

O RECONHECIMENTO FACIAL COMO INSTRUMENTO DE REFORÇO DO ESTADO DE COISAS INCONSTITUCIONAIS NO BRASIL

*Alisson Possa*⁵⁷

RESUMO: O presente artigo busca demonstrar a possível relação de aprofundamento do Estado de Coisas Inconstitucional do sistema carcerário brasileiro através da adoção de algoritmos de reconhecimento facial para fins de segurança pública. Através de uma análise dos pressupostos reconhecidos pelo Supremo Tribunal Federal na ADPF 347 e dos indícios de existência de viés racial nos algoritmos de reconhecimento facial amplamente divulgadas pela mídia e em estudos recentes, será estudada a hipótese de que a utilização de sistemas com essa tecnologia acaba por agravar a situação reconhecida na decisão.

Palavras-chave: Estado de Coisa Inconstitucional. Sistema carcerário brasileiro. Reconhecimento facial. Segurança Pública. Discriminação algorítmica.

ABSTRACT: This article seeks to demonstrate the possible relationship of deepening the Unconstitutional State of Things in the Brazilian prison system through the adoption of facial recognition algorithms for public security purposes. Through an analysis of the assumptions made by the Federal Supreme Court in ADPF 347 and the evidence of the existence of racial bias in the facial recognition algorithms, the hypothesis studied will be that the use of systems with this technology ends up aggravating the situation recognized in the decision.

Keywords: Unconstitutional State of Thing. Brazilian prison system. Facial recognition. Public security. Algorithmic discrimination.

INTRODUÇÃO

As inovações tecnológicas que ocorrem no mundo estão trazendo ao Brasil novas possibilidades para soluções de problemas antigos. Um exemplo é a ideia de que a solução de muitos dos problemas do setor público brasileiro é a adoção de novas tecnologias. Entretanto, na área de combate ao crime e investigações criminais, o uso de algoritmos para combater os níveis elevados de violência do país podem aprofundar mais ainda problemas estruturais da sociedade.

O presente artigo propõe uma análise sobre a adoção de tecnologias de reconhecimento facial para investigações criminais e/ou solução para a diminuição dos índices de violência do país, e os possíveis riscos para direitos fundamentais em escala massificada dentro da realidade carcerária brasileira.

A adoção de tecnologias de reconhecimento facial em áreas públicas, principalmente por forças policiais, vem sendo alvo de críticas e exposição de abusos no mundo inteiro. Problemas envolvendo vieses raciais, acurácia de identificações para minorias étnicas e abusos repressivos do Estado são as principais críticas já

⁵⁷ Mestrando no IDP. E-mail: alisson.possa@gmail.com

comprovadas⁵⁸ por pesquisas. No Brasil, a adoção dessas tecnologias está tomando força nos últimos anos pelas forças policiais⁵⁹, mesmo com os problemas sendo expostos cotidianamente por entidades de defesas de direitos humanos.

O escopo desse trabalho é uma análise sobre a relação entre os problemas decorrentes dos vieses raciais e étnicos das tecnologias de reconhecimento facial e o Estado de Coisas Inconstitucional do problema carcerário brasileiro nas violações de direitos humanos, principalmente no que diz respeito à presunção de inocência e ao direito à igualdade de pessoas negras. Também será analisado o efeito de regulações em proteção de dados e inteligência artificial no Brasil afetam a utilização dessas tecnologias no âmbito persecutório.

Para tanto, a pergunta que o trabalho busca responder é: de que forma as tecnologias de reconhecimento facial trazem um novo elemento de aprofundamento do Estado de Coisas Institucional na realidade carcerária brasileira?

A hipótese trabalhada é que as tecnologias de reconhecimento facial podem reforçar o Estado de Coisas Inconstitucional no sistema prisional brasileiro, notadamente a o racismo existente, através do viés racial reproduzido algoritmicamente.

Para solucionar o problema proposto, a metodologia utilizada é predominantemente bibliográfica e documental através de pesquisa jurisprudencial, doutrinária e jornalística.

O marco teórico utilizado foi a decisão do Supremo Tribunal Federal que reconheceu o Estado de Coisas Inconstitucional no sistema carcerário brasileiro com enfoque nos problemas envolvendo as violações de direitos de minorias e presunção inocência.

Inicialmente é analisada a decisão do Supremo Tribunal Federal acima citada sendo identificado os elementos caracterizados de uma situação em estado de coisas inconstitucional.

Em seguida, será exposto como as tecnologias de reconhecimento facial possuem viés racial, seja por erros de reconhecimento, seja por serem frutos de um racismo estrutural da sociedade, e acabam por ser mais um meio de violação de direitos fundamentais de populações negras.

Também serão analisadas as possíveis consequências das novas regulações de

⁵⁸ Uma pesquisa da Georgetown Law School em 2016 indicou vieses raciais em algoritmos de reconhecimento facial utilizados por forças policiais nos Estados Unidos. Disponível em: <https://www.theguardian.com/technology/2016/apr/08/facial-recognition-technology-racial-bias-police>. Acesso em: 25 jun. 2021.

⁵⁹ No dia 28/01 foi inaugurado o Laboratório de Identificação Biométrica – Facial e Digital em São Paulo para auxiliar a polícia do estado em investigações criminais. Disponível em: <https://www.conjur.com.br/2020-jan-29/policia-paulista-usara-reconhecimento-facial-investigacoes>. Acesso em: 25 jun. 2021.

