Revista ARACÊ
ISSN: 2358-2472

NA COLÔNIA PENAL DIGITAL: AS LIÇÕES DE FRANZ KAFKA PARA A ADEQUADA IMPLEMENTAÇÃO DE SISTEMAS DE RECONHECIMENTO FACIAL NO BRASIL

https://doi.org/10.56238/arev7n3-178

Data de submissão: 18/02/2025 **Data de publicação:** 18/03/2025

Milton Pereira de França Netto
Doutorando em Direito pela Universidade Católica de Pernambuco e pela Universidade de Sevilha. Mestre em Direito pelo Centro Universitário Cesmac. Pesquisador e Professor de Direito Digital.
E-mail: milton.00000849969@unicap.br
ORCID: https://orcid.org/0000-0002-3671-1897

João Araújo Monteiro Neto
PhD em Direito pela Universidade de Kent no Reino Unido. Curso de Aperfeiçoamento em Resposta a Incidentes pela Organização dos Estados Americanos em parceria com o Instituto de Ciberseguridade da Espanha (INCIBE) e a Universidade de Leon na Espanha. Ex pesquisador da Universidade de Malta e Voluntário no Mandato do Relator Especial da ONU para o Direito a Privacidade. Professor de Direito Digital, Proteção de Dados Pessoais e Engenharia Jurídica no curso de Direito da Universidade de Fortaleza. Advogado especializado em Proteção de Dados e Privacidade, Presidente da Comissão de Direito Digital da OAB/CE. Certified Information Privacy Professional/Europe (CIPP/E) pela International Association of Privacy Professionals (IAPP) e Privacy Fellow pela Onetrust. Coordenador do Grupo e Estudos de Estudos em Tecnologia, Informação e Sociedade - GETIS e com atividades nas áreas de Direito da Tecnologia da Informação, Governança e Regulação da Internet, Digital Human Rights, Privacidade e Proteção de Dados Pessoais, Inteligência Artificial e Cibersegurança.
E-mail: joaoneto@unifor.br

João Paulo Allain Teixeira
Doutor em Direito pela Universidade Federal de Pernambuco. Mestre em Direito pela Universidade Federal de Pernambuco, Master em Teorías Críticas del Derecho pela Universidad Internacional de Andalucía, Espanha. Graduado em Direito pela Universidade Federal de Pernambuco. Professor na Universidade Católica de Pernambuco.
ORCID: https://orcid.org/0000-0001-9467-6973

RESUMO
O artigo visa investigar os perigos associados à implementação acrítica de sistemas de reconhecimento facial no Brasil, com especial enfoque no âmbito da segurança pública, a partir de uma releitura contemporânea do conto "Na Colônia Penal", de Franz Kafka. Servindo-se da revisão bibliográfica e da pesquisa documental, o estudo recorre à obra literária para estabelecer comparativos com os atuais dilemas enfrentados durante a implementação estatal de sistemas de reconhecimento facial, apresentando casos de erros de identificação de indivíduos. Na sequência, o trabalho se vale das lições doutrinárias de autores nacionais e estrangeiros, e de relatórios fornecidos pela iniciativa "O Panóptico" para delinear os contornos dos fenômenos do neocolonialismo digital e da discriminação algorítmica, e averiguar os seus impactos nocivos perante a população negra. Ao final, o artigo examina as previsões a respeito da temática contidas na versão mais recente do Projeto de Lei nº 2.338/2023, que se propõe a regulamentar a inteligência Artificial no Brasil, e no Artificial Intelligence

Revista ARACÊ
ISSN: 2358-2472

Act (AI Act), da União Europeia, sugestionando o aprimoramento normativo do texto nacional à luz da experiência estrangeira.

Palavras-chave: Reconhecimento Facial. Franz Kafka. Discriminação Algorítmica. Neocolonialismo Digital. Projeto de Lei Nº 2.338/2023. Artificial Intelligence Act (AI Act).

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

O constante receio de estar sendo vigiado simboliza a realidade contemporânea. Com a digitalização em massa das relações sociais, as idiossincrasias são convertidas em dados matematizados, utilizados para induzir comportamentos sob o comando silencioso de *big techs*. A inteligência artificial (IA) desponta como o aríete dessa era hiperconectada, automatizando tarefas por meio da descoberta de padrões subjacentes no oceânico *Big Data* informacional.

Dentre as suas aplicações mais controversas, os sistemas de reconhecimento facial se destacam pela evolução conferida a tais olhares espiões. Onipresentes em ruas, estádios de futebol, aeroportos, edifícios residenciais e empresariais, estações de metrô e lojas comerciais, eles permitem a instantânea identificação de pessoas após a captura de dados biométricos de seus rostos e a comparação com bancos de imagens pré-existentes.

Divulgados como respostas definitivas para os problemas que assolam a segurança pública, esses aparelhos despertam a fascinação dos entusiastas pelas novas tecnologias, materializando as advertências ficcionais acerca da admiração desmedida por máquinas cintilantes que foram sublinhadas por Frank Kafka, há mais de cem anos, no conto “Na Colônia Penal”.

O presente artigo se serve da metodologia dedutiva, ligada à revisão bibliográfica e à pesquisa documental, sob o desígnio de analisar os perigos provenientes da temerária utilização de instrumentos de reconhecimento facial à luz dos ensinamentos deixados pelo escritor tcheco na obra em questão.

Assim, o estudo recorre à narrativa kafkiana para traçar comparativos com os atuais dilemas enfrentados na implementação estatal dos sistemas de reconhecimento facial, assolada por inúmeros casos de erros de identificação. Mais à frente, a pesquisa se serve das lições doutrinárias de Alexandre Pimentel, Byung-Chul Han, Cathy O’Neil, Joy Buolamwini, Timnit Gebru, Giselle Beiguelman, Walter Lippold e Deivison Faustino para delinear os contornos do neocolonialismo digital e investigar como os algoritmos de avaliação facial se comportam em relação a grupos socialmente desprivilegiados.

Na sequência, o trabalho examina dados e relatórios publicados pela iniciativa “O Panóptico” para averiguar o nível de implementação de tais aparelhos no Brasil e o seu impacto nocivo perante a população negra, tida como o alvo central da problemática da discriminação algorítmica.

Por fim, o texto esmiuça as previsões sobre a temática contidas na versão mais recente do Projeto de Lei nº 2.338/2023, que se propõe a regulamentar a inteligência artificial no Brasil, e no *Artificial Intelligence Act (AI Act),* da União Europeia, que inaugurou o disciplinamento da área à nível global, para buscar soluções normativas aos obstáculos a ela associados.

Revista ARACÊ
ISSN: 2358-2472

2 A RELEITURA DE FRANZ KAFKA À LUZ DAS NOVAS TECNOLOGIAS

Idealizado em 1914 e publicado no ano de 1919, o conto "Na Colônia Penal" explora o cotidiano de uma instalação penitenciária insular que vem sendo afetada por discussões em torno de seu principal aparato punitivo: uma máquina autônoma de tortura lenta que se encontra desgastada após anos de contínuo funcionamento (Kafka, 2020).

Para tanto, a narrativa recorre a dois protagonistas: a) o Viajante, convidado pelo atual comandante da instalação para avaliá-la e representativo dos "olhos e ouvidos" do leitor; e b) o Oficial, munido das funções de juiz na circunscrição e de operador do citado aparato. As interações da dupla tangenciam a execução de um Condenado, que se via sob a escolta de um Soldado pela (suposta) prática do delito de desobediência[1].

Além de espelhar a tônica colonialista que deu vazão à Primeira Guerra Mundial, a obra adquire relevância ao permitir reflexões acerca de sua evolução contemporânea, o neocolonialismo digital, cuja tessitura compreende o monitoramento ininterrupto dos cidadãos-usuários, muitas vezes exercido por intermédio de ferramentas de reconhecimento facial.

