigor Lei Geral de Proteção de Dados, essa expressamente exclui de seu âmbito de incidência o tratamento de dados na segurança pública.

Por outro lado, há anteprojeto de lei em tramitação que visa regulamentar a matéria do tratamento de dados no âmbito da segurança pública, investigações penais e repressão de infrações penais. A existência de comissão especializada debatendo o tema reforça sua urgência e necessidade aqui defendidas.

Indo além, é de se ter em vista duas balizas: transparência e prestação de contas. Consequência disso é que somente tecnologias auditáveis poderão ser utilizadas pela máquina estatal, sem prejuízo das garantias constitucionais.

No mesmo sentido, indispensável é o controle da fonte primária dos algoritmos. É dizer, os sujeitos responsáveis por sua elaboração e programação, conquanto capazes de influir no funcionamento do sistema, merecem atenção dos responsáveis, a fim de que essa influência não acabe por perpetuar pré-conceitos.

Não se pode, ademais, adotar postura de conformidade com a situação a respeito dos vieses. É possível, paralelamente ao que já exposto, reagir a esse quadro de influência com a devida atenção aos desenvolvedores de *software*.

Ademais, cabe alertar os aplicadores da lei penal, aos quais ficará reservada a responsabilidade de apreciar a validade da informação obtida através de algoritmos de reconhecimento facial, a fim de que a credibilidade do referido sistema não se sobreponha à garantia de igualdade e à presunção de inocência.

Indispensável, também, a existência de bancos de dados confiáveis e com frequente atualização, para que se evite, por exemplo, prisões como aquela no Rio de Janeiro, em que a verdadeira infratora já se encontrava encarcerada.

A realidade do uso do reconhecimento facial algorítmico pelo Estado na segurança pública deve ser enfrentada, a fim de que a tecnologia associada à persecução penal não perpetue desigualdades, tampouco fira garantias fundamentais.

REFERÊNCIAS

ACHIUME, Tendayi. Racial discrimination and emerging digital technologies: a human rights analysis: report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance. **United Nations Digital Library**, Genebra, 18 jun. 2020. Disponível em: https://digitallibrary.un.org/record/3879751. Acesso em: 4 mar. 2021.

ALMEIDA, Emily. Homem é preso por engano em Copacabana. **Band News FM Rio**, [Rio de Janeiro, RJ], 24 jul. 2019a. Disponível em: https://bit.ly/3dEUflp. Acesso em: 4 mar. 2021.

ALMEIDA, Silvio Luiz de. **Racismo Estrutural.** São Paulo: Sueli Carneiro, 2019b.

ARBULU, Rafael. Mulher é detida por engano após erro em sistema de reconhecimento facial no RJ. **Canaltech**, [*s.l.*],10 jul. 2019. Disponível em: https://canaltech.com.br/governo/mulher-e-detida-por-engano-apos-erro-em-sistema-de-reconhecimento-facial-no-rj-143761/. Acesso em: 4 mar. 2021.

BARRETO, Pablo Coutinho; PAULO NETO, Octávio Celso Gondim; MARQUES, Paulo Rubens Carvalho. O anteprojeto da 'LGPD penal' e a (in) segurança pública e (não) persecução penal: O anteprojeto impacta na prova penal, nas técnicas especiais de investigação e no processo penal. **JOTA**, [*s.l.*], 9 dez. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-anteprojeto-da-lgpd-penal-e-a-in-seguranca-publica-e-nao-persecucao-penal-09122020. Acesso em: 5 mar. 2021.

BOEING, Daniel Henrique. **Ensinando um robô a julgar:** pragmática, discricionariedade e vieses no uso de aprendizado de máquina no judiciário. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Santa Catarina, Florianópolis, 2019. Disponível em: https://repositorio.ufsc.br/handle/123456789/203514. Acesso em: 4 mar. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 4 mar. 2021.

BRASIL. Ministério da Justiça e Segurança Pública. Gabinete do Ministro. Portaria n° 793, de 24 de outubro de 2019. Regulamenta o incentivo financeiro das ações do Eixo Enfrentamento à Criminalidade Violenta, no âmbito da Política Nacional de Segurança Pública e Defesa Social e do Sistema Único de Segurança Pública, com os recursos do Fundo Nacional de Segurança Pública, previstos no inciso I do art. 7º da Lei nº 13.756, de 12 de dezembro de 2018. **Diário Oficial da União**, Brasília, DF, 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em: 4 mar. 2021.

BRASIL. Câmara dos Deputados. Exposição de motivos do Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. [**Diário da Câmara dos Deputados**], [*s.l.*], [entre 2019 e 2021]. 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: 5 mar. 2021.