Inteligência Artificial e Proteção de Dados Pessoais que estão despontando em vários países no mundo e no Brasil na análise dos sistemas de reconhecimento facial e seus efeitos em direitos fundamentais na realidade brasileira.

Por fim, será estabelecida a relação entre as tecnologias de reconhecimento facial e o Estado de Coisas Inconstitucional no sistema carcerário brasileiro sendo demonstrado o preenchimento dos três requisitos identificados pelo Supremo Tribunal Federal para a caracterização da figura.

1 – O ESTADO DE COISAS INCONSTITUCIONAL NO BRASIL

O Estado de Coisas Inconstitucional é uma figura de violação permanente de direitos fundamentais, inicialmente desenvolvido pela Suprema Corte Colombiana⁶⁰ em 1997. As violações possuem três elementos em comum, conforme Machado (2020, p. 631-664) (i) são “o resultado de uma causa estrutural ou histórica” que (ii) “não pode ser atribuída a um único ente mas ao Estado em seu conjunto” e que (iii) “exige a adoção de medidas de longo prazo”.

No Brasil, a figura foi reconhecida pelo Supremo Tribunal Federal no julgamento da medida liminar da ADPF 347 em 2015 no sistema carcerário brasileiro.

O ponto de partida para o reconhecimento foi do voto do relator que listou as condições que os presos estão sujeitos no país, de acordo com o Ministro Marco Aurélio:

superlotação dos presídios, torturas, homicídios, violência sexual, celas imundas e insalubres, proliferação de doenças infectocontagiosas, comida imprestável, falta de água potável, de produtos higiênicos básicos, de acesso à assistência judiciária, à educação, à saúde e ao trabalho, bem como amplo domínio dos cárceres por organizações criminosas, insuficiência do controle quanto ao cumprimento das penas, discriminação social, racial, de gênero e de orientação sexual (AURELIO, 2015, p. 23).

Tais condições, segundo o ministro, criaram nos presídios um ambiente de estigmas, uma vez que aqueles sujeitos ao ambiente prisional se tornam “lixo do pior tratamento possível” e lhes são negados direitos básicos à existência mínima dentro do cárcere, segundo o ministro Marco Aurélio (2015, p. 25). Mas o estigma não termina aí, uma vez fora do ambiente prisional, a ressocialização não se concretiza, sendo comum a reincidência e perpetuando o problema (AURELIO, 2015).

Essa situação afeta principalmente pessoas negras, segundo os dados

⁶⁰ Por ocasião da Sentença 559 de 1997 que reconheceu vários elementos como estruturantes de um Estado de Coisas Inconstitucional.

apresentados no 14º Anuário Brasileiro de Segurança Pública: é relatado que em 2019 os negros representavam 66,7% da população carcerária brasileira. Segundo os dados do Anuário:

Por outro lado, quanto à raça/cor, identificamos também uma forte concentração entre a população negra. Em 2019, os negros representaram 66,7% da população carcerária, enquanto a população não-negra, aqui considerados brancos, amarelos e indígenas, segundo a classificação adotada pelo IBGE, representou 33,3%. Isto significa que para cada não-negro preso no Brasil em 2019, 2 negros foram presos. É um pouco mais que o dobro, quando comparado aos não-negros, em especial os brancos (ANUÁRIO, 2020, p. 307).

Isso não só reforça o argumento de um racismo estrutural no sistema carcerário brasileiro como também é consequência de um sistema estigmatizante, pois, ao negar o status de indivíduos dentro do cárcere, a sociedade perpetua o estereótipo de criminoso como um indivíduo de pele negra.

Em voto na mesma decisão, o ministro Luís Fachin também proferiu a mesma conclusão:

Os estabelecimentos prisionais funcionam como instituições segregacionistas de grupos em situação de vulnerabilidade social. Encontram-se separados da sociedade os negros, as pessoas com deficiência, os analfabetos. E não há mostras de que essa segregação objetiva - um dia - reintegrá-los à sociedade, mas sim, mantê-los indefinidamente apartados, a partir da contribuição que a precariedade dos estabelecimentos oferece à reincidência (FACHIN, 2015, p. 56).

O trecho acima reconhece jurisprudencialmente o que os números acima citados demonstram: que o sistema carcerário brasileiro tem como característica a segregação racial. Esse reconhecimento é importante quando da análise de pesquisas que indicam a reprodução do racismo através de algoritmos.

Ainda, é característica reconhecida pelos ministros na decisão em análise que o Estado de Coisas Inconstitucional não é atribuído a um ato ou a um Poder, mas sim é uma falha sistêmica, através de ações e omissões, de todos os Poderes e entes da federação. Nesse sentido, em sua preliminar, o ministro Marco Aurelio trouxe a seguinte visão panorâmica:

Há relação de causa e efeito entre atos comissivos e omissivos dos Poderes Públicos da União, dos Estados e do Distrito Federal, atacados nesta ação, e o quadro de transgressão de direitos relatado. O afastamento do estado de inconstitucionalidades, conforme se pretende nesta ação, só é possível mediante mudança significativa do comportamento do Poder Público, considerados atos de natureza normativa, administrativa e judicial (AURELIO, 2015, p. 22).

