# O reconhecimento facial e o viés algorítmico racista

# Facial recognition and racist algorithmic bias

DOI:10.34117/bjdv8n5-049

Recebimento dos originais: 21/03/2022
Aceitação para publicação: 29/04/2022

**Victor Benigno Porto**
Mestre em Direito
Instituição: Centro Universitário de Brasília (Uniceub)
Endereço: SEPN 707/907 - Bloco 3 - Asa Norte, Brasília-DF
E-mail: victorbporto@gmail.com

**Emiliana Kelly Cavalcante Rolim**
Bacharela em Direito
Universidade de Fortaleza (Unifor)
Endereço: Av. Washington Soares, 1321 - Edson Queiroz, Fortaleza
E-mail: emilianarolim@hotmail.com

**RESUMO**

Este artigo discute a utilização de tecnologia de reconhecimento facial sob o influxo da seletividade do direito penal. Contextualiza a necessidade de se enfrentar o tema demonstrando aspectos da vida cotidiana que tangenciam a matéria abordada, em correlação com o racismo estrutural. Aponta a relevância da matéria a partir da teoria crítica da raça e a necessidade de adequação do ordenamento jurídico às mudanças proporcionadas pelos avanços tecnológicos sob os parâmetros da Lei Geral de Proteção de dados. No estudo, se realiza revisão bibliográfica de doutrina pátria e estrangeira. A utilidade do presente trabalho se revela por meio de contribuição ao debate acadêmico no sentido da possibilidade de se reconhecer a importância de enfrentamento da matéria sob o prisma da inexistência de neutralidade das tecnologias de reconhecimento facial, alertando-se para a necessidade do seu exame sob o enfoque da proteção da pessoa humana.

**Palavras-chave:** reconhecimento facial, viés algorítmico, racismo estrutural, lgpd.

**ABSTRACT**

This paper discusses the use of facial recognition technology under the influx of criminal law selectivity. It contextualizes the need to address the issue by demonstrating aspects of everyday life that touch on the subject addressed, in correlation with structural racism. It points out the relevance of the matter from the critical theory of race and the need to adapt the legal system to the changes brought about by technological advances and its adequation under the brazilian data protection law. During the study, a bibliographical review of Brazilian and foreign doctrine is carried out. The usefulness of this paper is revealed through its contribution to the academic debate in the sense of the possibility of recognizing the importance of addressing the issue from the standpoint of the lack of neutrality of facial recognition technologies, drawing attention to the need for its examination from the standpoint of the protection of the human person.

**Keywords:** facial recognition, algorithmic bias, structural racism, lgpd.

## 1 INTRODUÇÃO

No ano de 2020, A Corte de Apelações britânica decidiu que o uso de certa tecnologia de reconhecimento facial, AFR Locate[1], pela polícia de Gales do Sul, violaria diversas normas e possuiria "deficiências fundamentais"[2].

O tribunal entendeu que não haveria clareza sobre quem estaria inserido na lista de observação e, tampouco, sobre os critérios utilizados para determinar onde a tecnologia de reconhecimento facial seria empregada. E, no caso concreto, também não ficou claro para aquele órgão julgador que a polícia teria avaliado se o algoritmo utilizado evidenciaria um viés relacionado à raça ou sexo.

Foi comprovado que, em evento realizado em 2017, de 2.500 (dois mil e quinhentos) reconhecimentos, 2.300 (dois mil e trezentos) apresentaram falso positivo. Esse dado revela que a adoção de tecnologia com esse grau de intrusão na esfera individual carece de regulamentação e de implementação adequada, do ponto de vista da programação, e de acordo com os objetivos propostos em políticas públicas claras.

É importante ressaltar que a Corte britânica não disse que o reconhecimento facial estaria proibido no Reino Unido. Apenas estabeleceu diretrizes sobre o que é admissível no uso da tecnologia e reconheceu a necessidade de as autoridades observarem os direitos fundamentais dos indivíduos.

Transpondo a situação acima para a realidade brasileira, se evidencia a necessidade de uma abordagem holística da relação da Lei Geral da Proteção de Dados com o direito penal e os seus reflexos na esfera dos indivíduos, inclusive sob o prisma criminológico.

A relevância prática da relação entre proteção de dados e direito penal pode ser extraída, também, a partir da notícia de que, em Detroit, nos Estados Unidos da América,

[1] Segundo a polícia de Gales do Sul, Reino Unido, o reconhecimento facial automático seria capaz de detectar faces em imagem ou vídeo e comparar com banco de dados de imagens faciais para fins de correspondência entre imagens capturadas em circuitos de câmeras e as armazenadas pelos órgãos de segurança, bem como para comparar a imagem da cena de um crime com essa mesma base de informações. É composto de duas etapas: identificar e localizar indivíduos. Na identificação são consideradas imagens estáticas de suspeitos desconhecidos e de pessoas que estão em espécie de lista de observação. Na etapa da localização, o *software* cruza dados de imagens "ao vivo" de faces com imagens situadas em banco de dados específico. Disponível em <https://afr.south-wales.police.uk/>. Acesso em 16 jul. 2021.

[2] **R (Bridges) -v- CC South Wales**, disponível em: <https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/>, acesso em: 15 ago. 2020.

um indivíduo, Robert Julian-Borchak Williams, foi equivocadamente preso, na frente de sua casa e diante de sua esposa e duas filhas, em razão de um suposto furto a uma loja de departamentos, com base em erro de algoritmo de reconhecimento facial[3].

A conduta do policial que procedeu à prisão sem verificar se o alvo da diligência era, de fato, quem deveria ser preso seria penalmente punível? E, na hipótese de inserção de informações dolosas que podem levar à prisão de um indivíduo, haveria responsabilização penal? A constatação de uma falha pelo gestor do tratamento dos dados e a omissão quanto à tomada de providências para sua correção é uma conduta penalmente relevante?

Questionamentos dessa natureza tendem a se multiplicar na medida em que o manejo de informações individuais seja mais utilizado na área de segurança pública e persecução penal.

Por ora, centra-se a preocupação na forma com a qual o uso da tecnologia de reconhecimento facial, associado a um mau desempenho das funções por parte dos agentes estatais sem mecanismos legais de contenção e repressão de condutas disfuncionais, traz mais problemas do que soluções à sociedade.

O presente estudo não enfrentará, de modo direto, as questões acima dispostas, mas abordará outro aspecto de extrema relevância, qual seja a influência de características relacionadas a cor dos indivíduos nas valorações realizadas por softwares destinados aos fins de controle de comportamentos desviantes.

Portanto, a partir do reconhecimento do racismo enquanto indesejável fenômeno social, da forte tendência de interação entre tecnologia e direito, bem como da concepção da proteção de dados enquanto direito fundamental, se pretende demonstrar, também mediante o enfoque criminológico, que o uso de tecnologias de reconhecimento facial representa alta possibilidade de discriminação de grupos historicamente marginalizados, em especial a população negra.

