UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIRETO

PROGRAMA DE GRADUAÇÃO EM DIREITO

MATHEUS SANTOS MENDONÇA

OS RISCOS DO RECONHECIMENTO FACIAL PARA A PERSECUÇÃO PENAL: uma discussão sobre violação de direitos fundamentais a partir da implementação no metrô de São Paulo

Brasília

2024

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIRETO
PROGRAMA DE GRADUAÇÃO EM DIREITO

MATHEUS SANTOS MENDONÇA

OS RISCOS DO RECONHECIMENTO FACIAL PARA A PERSECUÇÃO PENAL: uma discussão sobre violação de direitos fundamentais a partir da implementação no metrô de São Paulo

Monografia apresentada como requisito parcial de obtenção do título de Bacharel em Direito pelo Programa de Graduação em Direito da Universidade de Brasília.
Orientador: Professor Guilherme Gomes Vieira.

Brasília
2024

MATHEUS SANTOS MENDONÇA

OS RISCOS DO RECONHECIMENTO FACIAL PARA A PERSECUÇÃO PENAL: uma discussão sobre violação de direitos fundamentais a partir da implementação no metrô de São Paulo

Monografia apresentada como requisito parcial de obtenção do título de Bacharel em Direito pelo Programa de Graduação em Direito da Universidade de Brasília.
Orientador: Professor Guilherme Gomes Vieira.

Banca Examinadora

_____

Prof. Me. Guilherme Gomes Vieira
Orientador – Universidade de Brasília

_____

Profa. Dra. Fernanda de Carvalho Lage
Membra interna – Universidade de Brasília

_____

Prof. Dr. Evandro Charles Piza Duarte
Membro interno – Universidade de Brasília

AGRADECIMENTOS

Pensar na trajetória percorrida nesses últimos seis anos envolve um sentimento inefável.

É como se estivesse fazendo parte de um filme no qual não existe um protagonista, mas em que todos os atores exercem coletivamente esse papel. De qualquer forma, se pudesse nomear esse sentimento, diria que se trata de uma profunda gratidão, que vem da alma, em relação a todos que protagonizaram tantos momentos especiais durante esse período.

A começar pelo autor da vida e da história, agradeço a Deus pela oportunidade de dividir o espaço-tempo com pessoas que tornaram possível a realização de um objetivo que se iniciou ainda na adolescência. Bendigo a Ele por cada detalhe de amor e bondade durante esse percurso.

Agradeço à minha família, que, desde meus primeiros passos - literalmente falando - até o presente momento, foram os responsáveis pela formação de toda a minha essência. Agradeço, especialmente, aos meus pais, João Batista e Maria de Fátima, por cada dia de luta, debaixo de sol e de chuva, para que nada faltasse. Pelas noites mal dormidas, sacrifícios financeiros, humilhações no trabalho, enfim, por doarem tanto amor sem nunca terem exigido nada em troca. Sem vocês, nada teria sentido.

À minha avó, Eliana, pelo carinho incondicional, e meu avô, Manoel (*in memoriam*), por ter demonstrado que o trabalho é uma virtude e dignifica.

A meus irmãos, João Pedro, companheiro de vida e a quem sou grato por cada incentivo e apoio, Vinicius e Daniel, pelos conselhos e exemplos.

Agradeço, ademais, a todas as pessoas que estiveram ao meu lado de alguma forma nesse período: Thiago, que, seja nas caminhadas semanais, seja nas conversas e estudos compartilhados sobre direito, foi um parceiro ímpar até aqui, Wesley, Luan, João Victor e Matheus Carvalho. À Luana Martins, por todo afeto, dedicação e companheirismo, e por ser calmaria em meio ao intenso final de curso.

Aos que participaram de minha introdução na vida profissional: Sarah, que tanto me ensinou e a quem sou grato pela confiança e por cada oportunidade, Clarissa, Emmanuel e Isadora, no Ibaneis Advocacia; Kakay, Liliane, Turbay e secretários, no Almeida Castro, Bruno e Vanessa, no STF, e Carla, no STJ.

Também sou grato às amigas e amigos de estágio, com os quais compartilhei várias tardes agradáveis e de muito aprendizado: Stephanie, Juliana, Luna, Letícia Rejane, Beatriz Monlevade, Rafael, Vitor, Beatriz Canedo, Ana Clara e Lumi.