Na mesma linha, o ministro Luís Fachin também alude como pressuposto de um Estado de Coisas Inconstitucional a falha sistêmica do Poder Público como um todo:

As questões atinentes ao sistema penitenciário nacional há muito não encontram espaço fértil ou adequado de tratamento pelos poderes Executivo e Legislativo. Os

direitos dos encarcerados não encontram qualquer espaço na criação e implementação de políticas públicas (Executivo) e tampouco em qualquer atuação legislativa (Legislativo) (FACHIN, 2015, p. 50).

Portanto, é seguro concluir que a decisão, ao reconhecer a figura de inconstitucionalidade permanente no sistema carcerário, traz como pressuposto, conforme o reconhecimento de falhas dos três Poderes e dos entes da federação, que existam ações fora do sistema carcerário que contribuem para essa figura de violação estrutural de direitos fundamentais.

O reconhecimento das falhas pelos três poderes da União, dos Estados e do Distrito Federal é importante quando falamos de segurança pública, considerando que a adoção de sistemas de reconhecimento facial acontece em níveis municipais, estaduais e federais através de políticas estabelecidas pelos respectivos executivos, validadas pelos legislativos e as prisões delas decorrentes validadas pelos judiciários.

É nesse sentido que será demonstrado que as tecnologias de reconhecimento facial são mais uma maneira de perpetuação dessa situação no Brasil.

2 – AS TECNOLOGIAS DE RECONHECIMENTO FACIAL COMO REFORÇO AO RACISMO ESTRUTURAL

Primeiramente é necessário delinear como o debate sobre utilização da vigilância algorítmica passou a ser central no contexto da segurança pública no Brasil. Esse debate passa pelo desenvolvimento de tecnologias como Internet das Coisas e algoritmos com treinamentos baseados em estatísticas.

A evolução da tecnologia junto à evolução da internet como sistema de interconexão entre pessoas e máquinas resultou em meios de coleta de dados de forma massificada e em grande escala. Atualmente, principalmente impulsionado pelo interesse de mercado na utilização de dados como mecanismo de alcance de seus produtos e melhora na eficiência de seus resultados financeiros, todos os dispositivos que possuem acesso à uma conexão de internet coletam dados para finalidades que, em muitos casos, podem não ser claras.

Uma definição sobre Internet das Coisas é:

Um mundo onde objetos físicos são perfeitamente integrados em uma rede de informações, e onde objetos físicos se tornam participantes ativos nos processos negociais. Serviços são disponibilizados para interagir com esses "objetos inteligentes" pela Internet, consultar seu estado e informações associadas a eles, levando em conta problemas de segurança e privacidade (HALLER *et al.*, 2008).

O elemento de interconexão entre objetos físicos é de extrema importância, pois ele

permite a coleta de dados em maneira massificada, principalmente em áreas públicas, tanto de tipos quanto de quantidade de dados.

O atual estado de desenvolvimento da Internet das Coisas facilita a coleta de imagens sem que indivíduos tenham conhecimento, trazendo problemas de ordem da privacidade e no caso de reconhecimento facial para fins de segurança pública. Essa relação tem a ver com a falta de transparência e controle:

Entretanto, usuários frequentemente não tomam conhecimento de tecnologias de Internet das Coisas, uma vez que não existem mecanismos uniformes para a descoberta deles, muito menos acessar as configurações de privacidades que essas tecnologias podem suportar. Por exemplo, não existe uma maneira padronizada para determinar se uma área está sobre vigilância de vídeo e quais algoritmos são aplicados nas imagens coletadas pelas câmeras (por exemplo, reconhecimento facial, reconhecimento de expressões faciais, reconhecimento de cenas, mensuração de engajamento com produtos⁶¹ (DIAS *et al.*, 2018, p. 35-46).

A coleta desses dados fornece material para desenvolvimento de tecnologias com base em estatísticas, como as tecnologias de reconhecimento facial. O desenvolvimento dessas tecnologias acontece há mais décadas, mas é com a possibilidade de interconexão de objetos que as atuais tecnologias passaram a ter elevados graus de acerto e seu uso expandido para áreas como segurança pública.

Isso decorre do fato que é possibilitado ao Estado coleta de dados de imagem através de várias câmeras em locais públicos, garantindo a possibilidade de identificar qualquer indivíduo que transite pelo local.

As tecnologias de reconhecimento facial contam com algoritmos que realizam o uso dos dados da imagem de um indivíduo para realizar a identificação biométrica, algo que é também chamado de vigilância algorítmica (INTRONA; WOOD, 2004, p. 177-198).

Todavia, o mundo passou a ver com olhos críticos o desenvolvimento desses sistemas automatizados.