Diversos paralelos podem ser traçados em relação aos acontecimentos da trama a fim de se explicar como os modernos fenômenos tecnológicos têm o condão de ciclicamente repaginar questões problemáticas pretéritas. É o que se pretende fazer a seguir.

3 "É UM APARELHO PECULIAR": O MODERNO FASCÍNIO EM TORNO DAS FERRAMENTAS DE RECONHECIMENTO FACIAL

"É um aparelho peculiar" (Kafka, 2020, p. 18). Com essa frase inaugural, o texto kafkiano antecipa as controvérsias associadas à máquina de tortura, que não conseguia mais atrair o interesse dos residentes da ilha como de outrora, mas persistia como objeto de fascinação do Oficial, encarregado de sua manutenção e inicialização. A afeição deste pelo aparelho concebido por seu antigo comandante constitui o mote do escrito, voltado a debater o afã punitivista da época — orquestrado, nos dias atuais, pela opressora utilização das novas tecnologias, em especial da inteligência artificial (IA).

De maneira curiosa, o deslumbramento do personagem se assemelha àquele dos entusiastas dos contemporâneos sistemas de reconhecimento facial, onipresentes em vias públicas, edifícios residenciais e empresariais, estabelecimentos comerciais, aeroportos, estádios de futebol e estações de metrô. Conforme ensina o *Artificial Intelligence Act (AI Act)* europeu, tido como a proposta de

[1] Apesar de o material original grifar os nomes dos personagens em letras minúsculas, o presente texto se serve de letras iniciais maiúsculas nas menções ao quarteto a fim de facilitar a compreensão do leitor.

Revista ARACÊ
ISSN: 2358-2472

regulamentação da área mais avançada no mundo, tais máquinas de observação à distância representam sistemas de IA voltados precipuamente à "identificação de pessoas singulares sem a sua participação ativa, normalmente à distância, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência" (art. 3º, nº 41) (União Europeia, 2024).

Tal como o aparato da colônia, essas soluções comportam uma série de perigos. A começar pela captura e o processamento não autorizados de dados pessoais sensíveis que são protegidos pela Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e pela Constituição Federal[2].

Conforme esclarece a Agência Nacional de Proteção de Dados (ANPD) no relatório "Radar Tecnológico nº 2: Biometria e Reconhecimento Facial", embora o inciso III, do art. 4º, da LGPD, exclua o tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais do escopo de aplicação da lei, as determinações previstas nos §§1º a 5º do dispositivo permanecem como de observância obrigatória (Cebrian, 2024, p. 8-9).

Nessas hipóteses, o tratamento se norteará por uma legislação própria, respeitado o devido processo legal e os princípios gerais e direitos do titular contidos na LGPD (§1º) e preservadas as vedações impostas por esta a pessoas jurídicas de direito privado (§§2 e 4º). O documento acima constitui, inclusive, um desdobramento da abertura conferida à ANPD para emitir opiniões e recomendações acerca dos citados cenários excepcionais (§3º) (Cebrian, 2024, p. 8-9). Portanto, independentemente de sua destinação pública ou privada, as soluções de reconhecimento facial devem se atentar ao diploma protetivo em questão.

Outra ameaça reside nos riscos de discriminação algorítmica, em que são (re)infligidos prejuízos a indivíduos ou grupos historicamente desprivilegiados, como as populações feminina, preta e LGBTQIAPN+. Na modalidade direta do instituto, os enviesamentos são perceptíveis, pois se baseiam na flagrante deturpação de atributos personalíssimos (*e.g.* raça, gênero, etnia, ideologia política, orientação religiosa, preferência sexual e/ou dados biométricos) ao longo do funcionamento do sistema de IA. Contudo, os principais obstáculos residem em sua forma indireta, cujos modelos se afiguram estatisticamente irretocáveis, mas acabam por esconder perigosas discriminações (França Netto; Ehrhardt Júnior, 2022).

[2] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Incluído pela Emenda Constitucional nº 115, de 2022)".

Revista ARACÊ
ISSN: 2358-2472

Já em suas linhas iniciais, o escrito ficcional sinaliza a submissão do Condenado, que "parecia entregue de forma tão canina que a impressão era a de que seria possível deixá-lo perambular livremente pelas encostas e bastaria assobiar no início da execução para que ele viesse" (Kafka, 2020, p. 17), à figura do Oficial. A sujeição irrestrita também se revela um produto dos modernos instrumentos de vigilância, capazes de silenciosamente fiscalizar multidões de pessoas ao mesmo tempo sob o pretexto de garantir a sua segurança, assim como das redes sociais, ambientes ideais ao emprego de técnicas furtivas pelas *big techs* com o intento de capturar e manter a atenção dos usuários.

Nas páginas seguintes, vê-se que o Oficial se comunica com o Viajante em francês — idioma estranho ao Condenado — para graficamente relatar o funcionamento da máquina, cujo desígnio consistia em gravar na pele dos apenados os mandamentos que haviam descumprido, configurando um processo automatizado de tortura que os levaria à morte. Atados de bruços a uma cama de algodão, eles seriam perfurados por agulhas fincadas a um rastelo, que gravariam em suas costas as figuras submetidas ao "desenhador" a partir de esboços confeccionados pelo antigo comandante[3].

A história retratava um "tribunal de um homem só", apenas composto pelo Oficial e desprovido de instâncias revisoras, em que vigorava o axioma de que "a culpa é sempre indubitável". O Condenado não tinha ciência de sua sentença ou da possibilidade de defesa, sendo encaminhado ao aparelho mortal pela prática do crime de desobediência ao (supostamente) falhar em prestar continência ao seu ex-capitão. Sujeito a um julgamento sumário, ele estava na iminência de ser marcado, literal e figurativamente, por um delito que talvez não houvesse cometido.

4 "NA COLÔNIA PENAL" DIGITAL: OS EQUÍVOCOS NA IDENTIFICAÇÃO DE PESSOAS POR MEIO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Estigmas parecidos são forjados pelo panoptismo das lentes de reconhecimento facial. Sob o investimento inicial de R$ 18 milhões, o Sistema de Videomonitoramento da Polícia Militar do Rio de Janeiro integrará ferramentas desse tipo às 21 câmeras do Centro de Operações do Rio (COR) em funcionamento no bairro da Lapa, "visando o aumento da sensação de segurança na população". Ao localizar pessoas com pendências judiciais, o aparato aciona a equipe policial nas proximidades para efetuar abordagens e, eventualmente, prisões (Lisboa, 2024) — porém, desde a sua inauguração no *réveillon* de 2023, a máquina vem ganhando notoriedade por consecutivos casos de erros de identificação.

[3] Uma representação visual da máquina de tortura fictícia idealizada por Kafka encontra-se disponível em: https://thefunambulistdotnet.wordpress.com/wp-content/uploads/2013/04/kafka_torture-machine640.jpg. Acesso em 20 ago. 2024.

Revista ARACÊ
ISSN: 2358-2472

Em janeiro de 2024, uma mulher foi detida após ser constatada a existência de mandado de prisão em aberto em seu nome. Após averiguação, a Polícia Civil percebeu que este já havia sido cumprido e que as penas restritivas de liberdade haviam sido substituídas por sanções restritivas de direitos na sua condenação em regime aberto (Coelho *et al.*, 2024). Outrossim, um argentino foi preso após a detecção de um mandado de prisão ativo pelo roubo de um supermercado. Na audiência de custódia, verificou-se que o alvará de soltura em relação ao delito havia sido previamente expedido (Saleme, 2024).

Os equívocos não se resumem ao cenário fluminense. Durante uma festa de prévia carnavalesca em Aracaju no final de 2022, uma jovem foi confundida com uma foragida da justiça pelo sistema de reconhecimento facial em operação, em dois momentos distintos. Na segunda abordagem, após exclamar que não havia cometido qualquer irregularidade, ela relata ter recebido a réplica "você sabe o que você fez, né?" de um dos policiais, em meio ao truculento tratamento que lhe foi dispendido[4]. Como diria o postulado verbalizado pelo Oficial kafkiano: a culpa é sempre indubitável.