Por óbvio, também agradeço a todas as amizades que a UnB me concedeu e que pretendo levar com carinho para a vida: André Roberto, Asafe, Givago, João Vitor, João Aviani, que me acompanhou do início ao fim em tantos trabalhos e a quem sou grato pela parceria, Helena Sayuri, Rafaella Bacellar, Marcelo Cascaes, e todos os outros que de alguma forma estiveram ao meu lado nesses seis anos.

Por fim, agradeço ao corpo docente e aos demais profissionais técnicos da Faculdade de Direito da UnB, pois, exercendo brilhantemente suas funções, contribuíram para tornar mais leve uma jornada afetada pela pandemia, por uma greve, e permeada por vários dias de cansaço devido à rotina de transporte público. De modo especial, agradeço ao professor Guilherme Vieira, pela compreensão, atenciosidade e inteligência durante as correções e aprimoramentos desse trabalho.

A cada protagonista dessa história, meu muito obrigado!

"*O pensamento é a força criadora, irmão. O amanhã é ilusório porque ainda não existe. O hoje é real, é a realidade em que você pode interferir.*
(...)
Não espere o futuro mudar a sua vida, porque o futuro será a consequência do presente".

(A vida é desafio, Racionais MC's)

RESUMO

O emprego da tecnologia de reconhecimento facial para a identificação biométrica automatizada de suspeitos de crimes e foragidos da justiça tem acontecido, predominantemente, no âmbito da vigilância de massas em espaços urbanos. Esse uso, contudo, tem desconsiderado estudos técnicos e casos reais que demonstram a existência de vieses discriminatórios inerentes ao processo de desenvolvimento e utilização dessa ferramenta, além da ausência de disposições legais suficientes ou atualizadas no sentido de limitá-la e contornar eventuais erros judiciários. Nesse sentido, o presente trabalho discorre sobre os riscos e desdobramentos da utilização de reconhecimento facial na política de segurança pública para direitos fundamentais durante a persecução penal. Realizou-se um estudo de caso sobre a implementação dessa tecnologia no metrô da cidade de São Paulo, discutido na Ação Civil Pública nº 1010667-97.2022.8.26.0053/TJSP, a fim de verificar se a utilização dessa tecnologia, nos termos em que proposta, pode agravar o atual cenário de violação a direitos fundamentais no âmbito da persecução penal no Brasil. A construção dos pressupostos teóricos dessa análise, bem como de seu conteúdo em si, foi alicerçada na revisão bibliográfica e documental de livros, artigos, pesquisas e legislações sobre o tema, bem como nas informações obtidas por meio de acesso ao processo no sítio eletrônico do Tribunal de Justiça de São Paulo. Como resultado, constatou-se que a eventual aplicação do reconhecimento facial no contexto analisado poderá acarretar uma série de violações a direitos e garantias aos usuários e frequentadores do espaço. Concluiu-se, ademais, a premência de uma regulamentação que salvaguarde concretamente os direitos fundamentais de todos os que estejam submetidos a situações semelhantes no país. Ao final, também foram analisadas algumas das proposições legislativas que visam criar o novo arcabouço normativo, bem como apontadas as medidas mais relevantes para a superação das más consequências do uso desse sistema a serem incluídas nas disposições legais.

PALAVRAS-CHAVE: Reconhecimento facial; Tecnologia; Persecução penal; Segurança pública; Direitos fundamentais; Vieses discriminatórios.