Sob prisma metodológico, este trabalho apresenta abordagem teórica e, por meio de pesquisa exploratória bibliográfica e documental, se busca demonstrar que as discussões em torno do uso de recursos teconológicos que envolvam a coleta de dados biométricos e o seu posterior tratamento para fins de reconhecimento facial são indissociáveis de amplo debate e da assunção de que, de fato, há o risco real de

[3] COX, Kate. **Police arrested wrong man based on facial recognition fail, ACLU says | Ars Technica**. Ars Technica, disponível em: <https://arstechnica.com/tech-policy/2020/06/police-arrested-wrong-man-based-on-facial-recognition-fail-aclu-says/>, acesso em: 15 dez. 2020.

malferimento de direitos de populações que já convivem com um sistema repressivo que as tem como clientes preferenciais. Se pretende, também, alertar para a existência do viés algorítmico decorrente do inarredável fator humano na linguagem computacional.

O desenvolvimento do trabalho se subdivide em seis tópicos. No primeiro, se reconhece o racismo como fenômeno social indesejado. No segundo, se aborda a questão da algoritmização do direito e a dificuldade de se inserir na linguagem computacional elementos jurídicos sem a concomitante introdução da carga valorativa dos desenvolvedores de software. No terceiro, se examina, à luz da dogmática penal e criminológica, o avanço do punitivismo global e a criação de figuras socialmente indesejáveis. No quarto, se aborda a Teoria Crítica da Raça como ponto de partida para a minimização do viés algorítmico. No quinto, se discute, com o auxílio de dados empíricos extraídos de documentos que tangenciam o tema, como o atual uso da tecnologia de reconhecimento facial em âmbito brasileiro tem se revelado como instrumento de reforço do racismo estrutural existente. No sexto, se arrosta a discussão acerca da necessidade de observação da principiologia da Lei Geral de Proteção de dados no tratamento de dados pessoais sensíveis como instrumento auxiliar de proteção dos indivíduos.

## 2 DESENVOLVIMENTO

### 2.1 O RACISMO ENQUANTO FENÔMENO SOCIAL

O presente trabalho não tem por escopo o exame em torno dos fatores históricos que culminaram na atual estratificação étnica brasileira. Parte-se da premissa de que, no Brasil, o modo de produção escravocrata gerou reflexos sentidos até os dias de hoje, principalmente no tratamento do negro.

Conquanto seja pacífica a inexistência de comprovação científica de que não há fator biológico ou genético que permita a subdivisão da espécie humana em raças, o racismo existe e deve ser encarado como um fenômeno social indesejado.

Por oportuno, vale a menção ao voto condutor do acórdão do HC 82.424-QO, julgado pelo Plenário do Supremo Tribunal Federal em 2003, processo que ficou conhecido como “Caso Ellwanger”[4].

Naquela oportunidade, o Ministro Maurício Corrêa, Redator para o acórdão, consignou que “[e]mbora hoje não se reconheça mais, sob o prisma científico, qualquer

[4] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Habeas corpus 82.424-QO**. Paciente: Siegfried Ellwanger. Coator: Superior Tribunal de Justiça. Redator para Acórdão: Min. Maurício Corrêa. Disponível em https://jurisprudencia.stf.jus.br/pages/search/sjur96610/false. Acesso em 20/03/2021.

subdivisão da raça humana, o racismo persiste enquanto fenômeno social, o que quer dizer que a existência das diversas raças decorre da mera concepção histórica, política e social e é ela que deve ser considerada na aplicação do direito"[5].

Nesse contexto, o racismo, para prevalecer, precisa, em algum grau, da conivência dos membros da sociedade, tanto sob o prisma cultural quanto socioeconômico[6]. Assim, o aspecto identitário coletivo não pode ser desconsiderado como elemento mantenedor das desigualdades sociais e, ao mesmo tempo, como força propulsora de mudanças. Deve-se admitir o problema e enfrentá-lo[7].

É imperioso, portanto, que se reconheça a existência do racismo e, paralelamente à sua desconstrução, deve-se buscar identificar as circunstâncias em que a subjugação dos indivíduos negros ocorre simplesmente em razão da cor da sua pele.

As tecnologias de vigilância em massa, em especial o reconhecimento facial, parecem ser terreno fértil para a reafirmação desse fenômeno social. Assim, a abordagem do tema sob essa perspectiva pode contribuir para a minimização de injustiças que venham a ocorrer.

## 2.2 A ALGORITMIZAÇÃO DO DIREITO

Não há como se desenvolver este trabalho sem que se tenha melhor compreessão das consequências que podem advir da interação entre atitudes humanas e sistemas automatizados de decisão com base em algoritmos.

A expressão algoritmo decorre da latinização do nome árabe de Abu-Abdullah Muhammed ibn-Musa Al-Khwarizmi, matemático, considerado o pai da álgebra, que teria vivido entre 780 e 850 D.C., para quem o algoritmo seria a expressão da concatenação de instruções a serem seguidas para que se chegasse à solução de equações[8].

Posteriormente, Alonzo Church e Alan Turing trouxeram a lume os conceitos de computabilidade e funções computacionais para formalizar a possibilidade de se elaborar

[5] Ibid. p. 568.
[6]A propósito, Silvio Almeida considera que: "[a] permanência do racismo exige, em primeiro lugar, a criação e a recriação de um imaginário social em que determinadas características biológicas ou práticas culturais sejam associadas à raça e, em segundo lugar, que a desigualdade social seja naturalmente atribuída à identidade racial dos indivíduos ou, de outro modo, que a sociedade se torne indiferente ao modo com que determinados grupos raciais detêm privilégios". In: ALMEIDA, Silvio, **O que é racismo estrutural?**, São Paulo: Pólen, 2019, p. 45.
[7] BAUMAN, Zygmunt, **Identidade - Entrevista a Benedetto Vecchi**, 1. ed. Rio de Janeiro: Jorge Zahar, 2005, p. 44–45.
[8] ARNDT, A. B., Al-Khwarizmi, **The Mathematics Teacher**, v. 76, n. 9, p. 668–670, 1983.

sequencias de instruções a serem seguidas não apenas por humanos, mas, também, por máquinas.

Em 1961, Marvin Minsky foi além e vislumbrou a possibilidade de se introduzir "inteligência" nos sistemas computacionais, bem como a viabilidade da formulação de algoritmos com capacidade de aprender e ensinar sistemas computacionais[9].

Atualmente se tem a noção de *big data* como expressão do potencial dos algoritmos enquanto mecanismos de correlação de uma miríade de informações aparentemente desconexas e a produção de conclusões importantes tanto do ponto de vista do interesse estatal quando de agentes econômicos.

Conceitualmente, pode-se compreender o algoritmo como complexo descritivo de etapas que, se executadas na sequência correta, permite a determinado programa de computador se desincumbir de tarefa que foi pré-estabelecida.

Cabe destacar, principalmente diante do fato de que "muitos dos algoritmos-chave que afetam a vida pública são, também, considerados proprietários ou segredos comerciais"[10] a dificuldade de se difundir, sob o aspecto cultural, a importância do domínio desse conceito, em especial sob o prisma de sua legitimidade.

À guisa de exemplo, cite-se caso do robô virtual vinculado à empresa Microsoft que, em razão da sua capacidade de adaptar seu comportamento de acordo com as interações dos usuários, passou a se expressar de modo inadequado, com colocações preconceituosas[11].