Em 2020, a IBM, uma das maiores empresas de tecnologia do mundo abandonou o desenvolvimento de tecnologias de reconhecimento facial em massa em consequência do potencial de perpetuação do racismo pelos algoritmos nesses sistemas e fez um apelo ao

⁶¹ Tradução livre. No original; “Instead, users are often unaware of the presence of IoT technologies, as there is no uniform mechanism for discovering them, let alone accessing any privacy settings these technologies might support. For instance, there is no standardized way of determining whether an area is under video surveillance and what algorithms might be applied to the footage captured by cameras (for example, facial recognition, facial expression recognition, scene recognition, measuring engagement with products)”

Congresso norte-americano por regulação na área.⁶²

Na Europa, as duas autoridades responsáveis pela supervisão de aplicação das legislações de proteções de dados pessoais, European Data Protection Board e European Data Protection Supervisor, se posicionaram em junho de 2021 pela proibição de utilização de algoritmos de inteligência artificial para reconhecimento facial em ambientes públicos por seus riscos, principalmente para minorias:

Levando em conta os riscos extremamente altos impostos por identificação biométrica remota de indivíduos em espaços públicos, a EDPB e a EDPS clamam por um banimento geral em qualquer uso de inteligência artificial para reconhecimento automatizado de características humanas em espaços públicos, como reconhecimento facial, padrão de caminhada, digitais, DNA, voz, digitação ou outros sinais biométricos ou comportamentais, em qualquer contexto. Similarmente, a EDPB e a EDPS recomendam o banimento de sistemas de inteligência artificial que utilizam biometria para caracterizar indivíduos em grupos baseados em etnicidade, gênero, orientação política ou sexual, ou qualquer outros critérios em que a discriminação é proibida pelo Artigo 21 da Carta de Direitos Fundamentais.⁶³ (tradução nossa).

Entretanto, no Brasil a tendência segue na contramão⁶⁴. A sociedade brasileira clama por maneiras de diminuir a violência nos grandes centros urbanos, passando a ter um grau elevado de adesão a medidas autoritárias, resultando em uma propensão social em aceitar a utilização de sistemas de reconhecimento facial em espaços públicos como maneira de combate ao crime.

Segundo pesquisa conduzida pelo Fórum Brasileiro de Segurança Pública em 2015, intitulado Medo da Violência e o Apoio ao Autoritarismo no Brasil – índice de Propensão ao apoio a Posições Autoritárias:

E é com base nestas medidas de medo e de autoritarismo que o FBSP reitera o papel do medo da violência e da segurança pública na determinação dos rumos e sentidos do debate político brasileiro nos próximos meses. O modo como o tema será incorporado e priorizado pelos diferentes atores e pela sociedade civil deve determinar a maior ou menor probabilidade de sucesso de discursos radicais na agenda eleitoral que se avizinha. **Os resultados do índice de autoritarismo**

⁶² Notícia que foi divulgada mundialmente em grandes veículos de informações: IBM abandons 'biased' facial recognition tech. BBC. Londres. 09 de junho de 2020. Disponível em: <https://www.bbc.com/news/technology-52978191>. Acesso em: 30 jun. 2021.

⁶³ Nota conjunta das autoridades: EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. European Data Protection Board. Brussels. 21 de junho de 2021. Disponível em: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en. Acesso em: 30 jun. 2021.

⁶⁴ Notícia pela jornalista Tailane Muniz demonstrando que o reconhecimento facial já é utilizado para realização em prisões: Reconhecimento facial já prendeu 35 na Bahia; 3 mil são alvos da polícia. Correio 24 Horas. Salvador. 01 de junho de 2019. Disponível em: <https://www.correio24horas.com.br/noticia/nid/reconhecimento-facial-ja-prendeu-35-na-bahia-3-mil-sao-alvos-da-policia/>. Acesso em: 30 jun. 2021.

sugerem que segmentos que enxergam na aniquilação autoritária da cidadania e da liberdade a forma de impor e manter a ordem, a moral e os bons costumes parecem ganhar eco a partir das incertezas sociais e políticas em que vivemos. No entanto, como vivemos em uma sociedade dinâmica e plural, é possível supor que quem melhor administrar as expectativas e for capaz de propor um projeto político e institucional que faça frente ao medo e à insegurança tende a levar vantagem até mesmo em relação aos grupos mais radicais. (grifo nosso)

A utilização desses sistemas em espaços públicos garante vigilância constante do Estado, podendo monitorar as atividades de todos os cidadãos e violar a privacidade individual em nome do discurso de maior segurança.

Essa vigilância algorítmica para finalidade de segurança pública, seja em investigações criminais, seja para a prevenção de crimes, passou a ser adotada há alguns anos no Brasil e estudos já foram realizados demonstrando problemas de ordem racial. Em 2019 o Relatório Retratos da Violência – Cinco meses de monitoramento, análises e descobertas produzido pela Rede Observatório de Segurança analisou 151 casos de prisões com base em reconhecimento facial em quatro estados do Brasil e verificou que no estado da Bahia 90,5% dos presos eram negros.

Ocorre que algumas pesquisas recentes indicam erros de reconhecimento (troca de um indivíduo por outro ou não reconhecimento do indivíduo) que acontecem com maior frequência envolvendo pessoas negras. Isso leva a uma possível conclusão de que os algoritmos reproduzem preconceitos raciais da sociedade.

Em 2018 foi anunciado que um estudo conduzido pela pesquisadora Joy Buolamwini através do Massachusetts Institute of Technology encontrou taxa de erros de 0.8% em sistemas de reconhecimento facial para reconhecimento de homens de pele clara, enquanto para mulheres negras a taxa de erro ficou em 34%.⁶⁵

Esses erros decorrentes da execução do algoritmo que causam a identificação errada, trocando um indivíduo pelo outro, levam a violações de direitos fundamentais de toda a população negra, pois acaba por atingir pessoas que podem não estar envolvidas em crimes. Isso já ocorreu em 2020 com a prisão incorreta através de erro de algoritmo de reconhecimento facial com Robert Williams, um estadunidense negro na cidade de Detroit.⁶⁶

⁶⁵O estudo teve suas conclusões publicadas por Larry Hardesty na página de notícias da universidade: Study finds gender and skin-type bias in commercial artificial-intelligence systems. MIT News Office. Cambridge. 11 de fevereiro de 2018. Disponível em: <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>. Acesso em: 30 jun. 2021.