O estado de Sergipe sediou outro infame incidente durante a final do campeonato local de futebol, realizada em abril de 2024, quando um torcedor foi erroneamente identificado pelo sistema de reconhecimento facial do estádio Arena Batistão. Após ser abordado pelos policiais em meio à multidão presente, o indivíduo foi conduzido pelo gramado com as mãos para trás e detido, sendo pressionado por um dos profissionais a "falar a verdade", pois, supostamente, existiria um mandado de prisão em aberto em seu nome. O episódio de constrangimento auferiu notoriedade e levou o governo estadual a suspender o uso da ferramenta (Medo, 2024).

As situações acima narradas revelam os perigos da disseminação de instrumentos de vigilância sem as devidas salvaguardas daqueles sob o seu escrutínio. Um dos principais obstáculos para se contestar decisões provenientes de sistemas inteligentes, sobretudo de modelos avançados baseados na arquitetura de redes neurais artificiais, reside na explicabilidade, ou seja, na capacidade de sua compreensão pelo público leigo.

Assim como o Viajante, que enfrentou dificuldades ao tentar entender os desenhos do antigo comandante que guiavam a máquina, e como o Condenado, alienígena ao idioma francês utilizado

[4] Ao reconstituir o episódio, a jovem relata que: "Mais tarde, umas 18h30m, quando já estavam acomodando o trio da Ivete Sangalo, passei ao lado de um carro da PM e alguns me abordaram de forma totalmente diferente. Não perguntaram nome, nem meu documento. Jogaram meu copo no chão, pegaram meu celular, prenderam minhas mãos para trás, segurando com bastante força. Eu dizia 'não fiz nada'. Um PM falou 'você sabe o que você fez, né?'. Neste momento, urinei. Me colocaram no camburão. Toda encolhida, coagida, todo mundo me olhando, eu pedindo para que alguém filmasse. Mas ninguém me ajudou. Me levaram até uma tenda, onde tinham outros policiais. Cheguei chorando, desesperada" (RIBEIRO, 2023).

Revista ARACÊ
ISSN: 2358-2472

pelo Oficial, o cidadão médio não auferirá êxito ao delinear os meandros de algoritmos mais complexos. Compostos por múltiplas camadas entre as suas barreiras de entrada (*input*) e saída (*output*), que realizam a captura de padrões a partir dos dados, estes permanecem como uma incógnita até para os seus próprios desenvolvedores[5].

5 AS LIÇÕES DE KAFKA AO VIGILANTISMO DO PRESENTE

Ao pregar pela continuidade da operação da máquina na colônia, o Oficial suavizou as suas intempéries ao aduzir que ela era "muito complicada, de vez em quando alguma coisa arrebenta ou quebra; mas não se pode deixar enganar e julgar errado o conjunto" (Kafka, 2020, p. 52). Defesas similares são trazidas pelos correligionários dos saltos tecnológicos modernos, que comumente desconsideram os inúmeros percalços intrínsecos a tais acontecimentos.

Na derradeira porção da obra literária, o personagem rememora com nostalgia das antigas execuções promovidas na ilha, que atraíam multidões de espectadores. Temeroso frente às mudanças para encerrar tal processo em declínio de popularidade, o Oficial busca desesperadamente o apoio do Viajante. Este, por sua vez, opõe-se ao cotidiano de violência da localidade e relata que comunicará a sua opinião ao novo comandante, conforme lhe fora solicitado.

A resignação simboliza o desfecho do conto, quando o Oficial declara a liberdade do Condenado — enfim se comunicando em seu idioma — e exibe uma folha de sua carteira para o Viajante em que parecia constar a inscrição "seja justo". Atento ao mandamento, o Oficial se direciona à máquina, insere tal gravura no "desenhador" e repousa sobre a cama, dando início a um auto procedimento de tortura.

Ao lado do Condenado e do Soldado, o Viajante percebe que as engrenagens da máquina começaram a se soltar e que o rastelo não mais escrevia sobre a pele do Oficial, mas sim o estocava seguidamente. Indo até as últimas consequências para preservar a sua ideologia belígera, este se torna o último produto do aparelho que tanto admirara, agora em ruínas, sem alcançar a redenção habitual a todos que o precederam.

O fatídico destino do personagem serve como uma advertência para aqueles que, de maneira incauta, defendem inovações tecnológicas eivadas por potenciais lesivos aos seus usuários e destinatários. A inversão de papéis entre o Oficial e o Condenado sinaliza como, eventualmente, os ofensores podem se converter em ofendidos.

[5] A principal distinção entre algoritmos simplificados de Aprendizado de Máquina (*Machine Learning*) e a sua forma evolutiva do Aprendizado Profundo (*Deep Learning*) jaz na existência de múltiplas camadas entre a entrada de dados e a saída de uma informação de interesse.

Revista ARACÊ
ISSN: 2358-2472

No neocolonialismo digital, grupos minoritários são subrepresentados e, não raro, algoritmicamente oprimidos. Examinar as causas fundantes da situação se torna, portanto, imprescindível.

6 NEOCOLONIALISMO DIGITAL E ENGRENAGENS DA DISCRIMINAÇÃO ALGORÍTMICA

Consoante leciona Alexandre Freire Pimentel (2023, p. 55-85), a subjugação tecnológica moderna se caracteriza pela ubiquidade, ao transcender as limitações geográficas estatais e resultar na "relocalização do poder" no âmbito do ciberespaço, e pela desnecessidade do exercício coercitivo sancionatório, à medida que as adesões se desenrolam de forma "pseudoespontânea" em meio ao cenário de neocolonização digital.

Principal aparato desta, o tecnopoder se traduz no controle do agir humano para fins variados (*e.g.* políticos, econômicos e sociais). A dominação panóptica da sociedade disciplinar, fundada no perene receio de estar sendo vigiado, aperfeiçoa-se na sociedade de controle digital, instaurando-se o monitoramento "real, constante e aquiescido" do cidadão-usuário, cuja renúncia ou relativização da privacidade simboliza o preço para se existir na conjuntura artificial contemporânea (Pimentel, 2023, p. 55-85).

Por sua vez, Byung-Chul Han (2022, p. 7-24) descreve a transição entre os regimes soberano, disciplinar e da informação, a partir do elemento da visibilidade. Enquanto o primeiro se destacava pela excessiva autopromoção dos dominadores por meio de manifestações teatrais de poder, o segundo direcionava os seus holofotes aos dominados, expostos a contragosto nas células componentes da estrutura prisional *benthiana*.

Intrínseco ao capitalismo de vigilância, o regime da informação se diferencia pela voluntariedade das pessoas em se sujeitarem ao escrutínio alheio, notadamente no antro das redes sociais, infestado pelo hiper compartilhamento dos acontecimentos cotidianos. O filósofo sul-coreano sublinha como, de maneira paradoxal, a pretensa sensação de liberdade atua, na verdade, como combustível para o domínio — agora exercido sobre a psique (psicopolítica) e infinitamente abastecido pelas comunicações virtuais (Han, 2022, p. 7-24).

Giselle Beiguelman (2023, p. 55-96) tece uma interessante perspectiva a respeito do monitoramento moderno a partir do elemento da imagem, cada vez mais fabricada por máquinas (*e.g. QR Codes*) ou pelos instrumentos que estas operam (*e.g.* satélites). O original paradoxo do olhar humano — segundo o qual fintamos quem nos enxerga em retorno — é substituído por um novo modelo, em que a leitura unilateralmente efetuada pelos algoritmos resulta das fotografias (e demais

Revista ARACÊ
ISSN: 2358-2472

informações) que compartilhamos, de forma que "os grandes olhos que nos monitoram veem pelos nossos olhos" (Beiguelman, 2023, p. 69).