A ausência de julgamento moral sobre a situação posta sob processamento por meio de algoritmos parece demandar maior atenção na medida em que os processos decisórios, de maneira geral, tendem a se utilizar cada vez mais da inteligência artificial.

Outrossim, a ausência de regulamentação sobre o tema, a falta de transparência em torno dos elementos considerados para processamento e a sua forma de relacionamento com outros fragmentos de informação dão margem à concretização de condutas arbitrárias que devem ser combatidas.

A crescente confiança na inteligência artificial tem o condão ensejar o mesmo crescimento no grau de risco envolvido no seu uso constante. Nesta senda, erros nos algoritmos utilizados no sistema persecutório evidenciam risco sistêmico[12].

[9] OSOBA, Osonde A.; WELSER, William IV, **An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence**, Santa Monica: RAND Corporation, 2017, p. 4–5.
[10] *Ibid*., p. 6.
[11] *Ibid*., p. 7.
[12] *Ibid*., p. 3.

Outrossim, o funcionamento adequado de um equipamento dotado da capacidade de tomar decisões autonomamente demanda o processamento de um extenso volume de informações o que pode colidir com eventual regime de proteção de dados em vigor[13].

No que diz respeito à transposição das regras vigentes em determinado sistema jurídico para a linguagem binária, pode-se falar em algoritmização do direito[14].

Hoje se espera que, no futuro, haja maior participação das máquinas na vida cotidiana dos indivíduos e, para cumprir esse objetivo, será necessário que se lhes confira cada vez mais autonomia, sem se olvidar, contudo, que um programa de computador tende a tomar decisões baseado na estrutura lógica desenhada, desconsiderando emoções e empatia, características inerentes à condição humana.

Nessa perspectiva, há aspecto relevante e ainda pouco debatido relacionado ao tema da tecnologia e direito, qual seja a possiblidade de se elaborar códigos de programação acrescentando-se em sua estrutura dispositivos legais.

Nesse contexto, a possibilidade de automação da tomada de decisões por agentes públicos e privados parece criar amplo espaço para o incremento da demanda por *softwares* e equipamentos que permitam aos atores sociais, que se utilizam desses instrumentos, terem a segurança de que autuam de acordo com a lei.

A objetividade subjacente a decisões tomadas por computador pode se revelar eticamente deficiente e é muito mais difícil se identificar essa particularidade. Há, ainda, outra situação preocupante: a complexidade da elaboração de legislação capaz de defender os indivíduos contra análises probabilísticas realizadas por programa de computador, de sorte que elementos discriminatórios podem fazer parte do algoritmo conquanto, caso aberto seu código-fonte, não se tenha nada que conecte diretamente o comportamento do *software* à tomada de decisões de cunho discriminatório.

Em muitas situações haverá o risco da tomada de uma decisão moralmente questionável, mas indefectível do ponto de vista lógico e o sistema legal deverá enfrentar esse tipo de evento.

Cuida-se de situação real, a exemplo da constatação por usuários de internet que o Google Photos, aplicativo da empresa Alphabet Inc., rotulava pessoas negras como

[13] MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy, Discriminação algorítimica à luz da Lei Geral de Proteção de Dados, *in*: **Tratado de proteção de dados pessoais**, Rio de Janeiro: Forense, 2021.
[14] HILGENDORF, Eric; FELDLE, Jochen, **Digitalization and the Law**, Baden-Baden: Nomos, 2018.

gorilas por meio de inteligência artificial[15], ou ainda, conforme já mencionado, de robô virtual vinculado à empresa Microsoft que se expressava de modo "racista, sexista e xenófobo"[16].

No campo jurídico-criminal, em relação ao sistema de justiça americano, Osoba e Welser consideram que "os agentes artificiais ajudam a aliviar a carga de gerenciamento de um sistema tão grande. Mas qualquer viés algorítmico sistemático nestas ferramentas teria um alto risco de erros e desvantagens cumulativas"[17].

Correlacionado ao tema, vale menção a estudo estatístico sobre o sistema de avaliação de risco criminal do Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), *software* comumente utilizado no sistema criminal dos Estados Unidos, no qual, após o exame de mais de 10.000 (dez mil) casos, se reconheceu viés racial grave na estimativa do risco do avaliado, pois "os réus negros tinham muito mais probabilidade do que os réus brancos de serem julgados incorretamente como correndo um risco maior de reincidência, enquanto os réus brancos tinham mais probabilidade do que os réus negros de serem marcados incorretamente como de baixo risco"[18].

No que concerne à tecnologia de reconhecimento facial, o National Institute of Standards and Technology (NIST), vinculado ao Departamento de Comércio dos Estados Unidos, em dezembro de 2019, publicou resultados de estudo no qual foram avaliados o desempenho de 189 *softwares* de 99 desenvolvedores na consecução de atividades nas quais a tecnologia normalmente é empregada, a exemplo de cruzamento de fotos do mesmo indivíduo e de um indivíduo em relação a uma base de dados[19].

A equipe que conduziu o trabalho utilizou 18,27 (dezoito vírgula vinte e sete) milhões de imagens de 8,49 (oito vírgula quarenta e nove) milhões de pessoas fornecidas por órgãos públicos americanos.

---

[15] SALAS, Javier, **Google conserta seu algoritmo "racista" apagando os gorilas**, EL PAÍS, disponível em: <https://brasil.elpais.com/brasil/2018/01/14/tecnologia/1515955554_803955.html>. acesso em: 17 dez. 2020.

[16] CANO, Rosa Jiménez, **O robô racista, sexista e xenófobo da Microsoft acaba silenciado**, EL PAÍS, disponível em: <https://brasil.elpais.com/brasil/2016/03/24/tecnologia/1458855274_096966.html>. acesso em: 17 dez. 2020.

[17] OSOBA; WELSER, **An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence**, p. 13.

[18] MATTU, Jeff Larson, Julia Angwin,Lauren Kirchner,Surya, **How We Analyzed the COMPAS Recidivism Algorithm**, ProPublica, disponível em: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm?token=hu_h_ohsz1Wn-XTk2j_VqS_evU4HvJdk>. acesso em: 30 dez. 2020.

[19] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee, **Face recognition vendor test part 3:: demographic effects**, Gaithersburg, MD: National Institute of Standards and Technology, 2019.

Não foram utilizadas imagens coletadas diretamente de redes sociais e de outros sítios eletrônicos. As imagens continham metadados trazendo informações acerca dos indivíduos, tais como idade, sexo, raça e nacionalidade.

Concluiu-se que os sistemas de reconhecimento facial, como regra, apresentam diferenças na capacidade de um algoritmo de cruzar duas imagens segundo a variação demográfica. Constatou-se, ainda, maior probabilidade de falsos positivos em relação a indivíduos negros e asiáticos.

Em relação aos sistemas desenvolvidos nos Estados Unidos, a taxa de erro permaneceu alta e dentro da linearidade encontrada. Em contrapartida, os sistemas desenvolvidos por países asiáticos apresentaram taxas menores de falsos positivos entre pessoas de etnias asiática e caucasiana.