⁶⁶A notícia foi publicada mundialmente pelas repercussões no discurso de igualdade racial: Polícia dos EUA prende injustamente homem negro identificado por tecnologia de reconhecimento facial. [S.L.]. 25 de junho de 2020. Disponível em: <https://gizmodo.uol.com.br/policia-prende-homem-negro-reconhecimento-errado/>. Acesso em: 30 jun. 2021.

Esses algoritmos, no Brasil, acabam por apresentar uma maneira de perpetuar o racismo estrutural que já é amplamente reconhecido no sistema penal:

Isso porque, a seletividade do sistema penal, demonstrada previamente, comprova que a população negra já sofre diuturnamente com o estereótipo de criminoso, desde microagressões que envolvem uma excessiva vigilância em estabelecimento comercial, cuja intencionalidade é facilmente negada, até casos de prisões indevidas e injustas. Com uma tecnologia em que o próprio algoritmo cumprirá este papel de indicar pessoas negras, equivocadamente, como potenciais suspeitas de um crime, novamente elas estarão “sujeitas à automatização de constrangimentos e violências, como abordagens policiais indevidas e atribuição inverídica de antecedentes criminais” (SILVA; SILVA, 2019, p. 12).

Ou seja, essa perpetuação do racismo estrutural via algorítmica tem como consequência a violação de direitos como igualdade e presunção de inocência, uma vez que indivíduos negros podem ser apontados como suspeitos de crimes como consequência de uma discriminação racial (*racial bias*) em seu treinamento.

Um exemplo utilizado Alex Najibi no cenário da polícia dos Estados Unidos da América ajuda a esclarecer o conceito de viés racista nos treinamentos algorítmicos:

Americanos negros possuem maior propensão à prisão e encarcerados por crimes de menor potencial ofensivo do que Americanos brancos. Consequentemente, Americanos negros são super-representados em bancos de fotos de prisão que algoritmos de reconhecimento facial utilizam para previsões. A presença de negros nesses sistemas cria um ciclo de realimentação em que estratégias policiais racistas levam à índices desproporcionais de prisão de negros, que por sua vez são objetos de vigilância (NAJIBI, 2020).

Esse tipo de erros decorrentes de discriminação racial nos algoritmos já foi verificado em grandes redes sociais, como o caso em que cortes de fotos na rede social Twitter dava preferência a pessoas brancas (CAPUTO, 2021).

Já existem estudos comprovando a discriminação racial em algoritmos:

Em 2016, um estudo da ProPublica demonstrou que uma das ferramentas mais utilizadas nos EUA para avaliação de risco de reincidência criminal, conhecida como COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), apresentava viés racial, classificando pessoas brancas como menos arriscadas e negras como mais arriscadas do que de fato eram, além de identificar afrodescendentes como duas vezes mais propícios do que os brancos ao cometimento de crimes violentos.⁸ Tal diferenciação ocorre principalmente em razão da utilização de dados históricos de prisões e condenações anteriores, que acabam por perpetuar práticas policiais e judiciais racistas, exacerbando as disparidades raciais enraizadas na sociedade (GUEDES, 2019, p. 2).

Com esses problemas, seja pela predisposição de um sistema indicar uma pessoa negra como possível autora de crime, seja pela identificação errada de uma pessoa negra

por outra, fazem dos sistemas de reconhecimento facial uma fonte de violações sistemáticas à direitos fundamentais como igualdade e presunção de inocência por parte do Estado, responsável pela adoção desses algoritmos ou pela omissão dele em não coibir a utilização dos sistemas.

3 – O EFEITO DAS REGULACÕES EM INTELIGÊNCIA ARTIFICIAL E PROTEÇÃO DE DADOS NO PROBLEMA EM ESTUDO

Uma das grandes tendências regulatórias do século XXI tem sido regulações para novas tecnologias que podem trazer danos à direitos fundamentais de indivíduos e minorias.

É preciso levar em conta como essas regulações podem afetar a utilização de sistemas de reconhecimento facial e as consequências no Estado de Coisas Inconstitucional do sistema carcerário brasileiro.

Destarte, a proteção de dados pessoais é, dentre os dois tipos de regulações, a mais antiga, mas que as recentes mudanças na lógica normativa incorporaram as preocupações de coletas massificadas e decisões automatizadas.

As regulações de proteção de dados pessoais remontam às décadas de 70 e 80 em países europeus como Alemanha, Áustria, Dinamarca, França, Noruega e Suécia (RUDGARD, 2019, p. 13).

Em 2016 foi aprovada a Diretiva 2016/680 na União Europeia, que trata sobre a proteção de dados pessoais no contexto investigativo, e como considerando trouxe as novas tendências tecnológicas:

(3) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A partilha e a recolha de dados pessoais registaram um aumento significativo. A tecnologia permite o tratamento de dados pessoais numa escala sem precedentes para o exercício de funções como a prevenção, investigação, deteção ou repressão de infrações penais e a execução de sanções penais.