ABSTRACT

The use of facial recognition technology for the automated biometric identification of criminal suspects and fugitives from justice has predominantly taken place in the context of mass surveillance in urban spaces. The use of this technology for the automated biometric identification of criminal suspects and fugitives from justice has taken place predominantly in the context of mass surveillance in urban spaces. This use, however, has disregarded technical studies and real cases that demonstrate the existence of discriminatory biases inherent in the process of developing and using this tool, as well as the absence of sufficient or up-to-date legal provisions to limit it and circumvent possible miscarriages of justice. In this sense, this paper discusses the risks and consequences of using facial recognition in public security policy for fundamental rights during criminal prosecution. A case study was carried out on the implementation of this technology in the São Paulo subway, discussed in Public Civil Action No. 1010667-97.2022.8.26.0053/TJSP, in order to verify whether the use of this technology, as proposed, could aggravate the current scenario of violation of fundamental rights in the context of criminal prosecution in Brazil. The construction of the theoretical assumptions of this analysis, as well as its content, was based on a bibliographical and documentary review of books, articles, research and legislation on the subject, as well as information obtained by accessing the case on the website of the São Paulo Court of Justice. As result, it was found that the possible application of facial recognition in the context analyzed could lead to a series of violations of rights and guarantees of users and regular visitors of the space. This scenario also highlighted the urgent need for a regulation that concretely safeguards the fundamental rights of all those who are subjected to similar situations in the country. By the end, some of the legislative proposals aimed at creating the new regulatory framework were also analyzed, as well as pointing out the most relevant measures for overcoming the bad consequences of using this system to be included in the legal provisions.

KEYWORDS: Facial recognition; Technology; Criminal prosecution; Public security; Fundamental rights; Discriminatory biases.

LISTA DE FIGURAS E TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACP – Ação Civil Pública

ANPD – Autoridade Nacional de Proteção de Dados

BBW – *Big Brother Watch*

CCJ – Comissão de Constituição e Justiça

CCO - Centros de Controle Operacional

CCTV - *Closed Circuit Television*

CDC – Código de Defesa do Consumidor

CESeC - Centro de Estudos de Segurança e Cidadania

CF/88 – Constituição Federal de 1988

CIA - *Central Intelligence Agency*

CJF – Conselho da Justiça Federal

CMSP – Companhia do Metropolitano de São Paulo

CNJ – Conselho Nacional de Justiça

COMPAS - *Correctional Offender Management Profiling for Alternative Sanction*

CP – Código Penal

CPP – Código de Processo Penal

DPERJ – Defensoria Pública do Estado do Rio de Janeiro

DPESP – Defensoria Pública do Estado de São Paulo

DPU – Defensoria Pública da União

ECA – Estatuto da Criança e do Adolescente

EUA – Estados Unidos da América

FERET - *Facial Recognition Technology*

FRGC - *Face Recognition Grand Challenge*

FVRT - *Face Recognition Vendor Test*

GDPR - *General Data Protection Regulation*

HC – *Habeas Corpus*

IA – Inteligência Artificial

IoT – *Internet of Things*

IBGE – Instituto Brasileiro de Geografia e Estatística

IDEC - Instituto de Defesa do Consumidor

LAPIN - Laboratório de Pesquisa em Políticas Públicas e Internet

LGPD – Lei Geral de Proteção de Dados

LPI – Licitação Pública Internacional

NIJ - *National Institute of Justice*

NIST - *National Institute of Standards and Technology* p

PL – Partido Liberal

PL* – Projeto de Lei

PMERJ – Polícia Militar do Estado do Rio de Janeiro

PPB - *Pilot Partiament Benchmark*

PSD – Partido Social Democrático

PSOL – Partido Socialismo e Liberdade

RHC – Recurso em *Habeas Corpus*

RIPDP - Relatório de Impacto de Proteção de Dados Pessoais

SME – Sistema de Monitoramento Eletrônico

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TJSP – Tribunal de Justiça de São Paulo

TRF – Tecnologia de Reconhecimento Facial

SUMÁRIO

INTRODUÇÃO

Hoje podemos observar o limiar de uma verdadeira sociedade informacional[1] (Castells, 1999) repleta de instrumentos capazes de revolucionar a dinâmica das relações intersubjetivas em suas dimensões social, política, econômica e jurídica. Por outro prisma, a surgimento de aparelhos físicos (*hardwares*, como câmeras e *smartphones*) e virtuais (*softwares*, como programas e aplicativos) desenvolvidos por grandes corporações do ramo da tecnologia (*big techs*) tem potencializado um cenário de risco para os cidadãos, especialmente quando utilizadas pelo estado com a finalidade de restringir liberdades individuais por meio da vigilância de massas.