Há que se ressaltar que o estudo referido não se debruçou em encontrar as relações de causa e efeito, mas nos parece possível correlacionar os erros a quem desenvolve o algoritmo e aos dados utilizados para "treinar" o algoritmo, de sorte que o uso de dados diversificados pode trazer resultados menos díspares.

Em âmbito brasileiro, há fator que não pode ser desconsiderado, pois as tecnologias de reconhecimento facial adotadas pela administração pública são oriundas de países como China, Israel e Estados Unidos[20]. Ou seja, não há o desenvolvimento propriamente brasileiro desses sistemas o que pode vir a revelar menor aptidão dos programas utilizados para se atingir as finalidades pretendidas.

## 2.3 O AVANÇO DO PUNITIVISMO GLOBAL E OS SEUS REFLEXOS NAS TECNOLOGIAS DE RECONHECIMENTO FACIAL

Com efeito, não há como se dissociar o avanço do punitivismo de forma global do modelo socioeconômico predominante nos países ocidentais.

Roger Matthews, em artigo intitulado “O mito da punitividade revisitado”[21], observa uma confluência de valores tanto “de baixo para cima”, dos membros da sociedade em geral, quanto de “cima para baixo”, de políticos que pautam sua atuação na exarcebação da persecução penal no afã de aumentar o seu apoio eleitoral.

[20] REIS, Carolina; ALMEIDA, Eduarda; DA SILVA, Felipe, **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil.**, Brasília: Laboratório de Políticas Públicas e Internet, 2021, p. 24.
[21] MATTHEWS, Roger, O mito da punitividade revisitado, **Justiça Criminal e Democracia II**, n. 1, p. 432, 2015.

O autor aborda o conceito de “punitividade populista”, o qual se apresenta como um dos principais componentes da política penal e de fixação da pena. Tem grande relevância na construção do direito penal vigente, pois identifica um distanciamento da opinião dos especialistas conduzindo à produção de um direito penal que adota penas mais duras, com maior uso da prisão e, em suma, de maior conteúdo retributivo.

A fim de conferir robustez ao seu raciocínio, Matthews busca estabelecer alguns conceitos importantes.

Começa por “Punitividade”. Reconhece a imprecisão terminológica em torno da expressão, o que justificaria, em certa medida, sua ampla utilização. Todavia, suscita sua inadequação para expressar de modo amplo e coerente as possibilidades de incidência das sanções penais e propõe a adoção do termo tolerância, o qual se consubstancia, a um só tempo, como indutor da ideia de limite, mais do que de condenação de ações penalmente relevantes.

Aponta, também, um condicionamento do direito penal fortemente influenciado pelas classes dominantes que têm suas ideias propagadas através de agentes políticos e dos meios de comunicação e aponta um fenômeno crescente de divisão da sociedade entre ricos e pobres.

Assim, o direito penal atuaria como instrumento de controle da sociedade, perdendo o seu foco individual.

Cabe destacar, ainda dentro do estudo do autor, a tensão entre linhas de pensamento que reconhecem na punitividade uma forte carga de crueldade e de valores morais e, de outro, que aqueles que apontam apenas uma antecipação da tutela penal (risco) desprendida de carga moral.

O que se percebe é um movimento dos fins da pena no sentido de se afastar das finalidades tradicionais de retribuição e prevenção e caminhar em direção à noção de gerenciamento social, retirando de circulação sujeitos socialmente malquistos.

Com efeito, o crescimento dos índices de encarceramento não seriam, necessariamente, um produto de uma nova moldura punitivista. Haveria forte influência da disfuncionalidade que o sistema de gerenciamento de riscos penalmente relevantes, associado a uma inerente impessoalização do direito penal, gera na sociedade.

Há verdadeira convergência de ideias e opiniões, principalmente a partir da consagração dos valores neoliberais, no sentido de robustecer o sentimento social, induzido, ou não, de necessidade de incremento das sanções penais e de medidas de segurança pública. Assim, os agentes que detém condições de influenciar a política

criminal de modo efetivo, ainda que em posições políticas antagônicas, defendem, nesse ponto, a mesma bandeira.

Com efeito, a cognominada "punitividade populista" parece estar intimamente relacionada ao tema em debate, porquanto os novos mecanismos de fiscalização, em especial o reconhecimento facial, podem se convolar em poderoso instrumento de constrição da liberdade de grupos historicamente desfavorecidos e clientes habituais do sistema penal.

Dentro da realidade brasileira, conquanto não se cuide de situação de atuação de inteligência artificial, vale a menção ao caso de Bárbara Querino, "condenada a cinco anos de prisão por um assalto que ocorreu na Cidade Ademar, zona sul de São Paulo, enquanto ela estava no município do Guarujá, a trabalho"[22], com base em reconhecimento fotográfico.

Por oportuno, vale a reflexão feita por Rosane Silva e Fernanda da Silva: "[se] somente por meio do reconhecimento fotográfico – instrumento este que também sofre questionamentos dentro do Direito -, uma jovem negra foi condenada à prisão, imagine-se com o uso indiscriminado e não reflexivo das tecnologias de reconhecimento facial"[23].

Em outros países, o uso da tecnologia de reconhecimento facial tem fomentado discussões, como se infere a partir de petição elaborada pela The American Civil Liberties Union (ACLU)[24], na qual a entidade aponta que Robert Williams foi equivocadamente preso, na frente de sua casa, diante de sua esposa e duas filhas, em razão de um suposto furto a uma loja de departamentos, com base em erro de algoritmo de reconhecimento facial, no bojo de investigação de subtração de cinco relógios avaliados em aproximadamente $3,800 (três mil e oitocentos) dólares.

Os investigadores, ao revisarem as imagens de câmeras de segurança, identificaram um homem, aparentemente negro, um boné de *baseball* e uma jaqueta escura. Em março de 2019, a polícia aplicou um sistema de reconhecimento facial sobre as imagens e chegou à imagem da carteira de motorista de Robert Julian-Borchak Williams que foi preso.

---

[22] COSTA, Amarilis *et al*, Bárbara Querino e a realidade carcerária brasileira.
[23] SILVA, Rosane Leal da; SILVA, Fernanda dos santos Rodrigues da, Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro, *in*: , 5 CONGRESSO INTERNACIONAL DIREITO E CONTEMPORANEIDADE: mídias e direitos da sociedade em rede, 02, 03 set: Universidade Federal de Santa Maria, RS, 2019, p. 13.
[24] COX, Kate, **Police use of facial recognition violates human rights, UK court rules**, Ars Technica, disponível em: <https://arstechnica.com/tech-policy/2020/08/police-use-of-facial-recognition-violates-human-rights-uk-court-rules/>. acesso em: 15 ago. 2020.

De acordo com a mencionada petição, erros dessa natureza têm muito mais chances de acontecer quando se cuida de pessoas negras e, certamente, poderiam ser evitados.

É imprescindível que novas tecnologias não contemplem a perpetuação de práticas equivocadas.

No que concerne ao reconhecimento facial, a adoção de sistema de vigilância massivo baseado nessa tecnologia, pode potencializar essas formas de discriminação[25].