No Brasil, o efeito disso foi a aprovação da Lei nº 13.709/2018, com entrada em vigor em setembro de 2020. Ocorre que a legislação não se aplica às atividades de segurança pública e atividades de investigação e repressão penal.⁶⁷

Ocorre que o Supremo Tribunal Federal, em maio de 2020, julgou as ADIs 6.387,

⁶⁷ Segundo o artigo 4º, inciso II, alíneas “a” e “d”.

6.388, 6.389, 6.390 e 6.393 que contestavam a Medida Provisória 954/20 pois ela demandava o compartilhamento de dados pessoais constantes nos bancos de dados das companhias telefônicas para o IBGE a fim de realizar o censo de 2020.

O julgamento reconheceu a autodeterminação informativa e a proteção de dados pessoais como direitos fundamentais depreendidos da Constituição Federal. O ministro Luis Fux expôs o seguinte raciocínio:

A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), todos previstos na Constituição Federal de 1988 (FUX, 2020, p. 59).

Autodeterminação informativa remonta à decisão semelhante do Tribunal Constitucional Alemão de 1983:

Dessa forma, o Tribunal Constitucional Federal constata que o art. 2 §1 combinado com o art. 1 §1 LF resultaria um direito fundamental à autodeterminação informativa que garantiria “o poder do indivíduo em determinar fundamentalmente por si mesmo sobre a coleta e utilização de seus dados pessoais (MENDES, 2019, p. 188).

Assim, ainda que a legislação infraconstitucional brasileira não seja aplicada à coleta de dados para as finalidades do art. 4º, inciso II, alíneas “a” e “d” cujos objetos são justamente o que é analisado no presente artigo, a proteção no nível constitucional existe.

Fica garantido aos alvos de tecnologias de reconhecimento facial na esfera criminal o direito de controle sobre o uso de seus dados biométricos como um direito de ordem constitucional.

A leitura que pode ser feita, portanto, é de um argumento no nível constitucional de que as tecnologias de reconhecimento facial não só trazem consequências de agravamento Estado de Coisas Inconstitucional no sistema prisional, mas também reforça a inconstitucionalidade da utilização desses sistemas pelo poder público no contexto analisado.

A segunda grande tendência regulatória que acaba por trazer maior possibilidade de análises sobre o uso de reconhecimento facial como instrumento de segurança pública trata sobre o desenvolvimento de algoritmos de inteligência artificial, utilizados nos sistemas de monitoramento para a identificação.

A União Europeia busca garantir a vanguarda desse tipo de regulação, lançando a

primeira proposta de Regulação em Inteligência Artificial em 21 de abril de 2021. Nos considerandos 18 e 19 da proposta regulatória são expostas as preocupações com essas tecnologias, requerendo, inclusive, o seu banimento (com exceção de 3 casos específicos).⁶⁸

Deve-se fazer uma ressalva: a União Europeia não sofre com o estado precário de sua estrutura carcerária que acaba por violar sistematicamente direitos de minorias raciais como o Brasil. Esse contexto, se analisado sob o prisma que até mesmo países com estruturas que não ofendem direitos fundamentais como o nosso reconhecem a necessidade de limitação/proibição de algoritmos de reconhecimento facial, acaba por reforçar a conclusão de extrema potencialidade de ofensa dessas tecnologias em países com situação de violação sistemáticas de direitos fundamentais de minorias no contexto criminal.

Por sua vez, o Brasil, em 06 de julho de 2021, aprovou o regime de urgência para a tramitação do PL 21/2020, que institui o Marco Legal de Inteligência Artificial. Todavia, diferente da diretiva europeia, ele não possui previsões sobre vedações de utilização para desenvolvimento de algoritmos utilizados na identificação facial, ainda que traga entre seus princípios a não discriminação como impossibilidade de uso dos sistemas para fins discriminatórios, ilícitos ou abusivos (redação do art. 6º, inciso III do texto original).

Ao contrário, a proposta estimula a adoção das tecnologias de inteligência artificial

⁶⁸ Segundo o considerando 18 :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 manutenção da ordem pública é considerada 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. Além disso, dado o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções da utilização desses sistemas que funcionam «em tempo real», estes dão origem a riscos acrescidos para os direitos e as liberdades das pessoas visadas pelas autoridades policiais. Já o considerando 19 pede a proibição geral da utilização de algoritmos para reconhecimento facial para manutenção da ordem pública, listando três exceções: “Como tal, deve ser proibida a utilização desses sistemas para efeitos de manutenção da ordem pública, salvo em três situações enunciadas exaustivamente e definidas de modo restrito, em que a utilização é estritamente necessária por motivos de interesse público importante e cuja importância prevalece sobre os riscos. Essas situações implicam a procura de potenciais vítimas de crimes, incluindo crianças desaparecidas, certas ameaças à vida ou à segurança física de pessoas singulares ou ameaças de ataque terrorista, e a deteção, localização, identificação ou instauração de ações penais relativamente a infratores ou suspeitos de infrações penais a que se refere a Decisão-Quadro 2002/584/JAI do Conselho 38 , desde que puníveis no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro. Esse limiar para a pena ou medida de segurança privativa de liberdade prevista no direito nacional contribui para assegurar que a infração seja suficientemente grave para justificar potencialmente a utilização de sistemas de identificação biométrica à distância «em tempo real». Além disso, das 32 infrações penais enumeradas na Decisão-Quadro 2002/584/JAI do Conselho, algumas são provavelmente mais pertinentes do que outras, já que o recurso à identificação biométrica à distância «em tempo real» será previsivelmente necessário e proporcionado em graus extremamente variáveis no respeitante à deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito das diferentes infrações penais enumeradas e tendo em conta as prováveis diferenças em termos de gravidade, probabilidade e magnitude dos prejuízos ou das possíveis consequências negativas.”

no Poder Público como um todo para diminuição de custos e aumento de eficiência, sem distinções de objetos e finalidades, o que é possível interpretar como um estímulo à adoção de algoritmos de reconhecimento facial nas atividades persecutórias públicas.