Nesse sentido, hodiernamente, merece atenção a proliferação do uso da tecnologia de reconhecimento facial – TRF (*facial recognition tecnology*), baseada em inteligência artificial[2], por parte de órgãos estatais, com a finalidade de aprimoramento da segurança pública (prevenção de delitos), e de fornecimento de elementos probatórios para subsidiar investigações e eventuais processos criminais contra suspeitos e acusados (repressão de delitos).

Ao abrir os noticiários, é possível observar uma expansão da adoção da referida tecnologia nos espaços urbanos enquanto estratégia de monitoramento e vigilância, que, usualmente, integra projetos governamentais para a modernização dessas atividades e para a formação de verdadeiras cidades inteligentes (*smart cities*).[3]

Tal fenômeno, embora recente, possui como pano de fundo um dualismo historicamente estabelecido e discutido no mundo jurídico que se origina na oposição entre aspectos constitucionalmente estabelecidos, a saber, o dever estatal de manutenção da segurança pública (art. 144, CF/88), e direitos e garantias individuais, como os direitos à privacidade/intimidade em suas diversas expressões (imagem, liberdade de expressão, reunião, etc.) (art. 5, X, XII, XVI, CF/88), à não discriminação (art. 3º, IV, e art. 5º, *caput*,

[1] "O termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido as novas condições tecno16gicas surgidas nesse período histórico". (Castells, 1999, p. 65).

[2] O Grupo de Peritos de Alto Nível em IA (AI-HLEG, 2019), criado pela comissão de inteligência artificial da União Europeia, conceituou a Inteligência Artificial como sendo um sistema de software - ou *hardware* desenvolvido por humanos que, atuando na dimensão física ou digital, é dotado da capacidade de coletar dados e interpretá-los (processá-los) com a finalidade de decidir, de forma automatizada, acerca das melhores ações a serem tomadas para alcançar determinado objetivo.

[3] Como exemplo de projeto governamental de implementação de *smart city* no contexto brasileiro, a prefeitura de São Paulo pretende modernizar a infraestrutura da cidade por meio da instalação de dispositivos integrados de tecnologia nos espaços públicos urbanos. (Coelho, 2023).

CF/88) à presunção de inocência (art. 5º, LVII, CF/88), e, mais recentemente, à proteção de dados pessoais (art. 5º, LXXIX, CF/88).

Especificamente no caso do uso da TRF para fins de segurança pública, a finalidade seria a identificação de possíveis suspeitos da prática de ilícitos criminais, das vítimas de tais crimes e de bens e pessoas desaparecidas, maximizando os resultados, num momento posterior, da atuação de órgãos responsáveis pelas atividades de persecução penal.

No entanto, a partir de uma simples pesquisa na *internet*, é possível verificar uma série de notícias sobre erros oriundos da utilização da TRF no país e no mundo como meio de identificação de indivíduos, que, em sua maioria, foram incorretamente apontados como suspeitos da prática de ilícitos quando do processamento e cruzamento dos dados obtidos com outros bancos de informações preexistentes.

Isso tem tido amplo contorno na realidade brasileira, especialmente no cotidiano das grandes capitais e metrópoles do país, locais que revelam sobremodo nossa histórica desigualdade socioeconômica e nos quais as inovações tecnológicas tendem a ser implementadas mais rapidamente.

E mais: tal imprecisão tem sido relacionada, geralmente, a critérios demográficos, como etnia, sexo, cor, nacionalidade, etc., representado, assim, diversos falsos positivos envolvendo pessoas de baixa classe econômica, imigrantes, residentes das periferias e negras.

Assim, a presente pesquisa parte do pressuposto de que a inserção do mecanismo da TRF na salvaguarda da segurança pública em nosso contexto de desigualdades sociais tem potencializado relações de poder historicamente estabelecidas em detrimento de direitos fundamentais, "ponto em que os castigos universais das leis vêm se aplicar seletivamente a certos indivíduos e sempre aos mesmos". (Foucault, 2014, p. 216).

Além disso, um segundo problema pertinente ao tema ora analisado é a ausência de um marco normativo específico.