## 2.4 A TEORIA CRÍTICA DA RAÇA: UM PONTO DE PARTIDA PARA A MINIMIZAÇÃO DO VIÉS ALGORÍTMICO

No ponto, se mostra pertinente a referência ao estudo realizado por Tukufu Zuberi, o qual, conquanto se refira às ciências sociais, se mostra de todo aplicável às ciências exatas quando atuam em intersecção com as sociais.

O autor realiza um cotejo entre a Teoria Crítica da Raça no direito e as teorias críticas da raça nas ciências sociais.

Considera que o conhecimento produzido nas ciências sociais reflete os sistemas de opressão com matizes de dominação. Tem-se um processo de padronização a partir de um modelo de indivíduo: branco, heterossexual, burguês, homem. Tudo aquilo que está fora desse padrão estabelecido seria reconhecido como desvio.

A Teoria Crítica da Raça (TCR) é um dos movimentos mais importantes, pois torna possível visualizar o papel fundamental que o direito desempenha na manutenção da hierarquia racial e fornece substrato para que essa realidade possa ser modificada.

Com efeito, não se pode olvidar que as ciências sociais, em determinado momento, se desenvolveram em um período no qual a estratificação social com base na raça precisava ser justificada e a continuação da segmentação mesmo em ambientes democráticos e, em algumas realidades, com justificação constitucionalmente amparada "não fez nascer a objetividade na análise da raça, nem permitiu que as ciências sociais refletissem sobre a tradição crítica já presente no século XIX. As ciências sociais desenvolveram teorias e métodos de análises que ajudaram a justificar a estratificação racial"[26].

[25] SILVA; SILVA, Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro.

[26] ZUBERI, Tukufu, Teoria crítica da raça e da sociedade nos Estados Unidos, **Cadernos do CEAS**, n. 238, 2016, p. 469.

Outrossim, para o referido autor, "a integração das ciências sociais não foi feita com a finalidade de transformar a teoria sociológica ou seus métodos; de fato, muitos cientistas sociais de cor e mulheres que integraram as disciplinas se tornaram 'acadêmicos brancos com peles negras'"[27].

Este fato levou os cientistas críticos sociais a uma tradição que desafiava estes parâmetros, uma tradição que fora isolada do prestígio do pensamento central da academia"[28], sendo certo que "uma perspectiva assimilacionista" dominou a sociologia da raça e "a partir desta perspectiva, [não-brancos] representavam um problema de assimilação social"[29].

Considera, ainda, que a maioria dos sociólogos "seguiam a pesquisa nas ciências sociais sem qualquer reserva à influência da raça e da economia de mercado"[30] em suas perspectivas.

Estes estudos com frequência produziam estatísticas raciais diferentes, as quais eram usadas para justificar a continuidade da estratificação racial e rejeitar a humanidade dos não-brancos, de sorte que "as tendências dentro do espectro da perspectiva assimilacionista variam de acordo com a moralização dos vários autores por meio de pesquisas em segregação e estratificação social e econômica"[31].

Nesse trilhar, a TCR, ao se voltar para o exame do poder social dentro da sociedade, se revela como "articulação moderna da crítica desenvolvida no início do século XX sobre as fundações da racionalidade ocidental que dão base à lógica branca"[32].

As perspectivas críticas, em sua maioria, são temperadas com referenciais antagônicos e, com o tempo, se revelam mais ideológicas do que efetivamente transformadoras da sociedade[33].

É válida, ainda, a advertência feita por Manoel Gonçalves Ferreira Filho no sentido da necessidade de se analisar de forma completa os aspectos relacionados ao racismo, no afã de não se estimular ainda mais segregação com a adoção de medidas protetivas irrefletidas[34].

---

[27] *Ibid*.
[28] ZUBERI, Teoria crítica da raça e da sociedade nos Estados Unidos.
[29] *Ibid*.
[30] *Ibid*.
[31] ZUBERI, Teoria crítica da raça e da sociedade nos Estados Unidos, p. 470.
[32] *Ibid*., p. 473.
[33] ZUBERI, Teoria crítica da raça e da sociedade nos Estados Unidos, p. 474–475.
[34] FILHO, Manoel Gonçalves Ferreira, **Comentários à Constituição Brasileira de 1988**, 2. ed. São Paulo: Saraiva, 1997, p. 57.

A referência que se faz sobre a teoria crítica da raça se dá justamente para se enfatizar a necessidade de se considerarem os grupos desfavorecidos durante todo o processo de criação e de implementação de políticas públicas, sob pena de, por meio do pretexto de avanço tecnológico, se estar robustecendo o sistema segregador e isolacionista de sujeitos tidos como socialmente indesejáveis[35].

## 2.5 O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NO BRASIL E O RISCO DE REFORÇO DO RACISMO ESTRUTURAL

No ano de 2021, o Governador do Estado de São Paulo vetou Projeto de Lei que tornava obrigatória a instalação de câmeras de reconhecimento facial em todas as estações do Metrô e da Companhia Paulista de Trens Metropolitanos (CPTM), bem como no interior dos vagões das composições[3637].

Na contramão dessa medida, aponta-se a Portaria nº 793/2019[38] que prevê como eixo do enfrentamento à criminalidade violenta o fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* (OCR), uso de inteligência artificial ou outros, sem referência a qualquer contramedida de limitação no uso dessa tecnologia. Outros entes da federação também utilizam essa tecnologia: os Estados do Ceará, Rio de Janeiro, Bahia e Distrito Federal[39].

Mais recentemente sobreveio a notícia, veiculada pelo Ministério da Justiça e Segurança Pública, dando conta de que a Polícia Federal do Brasil teria firmado contrato

[35] Em estudo recente realizado pela Rede de Observatórios da Segurança, projeto do Centro de Estudos de Segurança e Cidadania (CESeC) da Universidade Candido Mendes, se constatou, a partir do monitoramento de casos de prisões e abordagem com o uso de reconhecimento facial em 4 (quatro Estados) que "em relação aos casos em que havia informações sobre raça e cor, ou quando havia imagens dos abordados (42 casos), 90,5% das pessoas eram negras e 9,5% eram brancas". In: NUNES, Pablo, **Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil**, Retratos da Violência Cinco meses de monitoramento, análises e descobertas, disponível em: <https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf>. acesso em: 17 jul. 2021.

[36] LEAL, Aline, **Doria veta projeto para instalação de reconhecimento facial no Metrô**, Agência Brasil, disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2021-03/doria-veta-projeto-para-instalacao-de-reconhecimento-facial-no-metro>. acesso em: 23 mar. 2021.

[37] Medida similar foi adotada pelo governo do Estado de Nova Iorque no ano de 2020. In: NYCLU, The New York Civil Liberties Union, **New York Creates First-in-the-Nation Moratorium on Facial Recognition in Schools**, disponível em: <https://www.nyclu.org/en/press-releases/new-york-creates-first-nation-moratorium-facial-recognition-schools>. acesso em: 2 fev. 2021.

[38] BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 793/2019 que 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: Publicado em: 25/10/2019, Edição: 208, Seção: 1, Página: 55.

[39] REIS; ALMEIDA; DA SILVA, **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil.**

para a aquisição de sistema que pretende coletar, armazenar e cruzar dados pessoais sensíveis de brasileiros[40].