FERREIRA, Cláudio; OLIVEIRA, Marcelo. Anteprojeto sobre uso de dados na segurança pública deve ficar pronto em novembro: Proposta será apresentada por grupo de trabalho criado na Câmara dos Deputados. **Site Câmara dos Deputados**, [Brasília, DF], 22 set. 2020. Disponível em: https://www.camara.leg.br/noticias/694562-anteprojeto-sobre-uso-de-dados-na-seguranca-publica-deve-ficar-pronto-em-novembro/. Acesso em: 5 mar. 2021.

FRAGA, Clarice Lessa. **A influência das falsas memórias no reconhecimento fotográfico.** Trabalho de Conclusão de Curso (Graduação em Direito) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2020. Disponível em: https://www.pucrs.br/direito/wp-content/uploads/sites/11/2020/08/clarice_fraga.pdf. Acesso em: 4 mar. 2021.

G1 RIO. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. **G1 Rio de Janeiro**, Rio de Janeiro, 11 jul. 2019. Disponível em: https://glo.bo/2SLi-nec. Acesso em: 4 mar. 2021.

GARAY, Vladimir. Mal de Ojo: Reconocimiento Facial em América Latina. **Latin America in a Glimpse,** [*s.l.*], [dez./2019]. Disponível em: https://bit.ly/2H2baQA. Acesso em: 4 mar. 2021.

GROTHER, Patrick J; NGAN, Mei L.; HANAOKA, Kayee K. Face Recognition Vendor Test Part 3: Demographic Effects. **Site National Institute of Standards and Technology**, Gaithersburg, 19 dez. 2019. Disponível em: https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects. Acesso em: 4 mar. 2021.

INSTITUTO IGARAPÉ. Desde 2011 vem sendo utilizado o reconhecimento facial no Brasil. 2019. **Site Instituto Igarapé**, [*s.l.*], [entre 2019 e 2021]. Disponível em: https://bit.ly/2L89rvh. Acesso em: 4 mar. 2021.

KAUFMAN, Dora. **A inteligência artificial irá suplantar a inteligência humana?**. São Paulo: Estação das Letras e Cores, 2018.

LI, Stan Z; JAIN, Anil K. (eds.). **Encyclopedia of Biometrics**. 2nd ed. [Nova Iorque]: Springer US, 2015.

LIMA, João Lucas Figueiredo de; SILVA, Débora Letícia da; ARAÚJO, Romulo de Aguiar. Seletividade e violência racial das instituições policiais. *In:* ARAÚJO, Romulo de Aguiar. **Direitos Fundamentais e as ciências criminais**. Londrina: Thoth, 2021, p. 219-223.

LOPES JR., Aury. **Direito processual penal**. 16. ed. São Paulo: Saraiva Educação, 2019.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Bonet. **Curso de Direito Constitucional**. 12. ed. rev. e atual. São Paulo: Saraiva, 2017.

NUNES, Pablo. Uso de reconhecimento facial na segurança pública no Brasil. *In*: SEMINÁRIO PROTEÇÃO DE DADOS E OS IMPACTOS SOCIAIS, 2020, Rio de Janeiro. **Anais** [...]. Disponível em: https://www.youtube.com/watch?v=q7py8yePjQk&ab_channel=TVALERJ. Acesso em: 26 fev. 2021.

O'NEIL, Cathy. **Weapons of math destruction.** New York: Broadway Books, 2016.

RIO DE JANEIRO. Secretaria de Estado de Polícia Militar. Polícia Militar vai implantar programa de reconhecimento facial e de placa de veículos. **Site Polícia Militar do Estado do Rio de Janeiro**, [Rio de Janeiro, RJ], 22 jan. 2019. Disponível em: https://bit.ly/3bcqDdC. Acesso em: 4 mar. 2021.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 24. ed. São Paulo: Malheiros, 2005.

SILVA, Tarcízio. Racismo Algorítmico. *In*: SEMINÁRIO PROTEÇÃO DE DADOS E OS IMPACTOS SOCIAIS, 2020, Rio de Janeiro. **Anais** [...]. Disponível em: https://www.youtube.com/watch?v=q7py8yePjQk&ab_channel=TVALERJ. Acesso em: 26 de fev. 2021.

SOUZA, Marco Antônio de. A Biometria e suas aplicações. **Revista Brasileira de Ciências Policiais**, Brasilia,DF, 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: 4 mar. 2021.

VIEIRA, Leonardo Marques. A problemática da inteligência artificial e dos vieses algorítmicos: caso COMPAS. *In*: BRAZILIAN TECHNOLOGY SYMPOSIUM, 2019, Campinas. Disponível em: https://www.lcv.fee.unicamp.br/images/BTSym-19/Papers/090.pdf. Acesso em: 4 mar. 2021.