Isso porque, embora a legislação pátria possua a Lei Geral de Proteção de Dados pessoais - LGPD (Lei n. 13.709/2018) - que regulamenta o tratamento de dados pessoais -, bem como capítulo no Código de Processo Penal – CPP (Decreto-Lei nº 3.689/1941) estabelecendo balizas sobre o procedimento de reconhecimento de pessoas e coisas (art. 226 a 228), nota-se que: a) a LGPD, norma de caráter civil, possui disposição expressa pela inaplicabilidade de suas disposições, no tratamento de dados pessoais, para fins de segurança

pública e persecução penal[45]; b) o capítulo contido no CPP versa sobre o reconhecimento de pessoas feito presencialmente, de forma genérica e nos termos em que foi promulgado, ou seja, não foi alterado no sentido de estender suas disposições às novas formas de reconhecimento por meio de instrumentos tecnológicos.

Tendo em mente os aspectos acima pontuados, como forma de aferir os efeitos dessa novidade sobre a vida dos cidadãos, propôs-se a análise da discussão contida na Ação Civil Pública nº 1010667-97.2022.8.26.0053, que tramita no Tribunal de Justiça do Estado de São Paulo (TJSP) e versa, de modo pioneiro, sobre a implementação de um *software* de reconhecimento facial para fins de segurança pública no espaço das Linhas 1 (azul), 2 (verde), e 3 (vermelha) do metrô da cidade de São Paulo.

Essa análise se voltará, em síntese, para a resolução da seguinte questão: a eventual implementação da tecnologia de reconhecimento facial em espaços públicos como o metrô de São Paulo, previamente à regulamentação do assunto no contexto brasileiro, pode contribuir para a ocorrência de erros judiciários no processo penal, potencializando um cenário de violação a direitos fundamentais já existente?

Nesse ponto, será utilizado, num primeiro momento, o método dedutivo[6] de pesquisa, tendo em vista que se partirá de um marco teórico preestabelecido a respeito dos riscos que caracterizam o uso da TRF rumo à verificação da incidência dessa premissa num fenômeno particular, a saber, a implementação do Sistema de Monitoramento Eletrônico (SME) pela CMSP no espaço do metrô paulistano.

Posteriormente, a partir das constatações verificadas nesse caso, buscar-se-á depreender quais medidas minimizadoras dos eventuais problemas identificados deverão constar nas proposições legislativas voltadas para a formação de um marco regulatório que verse sobre o tratamento de dados pessoais na segurança pública e na persecução penal.

Para tanto, a pesquisa se guiará por estratégia de estudo de caso, com abordagem qualitativa, e será amparada pelo referencial teórico atual (revisão bibliográfica e documental)

---

[4] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: III - realizado para fins exclusivos de: a) segurança pública; (...) d) atividades de investigação e repressão de infrações penais.

[5] Para os fins deste trabalho, entende-se como "segurança pública" a atividade do estado voltada à prevenção ou diminuição de riscos do cometimento de crimes, enquanto "persecução penal" é a atividade estatal desenvolvida num momento posterior ao cometimento dessas condutas, composta pela apuração da ocorrência do delito por meio de atos de investigação praticados por órgãos policiais, e, ainda, pelo processo criminal, no qual são praticados atos judiciais voltados à aplicação das penas correspondentes às infrações penais previstas em lei (Pereira, 2021).

[6] "É possível – e até esperável – que no decorrer da observação apareçam novos elementos, inesperados, que levem a modificar as hipóteses iniciais e/ou a gerar novas hipóteses, ensejando assim a vertente indutiva da produção de conhecimento". (Cappi, 2017, p. 428).

atinente ao tema e pela consulta ao teor da ACP nº 1010667-97.2022.8.26.0053 no sítio eletrônico do TJSP.

No primeiro capítulo, será delineado o contexto de surgimento e os aspectos técnicos mais relevantes sobre o reconhecimento facial, ressaltando-se, no ponto, seu funcionamento, o grau de difusão no Brasil e no mundo, bem como os riscos de sua utilização na política de segurança pública.

No segundo capítulo, a atenção se volta para os riscos da utilização desmedida do reconhecimento facial sobre direitos fundamentais na persecução penal, especialmente se utilizado como elemento probatório. Isso porque, essa tecnologia, ao contrário de uma solução para os atuais problemas dos métodos de reconhecimento de pessoas existentes, tem se revelado como um potencial instrumento de atualização das mazelas que maculam nosso sistema penal.