Alguns estudos apontam que tecnologias aparentemente neutras utilizadas como instrumentos de aplicação da lei, a exemplo de testes de drogas, leitores automáticos de placas de veículos, não foram criados a partir de uma posição de neutralidade e tal circunstância tem afetado de modo desproporcional pessoas negras[41].

Rachel Fleischer identifica três modos de manifestação de vieses que impactam diretamente pessoas negras classificados da seguinte maneira: a) viés na forma como a tecnologia tem impacto direto nas Pessoas de Cor a partir de sua própria concepção; b) parcialidade na forma como os preconceitos implícitos de cada um afetam a utilização e implementação de tecnologia sem vícios em sua concepção; e c) enviesamento na forma como a utilização de tecnologia defeituosa em conjunto com enviesamentos implícitos inerentes ao projeto desde a sua concepção cria impacto díspar sobre as pessoas de cor negra[42].

Com efeito, conforme destacado por Sílvio Almeida, "o racismo é uma forma sistemática de discriminação que tem a raça como fundamento, e que se manifesta por meio de práticas conscientes ou inconscientes que culminam em desvantagens ou privilégios para indivíduos, a depender do grupo racial ao qual pertençam"[43].

Neste contexto, a significativa falta de precisão em torno da forma de desenvolvimento de tecnologias de reconhecimento facial pode conduzir a população negra a sentir mais direta e negativamente os impactos da vigilância de massa, conforme já ocorre atualmente sem o uso indiscriminado de novas tecnologias auxiliares de repressão policial[44].

---

[40] Segundo o Ministério da Justiça, o programa de Solução Automatizada de Identificação Biométrica (Abis) possibilitará a identificação de pessoas com coleta, armazenamento e o cruzamento de dados da impressão digital e o reconhecimento facial, de forma precisa e confiável. Sendo certo, ainda, que o programa seria projetado "para armazenar, em 48 meses, dados de 50,2 milhões de pessoas, com possibilidade para expansões posteriores que poderão conter dados de até 200 milhões de indivíduos". In: BRASIL, Ministério da Justiça e Segurança Pública, **Polícia Federal implementa nova Solução Automatizada de Identificação Biométrica**, Polícia Federal, disponível em: <https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica>. acesso em: 21 jul. 2021.

[41] A título de exemplo, cite-se o estudo de Rachel Fleischer. In: FLEISCHER, R. S., Bias In, Bias Out: Why Legislation Placing Requirements on the Procurement of Commercialized Facial Recognition Technology Must Be Passed to Protect People of Color., **Public Contract Law Journal**, v. 50, n. 1, p. 63–89, 2020.

[42] *Ibid*., p. 69.

[43] ALMEIDA, **O que é racismo estrutural?**, p. 22.

[44] SILVA; SILVA, Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro, p. 2.

É inarredável a necessidade de se questionar a suposta neutralidade dos algoritmos. Os sistemas de controle social são, como regra, frutos de uma decisão política anterior. Assim, a seletividade do sistema penal, ainda que de forma indireta, acaba por reforçar a repressão sobre categorias de indivíduos que já seriam destinatários naturais do sistema repressivo[45].

É certo que o uso de espaços públicos e a livre circulação de indivíduos devem ser encarados como manifestação concreta do princípio da dignidade da pessoa humana, insculpido no artigo 1º, III, da Constituição Federal.

O referido princípio se alicerça no respeito ao indivíduo pelo Estado e pela própria comunidade. Cuida-se, a um só tempo, de uma garantia de posições contra tratamento inadequado e de fonte de obrigação de tratamento adequado. É dizer: deve-se garantir aos indivíduos a possibilidade de pleno e livre desenvolvimento de sua personalidade a partir de um sistema recíproco de respeito por todos que se encontram inseridos em uma dada realidade.

Com efeito, não se pode olvidar da feição instrumental do direito enquanto fenômeno viabilizador da existência humana digna, sendo certo o relevante papel da jurisdição constitucional que, a partir do diálogo entre código e constituição, pode conduzir a soluções juridicamente racionais e aceitáveis para complexos problemas da vida humana.

É imprescindível que se pense a adoção de novas tecnologias à luz da questão do racismo, principalmente em um esforço preventivo de lesão a direitos fundamentais de minorias historicamente situadas à margem do comportamento estatal ético.

## 2.6 A NECESSIDADE DE OBSERVÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS NO TRATO DE DADOS SENSÍVEIS

O reconhecimento da proteção de dados como direito fundamental pelo Supremo Tribunal Federal[46] e a recente promulgação da Emenda Constitucional nº 115[47] conferem

[45] SILVA, Tarcizio da, VISÃO COMPUTACIONAL E RACISMO ALGORÍTMICO: BRANQUITUDE E OPACIDADE NO APRENDIZADO DE MÁQUINA, **Revista da Associação Brasileira de Pesquisadores/as Negros/as (ABPN)**, v. 12, n. 31, 2020, p. 445.

[46] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Ação Direta de Inconstitucionalidade nº 6.387. Rel. Min. Rosa Weber. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true>. Acesso em: 9 dez. 2020.

[47] A Emenda Constitucional nº 115 "altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais".

à discussão matriz constitucional o que se revela bastante interessante, principalmente se considerados os riscos de vulneração da dignidade da pessoa humana associados ao reconhecimento facial, servindo de exemplo o já mencionado reforço do racismo estrutural existente na sociedade brasileira.

Conforme sugerido pelo nome da tecnologia, o reconhecimento facial funciona a partir do processamento de elementos únicos da face dos indivíduos. São coletadas certas informações, as quais são processadas por software e, mediante correlação dos dados colhidos, se individualiza alguém. Esse tipo de dado é considerado biométrico[48] o qual é destinatário de proteção especial pela Lei Geral de Proteção de dados (LGPD), porquanto considerado dado sensível[49].

Segundo Rodotà, "a classificação desses dados na categoria de dados 'sensíveis', particularmente protegidos contra os riscos da circulação, deriva de sua potencial inclinação para serem utilizados com finalidades discriminatórias"[50]. Deveras, se vislumbra certa dificuldade na adoção desse recurso tecnológico de vigilância em massa pelas razões que se passa a expor.

Primeiro, em linha de princípio, o reconhecimento facial, para ser realizado, não depende da aceitação da pessoa que tem o dado coletado. Em verdade, sequer é necessário o seu conhecimento a respeito do fato. Em segundo lugar, o risco de discriminação sistemática de certos grupos também não pode ser ignorado. Em terceiro, a categoria especial do dado tratado requer maior rigidez em seu processamento.

Demais disso, o princípio da autodeterminação informativa parece inviabilizar o uso do dado biométrico quando há o risco de sua coleta e tratamento sem o conhecimento do titular. Valendo, destacar, também, que a transparência é a premissa para uma participação efetiva dos indivíduos, fontes de dados, no processamento e circulação de informações sobre si.

Outrossim, conquanto a LGPD exclua de seu âmbito de aplicação atividades de investigação e repressão de infrações penais, há previsão expressa de observância dos princípios gerais de proteção e os direitos do titular previstos naquela lei[51].