Assim, temos em nível de legislativo infraconstitucional a possibilidade de um estímulo à utilização de tecnologias que reproduzem uma estrutura de racismo social, o que foi um dos argumentos explorados pelo Supremo Tribunal Federal sobre o Estado de Coisas Inconstitucionais no sistema carcerário brasileiro: todos os poderes acabam por adotar práticas e se omitir em suas competências que afetam a estrutura da segregação racial no cárcere brasileiro.

Portanto, até mesmo sob a análise das novas tendências regulatórias é possível encontrar argumentos que reforçam o caráter prejudicial das tecnologias de reconhecimento facial.

CONCLUSÃO

O ensaio partiu da conceituação da figura do Estado de Coisa Inconstitucional no sistema carcerário brasileiro pelo Supremo Tribunal Federal que verificou a existência dos três requisitos: o resultado de uma causa estrutural ou histórica; que não pode ser atribuída a um único ente, mas ao Estado em seu conjunto e que exige a adoção de medidas de longo prazo.

Em seguida, foi demonstrado como os algoritmos de sistemas de reconhecimento facial utilizados para identificação biométrica podem afetar direitos fundamentais, principalmente para indivíduos negros, considerando erros dos algoritmos e a predisposição desses sistemas apontarem pessoas negras como autoras de crimes, em consequência de um racismo estrutural que é replicado por algoritmos.

Ainda, com essa relação entre a predisposição de algoritmos de reconhecimento facial indicarem pessoas negras como autoras de crimes ou errar a pessoa reconhecida por problemas envolvendo a análise da cor de pele e, é criada mais uma maneira de levar indivíduos de pele negra para o sistema carcerário brasileiro, uma ofensa permanente ao direito fundamental da presunção de inocência para negros.

Por sua vez, dentro do sistema carcerário, o estereótipo social de pessoas negras como criminosas reforça o Estado de Coisa Inconstitucional dentro e fora do cárcere, renegando negros à uma subcategoria de pessoas, ofendendo o direito fundamental da igualdade.

Assim, fica evidenciado que a utilização dessas tecnologias reforça o Estado de Coisas Inconstitucional no seu primeiro requisito.

Também é possível verificar que a adoção desses sistemas reforça a figura em seu segundo requisito, pois os três Poderes acabam por estar envolvidos: o Executivo, através das forças policiais, que realiza a contratação e utilização dos sistemas; o Legislativo, através da omissão de proibição legal de utilização de sistemas de reconhecimento facial em locais públicos e para utilização em matéria penal; e o Judiciário, que valida as prisões em que os sistemas foram empregados.

O último requisito para o reconhecimento do Estado de Coisas Inconstitucional acaba reforçado por essas tecnologias pois elas perpetuam o racismo estrutural que ainda faz parte da sociedade brasileira e demandará muitos anos de luta por igualdade racial e pela predisposição da sociedade em aceitar medidas autoritárias e invasivas, como utilização de algoritmos para possibilitar a perda de liberdade em prol de segurança pública.

Por fim, a análise das novas tendências regulatórias reforça o argumento de que os algoritmos para reconhecimento facial encontram resistências de ordem constitucional sob o prisma do direito à igualdade, dignidade da pessoa humana e de autodeterminação informativa, principalmente de minorias raciais que sofrem em um sistema carcerário que viola sistematicamente esses direitos.

REFERÊNCIAS BIBLIOGRÁFICAS

ANGWIN, Julia; KIRCHNER, Lauren; LARSON, Jeff; MATTU, Surya. Machine Bias: **There's software used across the country to predict future criminals. And it's biased against blacks.** ProPublica, 23 mar. 2016. Disponível em: www.propublica.org/article/machine-bias-riskassessments-in-criminal-sentencing. Acesso em: 30 jun. 2021.

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA 2020. São Paulo: Fórum Brasileiro de Segurança Pública, 2020. Ano 14. ISSN 1983-7364. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2020/10/anuario-14-2020-v1-interativo.pdf>. Acesso em: 29 jun. 2021.

BRASIL. Supremo Tribunal Federal. **Acórdão.** Medida cautelar em ação direta de inconstitucionalidade. referendo. medida provisória nº 954/2020. emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19). compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. fumus boni juris. periculum in mora. deferimento. Brasília, DF, 7 de maio de 2020. Disponível em:

<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567>. Acesso em: 20 ago. 2021.

BRASIL. Supremo Tribunal Federal. **Acórdão**. Medida cautelar na arguição de descumprimento de preceito fundamental 347 Distrito Federal. Brasília, DF, 9 de setembro de 2015. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10300665>. Acesso em: 29 jun. 2021.