Por derradeiro, no terceiro capítulo, visa-se analisar o caso da implementação do reconhecimento facial no metrô de São Paulo, e, a partir da identificação dos possíveis riscos decorrentes desse uso, verificar de que maneira as proposições de regulamentação hoje existentes no país encetam caminhos para a superação da problemática.

Capítulo 1: Aspectos técnicos do reconhecimento facial: funcionamento da tecnologia baseada em inteligência artificial e o risco de seu uso na segurança pública

> (...) hoje, a Ciência, no sentido antigo, quase deixou de existir.
> Em *Novalíngua* não há nenhuma palavra para "Ciência".
> O método empírico de pensamento, no qual todas as conquistas científicas do passado foram fundadas, se opõe aos princípios mais fundamentais do *Socing*.
> E até mesmo o progresso tecnológico só acontece quando seus produtos podem de alguma forma ser utilizados para a diminuição da liberdade humana.
>
> - *George Orwell, 1984*

À medida em que descreveu o mundo distópico explorado pelo protagonista Winston Smith no livro intitulado "1984", George Orwell (2009) retratou uma realidade na qual o poder e a tecnologia caminhavam juntos. No enredo, o governo autoritarista do *big brother*, alegoria do que seria um cruel ditador, podia antever cada movimento de Winston por meio de um sistema de vigilância onisciente denominado "teletela", que nunca podia ser desligado.

De modo semelhante, presenciamos, na realidade, uma proliferação de novidades tecnológicas capazes de realizar o monitoramento do comportamento humano com a finalidade precípua de manutenção da ordem e controle de padrões desviantes no cotidiano social.

É o caso da tecnologia de reconhecimento facial, que tem se apresentado como ferramenta moderna de poder no contexto da segurança pública.

Sua utilização em espaços públicos nos quais uma grande massa de pessoas transita diariamente tem acentuado a preocupação de estudiosos a respeito dos riscos que seu emprego pode representar para direitos fundamentais, como a privacidade, a presunção de inocência e a não discriminação.

Veremos que os processos de tomada de decisão mecanizados e inerentes ao reconhecimento facial se valem de um complexo e nada transparente sistema de inteligência artificial desenvolvido por grandes empresas do ramo da tecnologia, o que tem provocado uma legítima preocupação com as repercussões jurídicas e sociais de tal instrumento.

Assim, neste primeiro capítulo, busca-se dar contornos ao reconhecimento facial enquanto objeto de estudo explanando um panorama geral a respeito de seu surgimento no

contexto da quarta revolução industrial, bem como de seu funcionamento, das vantagens e dos riscos de sua utilização direcionada para a segurança pública.

Ademais, serão apresentados, sem pretensão de esgotamento, os cenários nacional e internacional de implementação e regulamentação do reconhecimento facial para fins de segurança pública, a fim de demonstrar que, na maioria dos países, o uso precoce da referida tecnologia tem culminado numa série de erros de identificação e em violações de direitos de populações historicamente discriminadas.

1.1 Apontamentos sobre a evolução tecnológica no contexto da quarta revolução industrial

A partir do surgimento do modelo capitalista de mercado, houve a superação da agricultura enquanto principal meio de prática comercial e a inauguração de uma sociedade industrial, ponto a partir do qual a utilização de máquinas a vapor (primeira revolução) e o aprimoramento do emprego da energia (segunda revolução) representaram o desenvolvimento da exploração dos meios de produção.

Já no contexto subsequente à Segunda Guerra Mundial, a humanidade presenciou um grande avanço na produção tecnológica (terceira revolução), ponto em que surgiram os computadores e a *internet*, no que se entendeu como uma ruptura com a sociedade industrial e a formação de uma sociedade pós-industrial (Bioni, 2019).

O mencionado processo histórico de evolução da economia é pano de fundo para o que, nos dias atuais, tem-se denominado como quarta revolução industrial.

De acordo com Klaus Schwab (2016), trata-se de uma verdadeira era informacional, marcada pela sofisticação das primeiras tecnologias digitais desenvolvidas no final do século XX em escala mundial, bem como pela diminuição dos dispositivos físicos e aumento da velocidade no processamento e armazenamento de dados, permitindo-se, assim, o limiar de processos complexos de conversão de leitura de informações por computadores em produtos e serviços.