Para além disso, a autora destaca como a biopolítica da dadosfera torna-se porosa, sutilmente adentrando nossos corpos por meio de sistemas de sensoriamento remoto, hábeis em capturar informações sem a necessidade de contato físico. Ao resgatar a noção de "imagens operacionais" cunhada pelo cineasta alemão Harun Farocki, que se fazem presentes, por exemplo, em câmeras térmicas mensuradoras da assinatura espectral das pessoas, ela ilustra o quão frágil a privacidade se configura diante da naturalização de tais ferramentas, cujos produtos se afiguram imperceptíveis e incompreensíveis ao arcabouço humano, mas são decifráveis pelos entes artificiais que assumem as rédeas dos processos de vigilância (Beiguelman, 2023, p. 55-96).

Deivison Faustino (2023, p. 184-190) e Walter Lippold acertadamente explicitam como o racismo, engendrador de colonizações pregressas e futuras, não é endereçado pelas análises de teóricos do colonialismo digital. Típica deste, a conversão de pessoas em mercadorias ao alvedrio das *big techs* ignora como tal elemento impacta o preço dos negros no *locus* digital, ainda tido como inferior.

Deste modo, sugerem a superação da popular expressão "racismo algorítmico", eximidora da responsabilidade dos programadores, pelo termo "racialização digital", que melhor reflete a conjuntura de concepção dos algoritmos, maculada por preterições de ordem racial no preenchimento de postos técnicos, na valorização dos criadores de conteúdo e na configuração de redes sociais e bancos de imagem. Dentre as nocivas materializações oriundas do fenômeno, situam-se as ferramentas de reconhecimento facial, cercadas por incongruências na identificação de pessoas negras (Faustino, 2023, p. 184-190).

Joy Buolamwini e Timnit Gebru (2018) descortinam as engrenagens dos mecanismos de análise facial automatizada para estudar a problemática da discriminação algorítmica. Ao performarem tarefas como a detecção, a classificação e o reconhecimento de rostos, esses sistemas de inteligência artificial podem produzir resultados enviesados quanto à raça e ao gênero, prejudiciais a grupos já historicamente desprivilegiados.

Imersos à ramificação do Aprendizado de Máquina (*Machine Learning - ML*), os seus algoritmos se destinam a encontrar padrões em meio a vultosas quantidades de dados, sem a necessidade de uma programação específica, a fim de originar um modelo que melhor conecte as informações de entrada (*input*) ao resultado de saída (*output*), subsidiando decisões, recomendações e previsões. Dentre as espécies de ML, as soluções de Aprendizado Supervisionado (*Supervised Learning*) se distinguem pela atribuição de rótulos (*labels*) aos dados de treinamento, que conferem atributos (*features*) aos objetos analisados (França Netto; Ehrhardt Júnior, 2022).

Revista ARACÊ
ISSN: 2358-2472

De início, as pesquisadoras observaram que rótulos de raça e etnia, utilizados para avaliar a existência de discriminações em certos tipos de dados, não se adequam ao exame de imagens visuais, diante da enorme variedade de atributos internos dessas categorias e das discrepâncias existentes entre países. Por conseguinte, elas optaram por utilizar uma rotulação interseccional baseada em dois atributos: a) o gênero, tido como masculino ou feminino; e b) o tipo de pele, à luz da escala dermatológica de Fitzpatrick, composta por seis gradações — três para tons de pele mais claros e três para tons de pele mais escuros[6].

Assim, a dupla selecionou os conjuntos de dados (*datasets*) IJB-A e Adience, tidos como importantes repositórios de fotografias de rostos para o treinamento de sistemas de IA, e manualmente identificou cada uma de suas imagens a partir dos dois fatores. Como resultado, verificou que os conjuntos de dados eram compostos, respectivamente, por 79,6% e 86,2% de indivíduos de pele mais clara, indicando a gritante sub-representação de pessoas de pele mais escura (Buolamwini; Gebru, 2018).

Sob uma classificação que conjuga os *features* em quatro categorias (homem mais escuro, homem mais claro, mulher mais escura e mulher mais clara)[7], observou-se a superrepresentação de homens mais claros nos dois *datasets* (59,4% no IJB-A e 44,6% no Adience) e a quase inexistência de mulheres mais escuras no IJB-A (4,4%) e de homens mais escuros no Adience (6,4%).

Em face desses flagrantes desequilíbrios, as cientistas formularam um referencial próprio, o Pilot Parliaments Benchmark (PPB), que compila imagens de parlamentares de três países africanos e de três países europeus[8], escolhidos pela maior facilidade em se encontrar fotos institucionais e pelo bom desempenho das nações em *rankings* de paridade de gênero em seus corpos legislativos. O PPB apresentou resultados promissores no que concerne à harmoniosa presença de pessoas mais claras (53,6%) e de pessoas mais escuras (46,4%) na amostra de dados, igualmente equilibrada em relação às categorias específicas — mulher mais escura (21,3%), homem mais escuro (25,1%), mulher mais clara (23,3%) e homem mais claro (30,3%) (Buolamwini; Gebru, 2018).

Ao final, três classificadores comerciais de gênero disponibilizados no mercado pelas empresas Microsoft, IBM e Face++ foram avaliados pelas pesquisadoras a partir da metodologia interseccional citada. Todos apresentaram taxas de erros mais elevadas para mulheres em comparação

[6] Como bem sublinham as pesquisadoras, as escolhas metodológicas utilizadas também se sujeitam a escrutínio, tendo em vista que a escala de Fitzpatrick não fielmente categoriza o tom sépia que caracteriza o resto do mundo e que a classificação binária de gênero exclui segmentos relevantes, como as pessoas não binárias e transexuais.
[7] Na tradução direta dos termos *darker male, lighter male, darker female e lighter female*, utilizados no texto original de Buolamwini e Gebru.
[8] Foram selecionados parlamentares de Ruanda, Senegal, África do Sul, Finlândia, Islândia e Suécia.

Revista ARACÊ
ISSN: 2358-2472

com homens e para pessoas mais escuras em comparação com as mais claras. Enquanto o grupo de mulheres mais escuras teve o pior desempenho, o de homens mais claros teve o melhor desempenho.

Caso irrefletidamente empregados, os sistemas de avaliação facial automatizada, sobretudo as ferramentas de reconhecimento de rostos no âmbito da segurança pública, podem se tornar Armas de Destruição Matemática (ADM) — *Weapons of Math Destruction (WMD)*, no original em inglês —, conforme alerta Cathy O'Neil (2020, p. 81-99), revestindo-se como versões digitalizadas da iniciativa analógica "parar-e-revistar".

Popularizada sob a lente de políticas de tolerância zero, esta incentiva a autoridade policial a realizar abordagens combativas a todas as modalidades de delito, o que, em tese, asseguraria a redução dos índices de criminalidade pela via do desestímulo. Assim como as soluções de policiamento preditivo (*e.g.* PredPol), que recorrem à IA para prever quais crimes tendem a ser cometidos em determinada localidade num certo horário, otimizando o direcionamento de seus contingentes de pessoal, esse tipo de prática se revela nocivo às populações negra e latina (O'Neil, 2020, p. 81-99).

Ambos se mostram pouco efetivos perante crimes de maior importância (*e.g.* homicídio e estupro), detendo maior aplicação frente àqueles de menor importância (*e.g.* porte de pequena quantidade de drogas e vadiagem), tidos como problemas endêmicos de bairros mais pobres. Quando sistemas como o PredPol são realimentados com dados de prisão dos citados grupos demográficos pela consumação dessas leves perturbações, produz-se um efeito de *looping* que direciona mais efetivos policiais para tais áreas, em busca de suspeitos com semelhantes características fenotípicas, num ciclo infinito de perseguição institucionalizada (O'Neil, 2020, p. 81-99).