CAPUTO, Manuela. Racismo algorítmico e o trabalho de pesquisadores da área para obterem reconhecimento. **MediaLab UFRJ**. Rio de Janeiro, 24 de maio de 2021. Disponível em: <http://medialabufrj.net/blog/2021/05/racismo-algoritmico-pesquisadores/>. Acesso em: 30 jun. 2021.

COLOMBIA. Corte Constitucional. **Sentencia 559/97**. Bogotá, 6 de novembro de 1997. Disponível em: <http://www.cor-teconstitucional.gov.co/relatoria/1997/SU559-97.html>. Acesso em: 29 jun. 2020.

DAS, Anupam; DEGELING, Martin; SMULLEN, Daniel; SADEH, Normal. Personalized privacy assistants for the internet of things: providing users with notice and choice. **IEEE Pervasive Computing**. Los Alamitos, Estados Unidos, v. 17, n. 3, p. 35-46. 2018.

EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. **European Data Protection Board**, Bruxelas, 21 de junho de 2021. Disponível em: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en. Acesso em: 30 jun. 2021.

FÓRUM Brasileiro de Segurança Pública (org.). **Medo da violência e o apoio ao autoritarismo no Brasil**: índice de propensão ao apoio a posições autoritárias. São Paulo: Fórum Brasileiro de Segurança Pública, 2017. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2019/04/FBSP_indice_propensao_apoio_posicoes_autoritarios_2017_relatorio.pdf. Acesso em: 30 jun. 2021.

GUEDES, Paula. Discriminação tecnológica: desmistificando a neutralidade da Inteligência Artificial em meio à crise de inclusão e de diversidade nas tecnologias emergentes. **ITS Rio**, Rio de Janeiro. 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/10/Discriminação-tecnológica_Paula_Guedes.pdf. Acesso em: 30 jun. 2021.

HALLER, Stephan; KARNOUSKOS, Stamatis; SCHROTH, Christoph. The internet of things in an enterprise context. **First Future Internet Symposium - FIS 2008**, Vienna, 2008. Disponível em: www.researchgate.net/publication/221142742_The_Internet_of_Things_in_an_Enterprise_Context. Acesso em: 30 jun. 2021.

HARDESTY, Larry. Study finds gender and skin-type bias in commercial artificial-intelligence systems. **MIT News Office**, Cambridge, 11 de fevereiro de 2018. Disponível em: <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>. Acesso em: 30 jun. 2021.

IBM abandons 'biased' facial recognition tech. **BBC News**, Londres, 9 de junho de 2020. Disponível em: <https://www.bbc.com/news/technology-52978191>. Acesso em: 30 jun. 2021.

INTRONA, Lucas; WOOD, David. Picturing algorithmic surveillance: the politics of facial recognition systems. **Surveillance & Society**, v. 2, p. 177-198. 2004. Disponível em: <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-200675>. Acesso em: 30 jun. 2021.

KIMBALL, Whitney. Polícia dos EUA prende injustamente homem negro identificado por tecnologia de reconhecimento facial. **Gizmodo Brasil**, 25 de junho de 2020. Disponível em: <https://gizmodo.uol.com.br/policia-prende-homem-negro-reconhecimento-errado/>. Acesso em: 30 jun. 2021.

MACHADO, Maira Rocha. Quando o estado de coisas é inconstitucional: sobre o lugar do poder judiciário no problema carcerário. **Revista de Investigações Constitucionais**, [S.L.], v. 7, n. 2, p. 631. 2020. Universidade Federal do Parana. Disponível em: <https://revistas.ufpr.br/rinc/article/view/60692/41975>. Acesso em: 29 jun. 2021.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 39, p. 185-216. 2019. Disponível em: <http://dfj.emnuvens.com.br/dfj/article/view/655/905>. Acesso em: 20 ago. 2021.

MUNIZ, Tailane. Reconhecimento facial já prendeu 35 na Bahia; 3 mil são alvos da polícia. **Correio 24 Horas**, Salvador, 1 de junho de 2019. Disponível em: <https://www.correio24horas.com.br/noticia/nid/reconhecimento-facial-ja-prendeu-35-na-bahia-3-mil-sao-alvos-da-policia/>. Acesso em: 30 jun. 2021.

NAJIBI, Alex. Racial discrimination in face recognition technology. **Science in the news**, Harvard, Boston, 24 de outubro de 2020. Disponível em: <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>. Acesso em: 30 jun. 2021.

REDE DE OBSERVATÓRIOS DA SEGURANÇA. Retratos da violência: cinco meses de monitoramento, análises e descobertas. Fortaleza: CESEC, 2019. Disponível em: https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf. Acesso em: 30 jun. 2021.

RUDGARD, Sian. Introduction to european data protection. **European data protection: law and practice**. 2. ed. International Association of Privacy Professionals (IAPP). 2019. Disponível em: <https://iapp.org/resources/article/european-data-protection/>. Acesso em: 30 jun. 2021.

SILVA, Rosane Lea; SILVA, Fernando dos Santos Rodrigues. Reconhecimento facial e segurança pública: os Perigos do uso da tecnologia no sistema penal seletivo brasileiro. **Anais do 5º Congresso Internacional de Direito e Contemporaneidade**. Santa Maria – RS: Universidade Federal de Santa Maria, 2019. Disponível em: <https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf>. Acesso em: 30 jun. 2021.