[48] REIS; ALMEIDA; DA SILVA, **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil.**
[49] Art. 5º, II e art. 11 da LGPD.
[50] RODOTÀ, Stefano, **A vida na sociedade da vigilância: a privacidade hoje**, Rio de Janeiro: Renovar, 2008, p. 95.
[51] Art. 4º, III, "d" e §1º, da LGPD.

Nesse contexto, a vigilância ampla, de forma irrestrita, em ambientes públicos não se coaduna com o princípio da finalidade do tratamento dos dados e, menos ainda, com o princípio da necessidade que preconiza a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados[52].

Ainda, não se pode ignorar o princípio da prevenção, insculpido no art. 6º, VIII, da LGPD, o qual preconiza a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. A adoção de tecnologia tão intrusiva quanto a que é objeto desse estudo deve ser acompanhada de cautela, principalmente quando há dúvidas sobre os impactos indesejáveis nas vidas dos indivíduos.

Cabe destacar, também, que o regime de tratamento de dados pessoais pelo Poder Público tem regulação específica a partir do art. 23 da LGPD e, dentro dos seus requisitos de legalidade, está o dever de informar as hipóteses em que, no exercício de suas competências, as pessoas jurídicas de direito público realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.

Ademais, o relatório de proteção de impacto à proteção de dados é instrumento que permite, nessa situação, a análise objetiva da relação entre os benefícios hauridos do uso da tecnologia e da intrusão na esfera da privacidade dos indivíduos, bem como potencializa a evolução da discussão na busca de medidas mitigadoras da lesão ao direito à proteção de dados. Apesar da importância da ferramenta, o uso de tecnologias de vigilância dessa natureza não vem sendo acompanhado da elaboração desse documento[53].

No direito comparado, a Diretiva 680/2016 estabelece a necessidade de aferição objetiva dos riscos do tratamento dos dados relacionados à segurança pública, devendo ser feita referência à natureza, âmbito, contexto e finalidades do tratamento[54]. Nesse contexto, o relatório de impacto de tratamento de dados é essencial para esse desiderato[55].

[52] Art. 6º, III, da LGPD.
[53] REIS; ALMEIDA; DA SILVA, **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil.**, p. 30.
[54] Considerandos 26, 51 e 52 do Regulamento 680/2016. In: UNIÃO EUROPEIA, **Regulamento (UE) 2016/680 do Parlamento Europeu e do Conselho**, disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=PT>. acesso em: 3 maio 2021.
[55] EUROPEAN COMISSION, **Guidelines 3/2019 on processing of personal data through video devices**, disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf>. acesso em: 15 jul. 2021.

Voltando ao contexto brasileiro, a opacidade dos algoritmos utilizados associada à falta de transparência dos poderes públicos quanto ao uso do reconhecimento facial[56] não permite o conhecimento pelos interessados do contexto no qual são tratadas as informações que lhe digam respeito e dificulta sobremaneira a contenção de condutas abusivas perpetradas pelos agentes de segurança pública e, também, de tratamento de dados.

Portanto, diante do volume e da sensibilidade dos dados coletados e processados e dos potenciais reflexos no direito ambulatorial dos cidadãos, ressoa inequívoca a necessidade de elaboração de lei específica uniforme, de alcance nacional, a qual estabeleça balizas normativas que viabilizem o uso da tecnologia e, ao mesmo tempo, preserve direitos e garantias fundamentais, não sendo suficiente a edição de normas locais[57].

Deve-se promover discussões amplas com a participação de diferentes setores da sociedade, similarmente ao que aconteceu durante aproximadamente oito anos em relação à LGPD[58] e vem ocorrendo em relação à "LGPD penal"[59] .

## 3 CONSIDERAÇÕES FINAIS

A tecnologia de reconhecimento facial não é infensa a erros. A tensão entre a promoção de avanços na segurança pública e a potencial restrição da liberdade e privacidade dos cidadãos revela um prospecto que requer absoluta cautela, principalmente no que concerne à formulação e implementação de políticas públicas relacionadas ao assunto[60].

---

[56] REIS; ALMEIDA; DA SILVA, **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil.**

[57] De acordo com o Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil, alguns Estados regulam o tema por meio de lei em sentido estrito, a exemplo do Distro Federal (Lei Distrital 6.172/2020) e outros por meio de atos infralegais como Estado da Bahia. In: *Ibid*.

[58] De acordo com o sítio eletrônico do Ministério da Justiça, os primeiros debates sobre a proteção de dados pessoais tiveram início em 30/11/2020. Disponível em: <http://pensando.mj.gov.br/debates/>. Acesso em 20 abr. 2021.

[59] COSTA, Eduarda; REIS, Carolina, **LGPD Penal: o que foi feito até aqui e quais são os próximos passos?**, LAPIN, disponível em: <https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/>. acesso em: 19 jul. 2021.

[60] A propósito, a Organização dos Estados Americanos (OEA), por meio de Declaração Conjunta do Relator Especial das Nações Unidas (ONU) para a Liberdade de Opinião e Expressão, do Representante da Organização para a Segurança e Cooperação na Europa (OSCE) para a Liberdade dos Meios de Comunicação, do Relator Especial da Organização dos Estados Americanos (OEA) para a Liberdade de Expressão e a Relatora Especial para a Liberdade de Expressão e Acesso à Informação da Comissão Africana de Direitos Humanos e dos Povos (CADHP), no ano de 2019, reconheceu: (...) a necessidade de abordar, dentro do contexto do direito internacional dos direitos humanos, os problemas graves que surgem no contexto das tecnologias digitais, entre os quais se encontram a desinformação; a incitação ao ódio; a

Com efeito, há que se abandonar a preconcepção de que os avanços tecnológicos são sempre benéficos[61]. A rapidez do progresso técnico-científico se contrapõe ao lento amadurecimento da capacidade de controle dos processos sociais que ladeiam essa evolução. Nesse contexto, o sujeito não pode ser considerado mera fonte de dados, deve haver o fortalecimento de sua posição jurídica através da implementação de mecanismos de controle sobre o tratamento de dados a seu respeito.

Não é o escopo do presente trabalho esmiuçar os aspectos que influenciam os algoritmos de reconhecimento facial e, tampouco, estabelecer critérios que conduzam à uma correta aplicação da tecnologia.

Todavia, entende-se que o uso de dados pessoais como instrumento de investigação e de segurança pública deve levar em consideração esses elementos, principalmente na elaboração e condução da política criminal de determinado Estado.

Um dos caminhos para a solução do problema do viés do algoritmo passa pela conciliação de abordagens técnicas e não técnicas, sendo a transparência o anteparo sobre o qual se projetarão as soluções.

É imprescindível que aspectos multiculturais sejam levados em consideração e conhecê-los parece ser passo fundamental, da mesma forma que se revela imperiosa consideração de que algoritmos podem, sim, por si sós, conduzir a resultados injustos.

Ainda, é preciso se reconhecer, dentro da tábua de valores dos modernos ordenamentos jurídicos, o direito fundamental à proteção de dados como garantia do pleno desenvolvimento da personalidade e, *a fortiori*, como garantia dos consagrados valores da liberdade e da democracia.