A despeito das inúmeras advertências acerca dos perigos associados ao emprego de sistemas de reconhecimento facial nos domínios públicos, notadamente no que alude aos equívocos cometidos durante a identificação de cidadãos — que podem subsidiar detenções indevidas e violações a direitos humanos —, os projetos nacionais na área se encontram em franca expansão.

7 A CONTROVÉRSIA EM TORNO DA IMPLEMENTAÇÃO DE SISTEMAS DE RECONHECIMENTO FACIAL NO BRASIL

Concebida em 2019 pelo Centro de Estudos de Segurança e Cidadania (CESeC) integrado à Universidade Cândido Mendes (RJ), a iniciativa "O Panóptico" direciona as suas atenções para os projetos nacionais que empregam tecnologias de reconhecimento facial na segurança pública, compilando estatísticas e estudos acerca da temática. A sua mais recente apuração (atualizada em

Revista ARACÊ
ISSN: 2358-2472

27/01/2025) contabiliza 337 projetos ativos no país[9], distribuídos entre as regiões Norte (27), Nordeste (56), Sul (63), Sudeste (102) e Centro-Oeste (89), que somados atingem a expressiva marca de 81 milhões de pessoas potencialmente vigiadas[10].

Em seu relatório "Um Rio de olhos seletivos: uso de reconhecimento facial pela polícia fluminense", é possível observar a linha do tempo de tais aplicações no estado do Rio de Janeiro, inaugurada pelo projeto-piloto de videomonitoramento executado pela Secretaria de Estado de Polícia Militar (SEPM) em colaboração com a empresa Oi no ano de 2019, cuja cobertura abrangeu, a princípio, o bairro de Copacabana, posteriormente se estendendo às imediações do Maracanã e do aeroporto Santos Dumont (Nunes, 2022).

O simbolismo da escolha da área nobre como ponto de partida desnuda o intento subjacente de limar as populações periféricas de seus espaços por meio do gerenciamento da movimentação de pessoas. Durante a primeira fase do experimento, 2.993.692 faces foram captadas e 2.465 foram reconhecidas, totalizando a ínfima taxa de correlação de 0,082%. Já em sua segunda fase, no curso de um jogo de futebol, onze pessoas foram identificadas e detidas nos arredores do Maracanã, todavia, apenas quatro delas possuíam mandados de prisão em aberto, configurando uma taxa de erro de 63% (Nunes, 2022).

Apesar da reduzida eficiência de tais aparelhos, o projeto "Cidade Integrada" emergiu em 2022 com a finalidade de instalar 22 câmeras (4 com reconhecimento facial) na favela do Jacarezinho, situada na Zona Norte do Rio de Janeiro, motivando críticas pautadas na dispensa do procedimento licitatório e na elevada onerosidade ao orçamento público. O seu aspecto mais alarmante reside no destaque conferido pelo estudo técnico preliminar formulado à função do sistema de auxiliar na produção de provas ratificadoras dos relatos policiais em ações judiciais, contraposto pelo silêncio em relação à violência corriqueira nas operações realizadas em comunidades (Nunes, 2022).

Preocupações análogas lastrearam a carta aberta endereçada ao atual Prefeito do Recife, João Campos, pelo Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) em conjunto a diversas agremiações científicas, motivada pela promessa de instalação de 108 relógios digitais na cidade, que, além de funções básicas, como a aferição de temperatura e o acesso à conexão à *Internet* via *WI-FI*, contariam com câmeras de reconhecimento facial dos cidadãos (Carta, 2021).

[9] Do ponto de vista metodológico, são considerados como "projetos ativos" aqueles que se encontram em fase de licitação, teste, uso eventual ou uso regular, cujas etapas de planejamento e preparação se mostram em andamento ou concluídas, com as tecnologias de reconhecimento facial sendo implementadas como uma política pública de segurança. O cálculo da quantidade de pessoas potencialmente vigiadas se baseia nos índices populacionais dos municípios afetados por tais ferramentas à luz dos números disponibilizados no "Censo Demográfico 2022" pelo Instituto Brasileiro de Geografia e Estatística (IBGE) (METODOLOGIA, 2024).

[10] Os estados de Goiás e São Paulo lideram a lista, respectivamente, no que concerne à quantidade de projetos ativos (72) e de pessoas potencialmente vigiadas (18,6 milhões).

Revista ARACÊ
ISSN: 2358-2472

Nela, sugeriu-se o alinhamento aos posicionamentos internacionais favoráveis ao banimento da tecnologia, sublinhando-se como aspectos problemáticos: a) a inadequação da medida frente às determinações da LGPD, sobretudo no que concerne ao apontamento da base legal do tratamento e das medidas de mitigação de danos; b) a ausência de menção a diretrizes de segurança; c) as potenciais violações à privacidade e a direitos civis, como as liberdades de reunião e de manifestação; d) os enviesamentos algorítmicos, passíveis de produzir resultados lesivos a pessoas pretas e pardas; e) a insegurança jurídica, que ensejou a suspensão judicial de editais de licitação na área no Brasil; e a f) questionável confluência de interesses públicos e privados. Ainda assim, a Prefeitura do Recife seguiu com a instalação dos equipamentos no ano de 2022 (Recife, 2022).

A busca por remédios tecnológicos capazes de sanar as mazelas da segurança pública também permeou as ações governamentais do estado do Ceará nas últimas décadas, desde a concepção do programa "Ronda do Quarteirão" (2005), marcado pelo acoplamento de câmeras a viaturas, passando pelo videomonitoramento em eventos esportivos de renome, como a Copa das Confederações (2013) e a Copa do Mundo (2014), até a criação do *app* "Portal de Comando Avançado" (2019), que viabiliza o reconhecimento facial através do aparelho celular de policiais, e a solidificação do *big data* informacional do segmento, nomeado "Odin", e de seu painel analítico, o "Cerebrum" (Martins *et al.*, 2024).

Com investimentos vultosos que ultrapassam a marca de meio bilhão de reais — em boa parte destinada a uma empresa brasileira (IPQ Tecnologia Ltda), com laços junto a uma corporação chinesa (Dahua Technology) —, a estrutura de vigilância arquitetada em solo cearense é caraterizada por um opaco emaranhado de interesses públicos e privados, cujos nós adicionais advém da participação da comunidade acadêmica local (Martins *et al.*, 2024).

Mais de 3,6 mil câmeras mantidas pelo governo estadual e de 4,5 mil câmeras sob o crivo da administração municipal de Fortaleza encontram-se em funcionamento (Martins, 2024). Vale lembrar que, no início de 2022, a capital atraiu a atenção nacional de maneira indesejada quando a Polícia Civil catalogou a imagem do astro de *Hollywood* Michael B. Jordan, que é afro-americano, para fins de reconhecimento fotográfico como um dos suspeitos de uma chacina que deixou cinco mortos (Foto, 2022).

As potenciais discriminações resultantes da utilização de sistemas automatizados de reconhecimento facial também circundam o elemento do gênero, afetando a população transexual ao resultarem na errônea identificação deste ou no não-reconhecimento da pessoa após procedimentos de transição. Sujeito a habituais modificações corporais, tal demográfico não se mostra representado de forma satisfatória por métricas algorítmicas treinadas para identificar rostos alegadamente masculinos

Revista ARACÊ
ISSN: 2358-2472

e femininos, o que pode contribuir para classificações discriminatórias, obstruções do acesso a determinados espaços públicos (*e.g.* vestiários e banheiros) e violações ao direito à identidade (Silva, 2021).

Como bem aponta Heloísa Silva (2021), a consolidação deste perpassa o reconhecimento pelos demais, muitas vezes preterido em função da passabilidade transexual no cotidiano. Num cenário de escassez de pesquisas voltadas a esse recorte populacional, ampliador de sua invisibilização e do esmaecimento das cobranças em torno dos problemas acima, é preciso entender que

> as tecnologias de vigilância são passíveis de serem instrumentalizadas para (a) reprodução de estruturas de poder consolidadas, calcadas em normativas sobre corpo, gênero, sexualidade e outras expressões de identidade, que identificam, rastreiam e excluem determinados segmentos como ameaças (SILVA, 2021, p. 57).

Na ausência de disciplinamentos específicos que resguardem os grupos afetados por tais aplicações de IA, convém investigar as propostas para a sua regulamentação no Brasil e em sua maior inspiração legislativa quanto à matéria, a União Europeia.

8 O RECONHECIMENTO FACIAL SOB A PERSPECTIVA DO PROJETO DE LEI Nº 2.338/2023 E DO *ARTIFICIAL INTELLIGENCE ACT (AI ACT)*

Concebido como o futuro marco legal da inteligência artificial no Brasil, o Projeto de Lei nº 2.338/2023 (Brasil, 2024) conquistou avanços significativos em sua tramitação no dia 10 de dezembro de 2024, quando, após um intenso período de enfrentamento ao *lobby* das *big techs*, foi aprovado pelo Senado Federal. Desde a sua versão original, o texto normativo adota uma abordagem dúplice na regulamentação dessa tecnologia, que se destina a classificar as suas utilizações à luz dos riscos que carregam (*risk-based approach*) e a assegurar uma série de direitos às pessoas por ela afetadas (*rights-based approach*) (Nunes, 2023).

Destarte, o documento faculta aos agentes de IA (desenvolvedores, distribuidores e aplicadores)[11] a realização de avaliações preliminares (art. 12) para a catalogação de seus respectivos sistemas como de risco excessivo (art. 13) ou alto risco (art. 14), caso performem alguma das finalidades listadas, ou, residualmente, como de risco baixo ou moderado.

A categoria de risco excessivo coíbe o desenvolvimento, a implementação e o uso de sistemas que afetem pessoas naturais ou grupos com o escopo de: a) instigar ou induzir o seu comportamento, resultando em danos à saúde, à segurança ou a outros direitos fundamentais próprios ou de terceiros;

[11] A efetuação de avaliação preliminar apenas é obrigatória para os desenvolvedores de sistemas de IA de propósito geral ou generativa (art. 29).

Revista ARACÊ
ISSN: 2358-2472

b) explorar quaisquer de suas vulnerabilidades, com semelhantes propósitos; c) avaliar os seus traços de personalidade, características ou comportamentos pretéritos, criminais ou não, para avaliar o risco da prática de crimes, infrações ou reincidência; e d) viabilizar a produção ou disseminação, ou facilitar a geração de materiais que ilustrem o abuso ou exploração sexual de crianças e adolescentes (art. 13, I, alíneas a, b, c e d).

Somam-se às hipóteses proibitivas: a) as aplicações da tecnologia pelo poder público para avaliar, classificar ou ranquear indivíduos, a partir de seus comportamentos sociais ou atributos da personalidade, por meio de um *score* universal, condicionante do acesso a bens e serviços e a políticas públicas, de maneira ilegítima ou desproporcional (art. 13, II); b) os sistemas de armas autônomas (SAA) (art. 13, III); e c) os sistemas de identificação biométrica à distância, em tempo real e em espaços acessíveis ao público (art. 13, IV).

Tidas como o objeto central do presente artigo científico sob a roupagem da segurança pública, estas ferramentas de monitoramento apenas têm a sua implementação autorizada em quatro cenários (art. 13, IV, alíneas a, b, c e d):

> Art. 13. São vedados o desenvolvimento, a implementação e o uso de sistemas de IA: [...]
> IV – em sistemas de identificação biométrica à distância, em tempo real e em espaços acessíveis ao público, com exceção das seguintes hipóteses:
> a) instrução de inquérito ou processo criminal, mediante autorização judicial prévia e motivada, quando houver indícios razoáveis da autoria ou participação em infração penal, a prova não puder ser feita por outros meios disponíveis e o fato investigado não constituir infração penal de menor potencial ofensivo;
> b) busca de vítimas de crimes e de pessoas desaparecidas, ou em circunstâncias que envolvam ameaça grave e iminente à vida ou à integridade física de pessoas naturais;
> c) flagrante delito de crimes punidos com pena privativa de liberdade superior a 2 (dois) anos, com imediata comunicação à autoridade judicial;
> d) recaptura de réus evadidos e cumprimento de mandados de prisão e de medidas restritivas ordenadas pelo Poder Judiciário.

O PL leciona que estas permissões deverão ser proporcionais e estritamente necessárias ao atendimento do interesse público, resguardados o devido processo legal, o controle judicial e os princípios e direitos enumerados em suas disposições, e, no que competir, os ditames da Lei Geral de Proteção de Dados Pessoais (LGPD), sobretudo no que concerne ao combate à discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável (art. 13, §2º).

Por sua vez, a classificação de alto risco abrange uma dúzia de designações e contextos de usos admitidos para o invento (art. 14), que reclamarão medidas de governança adicionais (art. 18) e a elaboração de uma avaliação de impacto algorítmico (art. 25) pelo desenvolvedor e/ou aplicador que

Revista ARACÊ
ISSN: 2358-2472

introduza ou coloque em circulação no mercado o sistema inteligente[12]. Dentre as hipóteses, figura o emprego de aparatos de identificação e autenticação biométrica para o reconhecimento de emoções (art. 12, XI), ressalvados aqueles dotados do propósito exclusivo de confirmar uma pessoa singular específica.

As pessoas impactadas por instrumentos de vigilância no domínio da segurança pública podem enfrentar dificuldades ao exercitarem os direitos enumerados pelo projeto de lei. A falta de transparência na implementação da IA desperta preocupações quanto ao desvirtuamento de preceitos alusivos à informação acerca das interações com tais sistemas (art. 5º, I) e à explicação a respeito das decisões, recomendações ou previsões por eles tomadas (art. 6º, I).

Como resultado, a inobservância de ambos tem o condão de afetar a contestação e o pedido de revisão do desfecho ofertado pelo algoritmo (art. 6º, II), igualmente ameaçados pela complexidade inerente à sua arquitetura. Não obstante a participação do ser humano no processo decisório tenha sido preservada, os diversos episódios de "falsos positivos" até aqui narrados evidenciam a insuficiência da supervisão exercida sobre a máquina, o que pode prejudicar a proteção frente à discriminação de ordem direta e indireta (art. 5º, III).

A despeito dos alertas de especialistas pontuando a inviabilidade das soluções de identificação de rostos em face de seus reduzidos índices de acerto e dos elevados custos para a sua contratação, a proposta normativa optou por seguir caminho distinto ao banimento.

Tido como inspiração central do PL nº 2.338/2023, o *Artificial Intelligence Act* (*AI Act*) (União Europeia, 2024) inaugurou a regulamentação da inteligência artificial no mundo. Já em seu Considerando nº 17, o *AI Act* estabelece uma dúplice classificação para os sistemas de identificação biométrica à distância, que podem operar: a) "em tempo real", quando as etapas de captura de dados biométricos, comparação perante a base de dados referencial e identificação ocorrerem de maneira instantânea, quase instantânea ou sem atrasos relevantes; e b) "em diferido", caracterizados pela existência de um intervalo temporal considerável entre a captura e as ulteriores etapas de comparação e identificação.

Nos sistemas "em tempo real", o uso dos materiais coletados (*e.g.* imagens ou vídeos de câmeras) ocorre "ao vivo" ou "quase ao vivo". Já nos sistemas "em diferido", o conteúdo a ser analisado é previamente capturado, por exemplo, a partir de "câmeras de televisão em circuito fechado ou dispositivos privados".

[12] Enquanto as medidas de governança adicionais devem ser tomadas, conjuntamente, pelo desenvolvedor e pelo aplicador de um sistema de IA (art. 18), a avaliação de impacto algorítmico deve ser produzida, alternativamente, por um ou pelo outro (art. 25).