Demais disso, sem menoscabar a importância da existência de normas gerais as quais estabelecem balizas normativas ao tratamento de dados, no caso de uso de tecnologias com alto grau de intrusão na esfera privada e elevado risco de restrição a direitos e garantias fundamentais, é imprescindível a elaboração de legislação específica sobre o tema que trace parâmetros precisos capazes de conferir segurança jurídica aos agentes de tratamento e, também, se proteger adequadamente os direitos dos titulares de dados.

discriminação e a violência; o recrutamento e a propaganda terroristas; a vigilância arbitrária e ilegal; a interferência a respeito do uso de tecnologias de encriptação e o anonimato, e o poder dos intermediários online. *In*: OEA, **OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo**, disponível em: <https://www.oas.org/pt/cidh/expressao/>. acesso em: 23 mar. 2021.

[61] RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**.

## REFERÊNCIAS

ALMEIDA, Silvio. **O que é racismo estrutural?** São Paulo: Pólen, 2019.

ARNDT, A. B. Al-Khwarizmi. **The Mathematics Teacher**, v. 76, n. 9, p. 668–670, 1983.

BAUMAN, Zygmunt. **Identidade - Entrevista a Benedetto Vecchi**. Trad. Carlos Alberto MEDEIROS. 1. ed. Rio de Janeiro: Jorge Zahar, 2005.

Brasil. Lei nº 13.709, DE 14 de agosto de 2018. Lei Geral de Proteção de dados. Diário Oficial da União - Edição extra de 15 ago. 2018

BRASIL. Ministério da Justiça e Segurança Pública. **Polícia Federal implementa nova Solução Automatizada de Identificação Biométrica**. Polícia Federal. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica>. Acesso em: 21 jul. 2021.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Ação Direta de Inconstitucionalidade nº 6.387. Rel. Min. Rosa Weber. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true>. Acesso em: 9 dez. 2020.

CANO, Rosa Jiménez. **O robô racista, sexista e xenófobo da Microsoft acaba silenciado**. EL PAÍS. Disponível em: <https://brasil.elpais.com/brasil/2016/03/24/tecnologia/1458855274_096966.html>. Acesso em: 17 dez. 2020.

CITRON, Danielle Keats; PASQUALE, Frank A. **The Scored Society: Due Process for Automated Predictions**. Rochester, NY: Social Science Research Network, 2014. Disponível em: <https://papers.ssrn.com/abstract=2376209>. Acesso em: 30 dez. 2020.

COSTA, Amarilis; VITORINO, Amanda; RICCI, Beatriz; *et al*. Bárbara Querino e a realidade carcerária brasileira. Disponível em: <http://www.justificando.com/2018/10/15/barbara-querino-a-realidade-carceraria-brasileira-2/>. Acesso em: 22 dez. 2020.

COSTA, Eduarda; REIS, Carolina. **LGPD Penal: o que foi feito até aqui e quais são os próximos passos?** LAPIN. Disponível em: <https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/>. Acesso em: 19 jul. 2021.

COX, Kate. **Police use of facial recognition violates human rights, UK court rules**. Ars Technica. Disponível em: <https://arstechnica.com/tech-policy/2020/08/police-use-of-facial-recognition-violates-human-rights-uk-court-rules/>. Acesso em: 15 ago. 2020.

EUROPEAN COMISSION. **Guidelines 3/2019 on processing of personal data through video devices**. Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf>. Acesso em: 15 jul. 2021.

FILHO, Manoel Gonçalves Ferreira. **Comentários à Constituição Brasileira de 1988**. 2. ed. São Paulo: Saraiva, 1997.

FLEISCHER, R. S. Bias In, Bias Out: Why Legislation Placing Requirements on the Procurement of Commercialized Facial Recognition Technology Must Be Passed to Protect People of Color. **Public Contract Law Journal**, v. 50, n. 1, p. 63–89, 2020.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face recognition vendor test part 3:: demographic effects**. Gaithersburg, MD: National Institute of Standards and Technology, 2019. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 15 ago. 2020.

HILGENDORF, Eric; FELDLE, Jochen. **Digitalization and the Law**. Baden-Baden: Nomos, 2018.

LEAL, Aline. **Doria veta projeto para instalação de reconhecimento facial no Metrô**. Agência Brasil. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2021-03/doria-veta-projeto-para-instalacao-de-reconhecimento-facial-no-metro>. Acesso em: 23 mar. 2021.

MATTHEWS, Roger. O mito da punitividade revisitado. **Justiça Criminal e Democracia II**, n. 1, p. 432, 2015.

MATTU, Jeff Larson, Julia Angwin,Lauren Kirchner,Surya. **How We Analyzed the COMPAS Recidivism Algorithm**. ProPublica. Disponível em: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm?token=hu_h_ohsz1Wn-XTk2j_VqS_evU4HvJdk>. Acesso em: 30 dez. 2020.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítimica à luz da Lei Geral de Proteção de Dados. *In*: **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

NUNES, Pablo. **Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil**. Retratos da Violência Cinco meses de monitoramento, análises e descobertas. Disponível em: <https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf>. Acesso em: 17 jul. 2021.

NYCLU, The New York Civil Liberties Union. **New York Creates First-in-the-Nation Moratorium on Facial Recognition in Schools**. Disponível em: <https://www.nyclu.org/en/press-releases/new-york-creates-first-nation-moratorium-facial-recognition-schools>. Acesso em: 2 fev. 2021.

OEA. **OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo**. Disponível em: <https://www.oas.org/pt/cidh/expressao/>. Acesso em: 23 mar. 2021.

OSOBA, Osonde A.; WELSER, William IV. **An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence**. Santa Monica: RAND Corporation, 2017. Disponível em: <https://www.rand.org/pubs/research_reports/RR1744.html>. Acesso em: 22 dez. 2020.

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

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SALAS, Javier. **Google conserta seu algoritmo "racista" apagando os gorilas**. EL PAÍS. Disponível em: <https://brasil.elpais.com/brasil/2018/01/14/tecnologia/1515955554_803955.html>. Acesso em: 17 dez. 2020.

SILVA, Rosane Leal da; SILVA, Fernanda dos santos Rodrigues da. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. *In*: 5 CONGRESSO INTERNACIONAL DIREITO E CONTEMPORANEIDADE: mídias e direitos da sociedade em rede, 02, 03 set: Universidade Federal de Santa Maria, RS, 2019. Disponível em: <Disponível em: https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/congresso-direito-anais.>. Acesso em: 16 dez. 2020.

SILVA, Tarcizio da. VISÃO COMPUTACIONAL E RACISMO ALGORÍTMICO: BRANQUITUDE E OPACIDADE NO APRENDIZADO DE MÁQUINA. **Revista da Associação Brasileira de Pesquisadores/as Negros/as (ABPN)**, v. 12, n. 31, 2020. Disponível em: <https://abpnrevista.org.br/index.php/site/article/view/744>. Acesso em: 23 mar. 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/680 do Parlamento Europeu e do Conselho**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=PT>. Acesso em: 3 maio 2021.

ZUBERI, Tukufu. Teoria crítica da raça e da sociedade nos Estados Unidos. **Cadernos do CEAS**, n. 238, 2016.