Revista ARACÊ
ISSN: 2358-2472

Como bem destaca o legislador europeu, as espécies acima não se confundem com as tecnologias de verificação biométrica, que habitualmente se servem do reconhecimento facial para fins de autenticação (*e.g.* atestar que as pessoas que tentam acessar um serviço são realmente quem alegam), diante de seu menor potencial lesivo perante direitos fundamentais individuais e da participação ativa dos sujeitos que são identificados ao longo desse processo.

A última versão da proposta em comento qualifica o emprego de sistemas de identificação biométrica à distância "em tempo real" e em espaços acessíveis ao público para efeitos de aplicação da lei como uma prática de inteligência artificial proibida[13], apenas autorizada para a indispensável consecução de três fins específicos.

> Art. 5º Práticas de IA proibidas
> 1. Estão proibidas as seguintes práticas de IA: [...]
> h) A utilização de sistemas de identificação biométrica à distância em "tempo real" em espaços acessíveis ao público para efeitos de aplicação da lei, a menos e na medida em que essa utilização seja estritamente necessária para um dos seguintes fins:
> i) busca seletiva de vítimas específicas de rapto, tráfico de seres humanos ou exploração sexual de seres humanos, bem como a busca por pessoas desaparecidas;
> ii) prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e atual ou real e previsível de um ataque terrorista;
> iii) a localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal, para efeitos da realização de uma investigação criminal, ou instauração de ação penal ou execução de uma sanção penal por alguma das infrações referidas no anexo II e puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos.
> A alínea h) do primeiro parágrafo não prejudica o disposto no artigo 9.º do Regulamento (UE) 2016/679 no que respeita ao tratamento de dados biométricos para outros fins que não a aplicação da lei.

O disciplinamento do Velho Continente se sobressai ao enumerar as espécies de delitos que ensejam a busca de vítimas, ao acrescer os cenários de ameaças a pessoas singulares e de articulações terroristas ao rol de usos autorizados da ferramenta, e ao fixar que a localização ou identificação de

[13] As razões motivadoras da proibição são listadas com uma clareza ímpar pelo Considerando nº 32 do documento: "A utilização de sistemas de IA para a identificação biométrica à distância "em tempo real" de pessoas singulares em espaços acessíveis ao público para efeitos de aplicação da lei é **particularmente intrusiva para os direitos e as liberdades das pessoas em causa, visto que pode afetar a vida privada de uma grande parte da população, dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais**. As imprecisões técnicas dos sistemas de IA concebidos para a identificação biométrica à distância de pessoas singulares podem conduzir a **resultados enviesados e ter efeitos discriminatórios**. Estes possíveis resultados enviesados e efeitos discriminatórios são particularmente relevantes no que diz respeito à idade, etnia, raça, sexo ou deficiência. Além disso, o impacto imediato e as oportunidades limitadas para a realização de controles adicionais ou correções no que respeita à utilização desses sistemas que funcionam em tempo real acarretam riscos acrescidos para os direitos e as liberdades das pessoas em causa no contexto, ou afetadas, pelas autoridades responsáveis pela aplicação da lei." (grifos nossos).

Revista ARACÊ
ISSN: 2358-2472

suspeitos tangencia delitos sancionáveis com penas não inferiores a quatro anos no Estado-Membro afetado[14].

Segundo o seu Considerando nº 33, as utilizações estritamente necessárias se baseiam em um "interesse público importante" que supere os riscos eventualmente existentes. Nessas hipóteses taxativas, além do escopo de confirmação da identidade do indivíduo visado, deverá ocorrer a ponderação acerca da natureza da situação ensejadora do uso do sistema e das consequências dele provenientes para os direitos e liberdades de todas as pessoas afetadas (art. 5º, nº 2, alíneas "a" e "b").

Cada emprego dos sistemas de biometria com fins de aplicação da lei[15] não prescinde da autorização prévia de autoridade judiciária ou administrativa independente — apenas dispensada em cenários de urgência justificada, desde que seja posteriormente solicitada no prazo de 24 horas —, que deve evidenciar que aquele se mostrou necessário e proporcional para o atingimento de um dos fins mencionados e que "se limita ao estritamente necessário no que diz respeito ao período de tempo e ao âmbito geográfico e pessoal" (art. 5º, nº 3).

Todo uso deve ser notificado às autoridades nacionais de fiscalização de mercado e de proteção de dados, encarregadas de elaborar relatórios anuais a serem endereçados à Comissão Europeia, que compilará e publicará essas produções, não incluindo dados operacionais sensíveis sobre as atividades de aplicação da lei nelas (art. 5º, nº 4 a 7).

Iniciada a vigência do diploma europeu, resta saber se, nas futuras votações do PL nº 2.338/2023, será importado o esmero no disciplinamento da IA — em especial quanto aos sistemas de reconhecimento facial, que são detalhadamente regulamentados —, garantida a observância das peculiaridades nacionais na aplicação da disruptiva tecnologia.

9 CONCLUSÃO

A recente expansão dos sistemas de reconhecimento facial no Brasil, sobretudo das soluções de identificação biométrica à distância no âmbito da segurança pública, gera justificadas preocupações atreladas à sua potencialidade lesiva em relação a indivíduos ou grupos historicamente desfavorecidos, como pessoas negras, mulheres e transgêneros. Subrepresentados nos conjuntos de dados usados

[14] Também merece destaque a importante vedação a soluções inteligentes que originem ou ampliem bases de dados de reconhecimento facial através do recolhimento aleatório de imagens de rostos da *Internet* ou de circuitos fechados de televisão (art. 5º, alínea e).

[15] Cada Estado-Membro poderá fixar autorizações totais ou parciais para a utilização dos sistemas de identificação biométrica à distância "em tempo real" e em espaços acessíveis ao público para fins de aplicação da lei, observadas as delimitações do art. 5º, nº 1 (alínea "h"), 2 e 3. Permite-se, inclusive, que as legislações nacionais prevejam normas mais restritivas em relação à matéria (art. 5º, nº 5).

Revista ARACÊ
ISSN: 2358-2472

durante a aprendizagem dos algoritmos, esses segmentos se tornam alvo de erros das máquinas que podem resultar em detenções indevidas e em gravosas violações a direitos humanos.

Desafortunadamente esquecidos durante o treinamento desses aparatos inteligentes, os indivíduos que integram tais coletividades apenas são lembrados durante a sua questionável aplicação, não raro acometida por reduzidas taxas de correlação, conforme ilustram as experiências fluminenses de videomonitoramento no bairro de Copacabana. Acrescente-se a isso a possibilidade de permanecerem em *loops* de punibilidade, à medida que se tornam os principais destinatários de consecutivos sistemas de IA (*e.g.* dados de um jovem negro detido pela prática de um delito leve sendo realimentandos num sistema de predição de reincidência), tal como elucida Cathy O'Neil.

O conto "Na Colônia Penal", de Franz Kafka, atua como um interessante paralelo para essas peculiares máquinas digitais, as quais, tal como o aparelho de tortura da ilha, apresentam um funcionamento obscuro, capaz de gerar sancionamentos desproporcionais ou descabidos, enfrentando a crescente resistência de institutos de pesquisa cientes de seus possíveis prejuízos (*e.g.* altos custos, discriminações algorítmicas, ausência de lisura nas relações público-privadas e vazamentos de dados sensíveis).

Cabe aos estudiosos da temática, factualmente elevados ao posto do Viajante, explorar os meandros dessa inóspita colônia digital, caracterizada por uma vigilância ininterrupta que se torna viável pela concessão pseudoespontânea de dados pelos usuários, agora convertidos em mercadorias — mas com preços distintos para os cidadãos negros, como bem lembram Deivison Faustino e Walter Lippold.

Apesar de o avançado regramento europeu em torno da inteligência artificial não ter adotado o caminho do banimento das tecnologias de reconhecimento facial à distância e em espaços públicos para fins de aplicação da lei, o documento se sobressai por detalhadamente esclarecer quais são os seus usos permitidos e proibidos e categorizar com clareza as diversas ferramentas de análise existentes.

Nos futuros debates na Câmara dos Deputados destinados a otimizar a vigente redação do PL nº 2.338/2023, reflexões acerca dos aspectos positivos da proposta estrangeira e das potenciais facetas negativas das ferramentas de vigilância se fazem indispensáveis.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

BEIGUELMAN, Giselle. **Políticas da imagem**: Vigilância e resistência na dadosfera. 2. ed. São Paulo: Ubu Editora, 2023.

BRASIL. **Projeto de Lei nº 2.338**, de 10 de dezembro de 2024. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9881643&ts=1735605226813&disposition=inline. Acesso em: 28 jan. 2025.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades**: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency. Proceedings of Machine Learning Research 81:1–15, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 14 fev. 2024.

CARTA Aberta: Política de reconhecimento facial da PCR ameaça direitos de todos os cidadãos e cidadãs. **IP.rec**, Recife, 18 nov. 2021. Disponível em: https://ip.rec.br/blog/carta-aberta-politica-de-reconhecimento-facial-da-pcr-ameaca-direitos-de-todos-os-cidadaos-e-cidadas/. Acesso em: 15 fev. 2024.

CEBRIAN, Fabiana S. P. Faraco *et al.* **Radar Tecnológico nº 2**: Biometria e Reconhecimento Facial. ANPD: Brasília/DF, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/radar-tecnologico-biometria-anpd-1.pdf. Acesso em: 20 ago. 2024.

COELHO, Henrique; NASCIMENTO, Rafael; ALVES, Raoni. Mulher presa após reconhecimento facial é solta; mandado de prisão já tinha sido cumprido. **G1**, Rio de Janeiro, 4 jan. 2024. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/01/04/mulher-presa-apos-reconhecimento-facial-e-solta-mandado-de-prisao-ja-tinha-sido-cumprido.ghtml. Acesso em: 12 jan. 2024.

FAUSTINO, Deivison. **Colonialismo digital** [recurso eletrônico]: por uma crítica hacker-fanoniana / Deivison Faustino, Walter Lippold. 1. ed. São Paulo: Boitempo, 2023.

FOTO de astro do cinema Michael B. Jordan aparece em lista de procurados pela polícia do Ceará. **G1 CE**, [*S.l.*], 7 jan. 2022. Disponível em: https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml. Acesso em: 22 ago. 2024.

FRANÇA NETTO, Milton Pereira de; EHRHARDT JR., Marcos. **Os Riscos da Discriminação Algorítmica na Utilização de Aplicações de Inteligência Artificial no Cenário Brasileiro**. Revista Jurídica Luso-Brasileira, v. 3, 2022. Disponível em: https://www.cidp.pt/revistas/rjlb/2022/3/2022_03_1271_1318.pdf. Acesso em: 14 fev. 2024.

HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Petrópolis, RJ: Vozes, 2022.

KAFKA, Franz. **Na Colônia Penal** - ilustrações de Lourenço Mutarelli; tradução de Petê Rissatti. Rio de Janeiro: Editora Antofágica, 2020, p. 27.

LISBOA, Vinícius. Câmeras da Prefeitura do Rio na Lapa terão reconhecimento facial. **Agência Brasil**, Rio de Janeiro, 19 jan. 2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2

Revista ARACÊ
ISSN: 2358-2472

024-01/cameras-da-prefeitura-do-rio-na-lapa-terao-reconhecimento-facial#:~:text=O%20sistema%20de%20videomonitoramento%20da,milh%C3%B5es%2C%20entre%20equipamentos%20e%20softwares. Acesso em: 20 jan. 2024.

MARTINS, Helena. A adoção de tecnologias vigilantistas sem debate. **O Povo**, Fortaleza, 16 abr. 2024. Disponível em: https://mais.opovo.com.br/jornal/opiniao/2024/04/16/helena-martins-a-adocao-de-tecnologias-vigilantistas-sem-debate.html. Acesso em: 18 ago. 2024.

MARTINS, Helena *et al.* **Da construção de uma infraestrutura de vigilância à introdução do reconhecimento facial no Ceará** [livro eletrônico]. Rio de Janeiro : CESeC, 2024. Disponível em: https://drive.google.com/file/d/1sVRHIIdEVbFMDvaqkPpW29hdv3eTSEYc/view. Acesso em: 19 ago. 2024.

'MEDO, frustrado e constrangido', diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. **G1**, [*S.l.*], 21 abr. 2024. Disponível em: https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml. Acesso em: 22 ago. 2024.

METODOLOGIA de monitoramento. **O Panóptico**, [*S.l.*], 2024. Disponível em: https://docs.google.com/document/d/1CM4P68Npyr6zR2myvjo1ulqJtpdoqOuPam8TiFah7yI/edit. Acesso em: 14 fev. 2024.

NUNES, Dierle. Regulação da inteligência artificial e uso de técnicas subliminares. **Conjur**, [*S.l.*], 26 set. 2023. Disponível em: https://www.conjur.com.br/2023-set-26/dierle-nunes-regulacao-ia-uso-tecnicas-subliminares/. Acesso em: 14 fev. 2024.

NUNES, Pablo. **Um Rio de olhos seletivos** [livro eletrônico]: uso de reconhecimento facial pela polícia fluminense. Rio de Janeiro : CESeC, 2022.

O'NEIL, Cathy. **Algoritmos de destruição em massa** : como o big data aumenta a desigualdade e ameaça à democracia / Cathy O'Neil ; tradução Rafael Abraham. -- 1. ed. -- Santo André, SP : Editora Rua do Sabão, 2020.

PIMENTEL, Alexandre Freire. **Tratado de Direito e Processo Tecnológico** – (Vol. 01) – Vigilância Algorítmica e Neocolonização; O Controle Digital das Massas e Riscos e Atentados à Democracia (Incluindo o episódio do dia 08 de janeiro de 2023). Editora Publius: Recife, 2023.

RECIFE ganha a o primeiro de 108 relógios digitais. **Prefeitura do Recife**, Recife, 18 nov. 2022. Disponível em: https://www2.recife.pe.gov.br/noticias/29/12/2022/recife-ganha-o-primeiro-de-108-relogios-eletronicos-digitais. Acesso em: 15 fev. 2024.

RIBEIRO, Aline. Vivi para contar: 'Me confundiram duas vezes com uma foragida na mesma festa', diz jovem alvo de reconhecimento facial. **O Globo**, São Paulo, 5 jan. 2023. Disponível em: https://oglobo.globo.com/brasil/noticia/2024/01/05/vivi-para-contar-me-confundiram-duas-vezes-com-uma-foragida-na-mesma-festa-diz-jovem-alvo-de-reconhecimento-facial.ghtml. Acesso em: 12 jan. 2024.

Revista ARACÊ
ISSN: 2358-2472

SALEME, Isabelle. Dois dos quatro presos por reconhecimento facial no Rio de Janeiro são liberados. **CNN Brasil**, [*S.l.*], 5 jan. 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/dois-dos-quatro-presos-por-reconhecimento-facial-no-rio-de-janeiro-sao-liberados/. Acesso em: 12 jan. 2024.

SILVA, Heloísa Helena. Algoritmos de reconhecimento facial e as discriminações contra pessoas transexuais. **Revista Internet e Sociedade**, v. 2, n.2, dez/2021, p. 47-66. Disponível em: https://revista.internetlab.org.br/wp-content/uploads/2022/03/Algoritmos-de-reconhecimento-facial-e-as-discriminacoes-contra-pessoas-transexuais.pdf. Acesso em: 14 fev. 2024.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho**, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). Bruxelas, 13 jun. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689. Acesso em: 22 ago. 2024.