Nos dizeres de Bioni (2019, p. 34), inaugurou-se um tempo no qual a informação é o elemento "estruturante, que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial".

É nesse contexto que *softwares* capazes de armazenar informações em quantidades cada vez maiores, como o GPS e aplicativos de comunicação (redes sociais), além de *hardwares*, como câmeras e *smartphones*, geraram, a preço relativamente acessível, facilidade e produtividade sem precedentes aos usuários.

Essa intensificação do uso/dependência da tecnologia pelo ser humano se deve, em grande medida, à mencionada sofisticação dos elementos digitais até então existentes, que passaram a integrar um conjunto de instrumentos e serviços denominado Internet das Coisas (*Internet of things*- IoT), um "mundo" digital composto por máquinas marcadas pela conectividade, capacidade de armazenamento de dados em grande escala e uso de sensores (Magrani, 2019).

Foi a partir das inovações inerentes à IoT que o volume, a velocidade e a variedade de dados digitais contidos em dispositivos tecnológicos passaram a crescer de maneira exponencial, em um fenômeno denominado como *big data*[7] (Bioni, 2019).

O aumento de dados nessas três dimensões demandou, como já dito, a criação e o aprimoramento dos instrumentos tecnológicos, com o objetivo de processar, armazenar e compartilhar dados de forma integrada para as mais diversas finalidades, desde o desbloqueio de telas de aparelhos celulares, até a condução robotizada e autônoma de veículos automotores (Marques, 2021).

Nesse ponto, a principal maneira encontrada pelas grandes corporações do ramo da tecnologia para a otimização desse complexo processo foi o desenvolvimento do chamado "algoritmo". Segundo o entendimento de Magrani (2019, p. 18), trata-se de uma "sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa" de forma automatizada por uma máquina, o que antes só poderia ser realizado por humanos.

Em breve síntese, esse processo funciona como uma espécie de "emancipação" do dispositivo - ou rede de dispositivos - tecnológico em relação ao usuário quanto a determinadas operações que, antes, sem a intervenção humana direta, não seriam possíveis de acontecer. É o caso, por exemplo, de sistemas de tecnologia doméstica, como o robô Alexa, que, por meio de comando de voz, é capaz de solucionar determinadas tarefas, como acender as lâmpadas da residência que estejam a ele integradas.

[7] De acordo com Ricardo Bioni (2019, p. 58), o *Big Data* é compreendido a partir da ideia de volume, velocidade e variedade. E explica: "Volume e variedade, porque ele excede a capacidade das tecnologias "tradicionais" de processamento conseguindo organizar quantidades antes inimagináveis – dos bits aos *yottabytes* – e em diversos formatos – e.g., textos, fotos etc. – e, tudo isso, em alta velocidade".

Vê-se, assim, que o que ocorre é um verdadeiro aprendizado por parte da máquina (*machine learning*)[8] dotada de sistemas de inteligência artificial.

Tais sistemas têm a capacidade de realizar, de forma automatizada, um processo lógico-indutivo semelhante ao utilizado pelo cérebro humano para obter conclusões gerais a partir de fenômenos particulares.

Isso se dá, no caso das máquinas, pela leitura de alguns exemplos ou problemas a ela apresentados por indutores externos, e, a partir de um processo de análise dos atributos contidos em cada situação apresentada, o sistema passa a ter a capacidade de chegar a determinadas conclusões de forma automática, realizando operações de classificação e identificação de outras amostras antes desconhecidas (Monard; Baranauskas, 2003).

Todo esse arcabouço digital baseado em *big data*, inteligência artificial, internet das coisas (IoT), dentre outros eventos inovadores, representou, ademais, um fenômeno de substituição de trabalho humano por ativos digitais, como robôs e algoritmos, numa verdadeira "terceirização" de empregos e serviços (Schwab, 2016).

Para além do impacto desse movimento no mercado de trabalho, com a diminuição de tarefas praticadas por humanos que as máquinas podem realizar a menor custo, observa-se, ainda, que o avanço tecnológico trouxe consigo a noção generalizada de que as novas ferramentas e sistemas de inteligência estariam associados, automaticamente, à ideia de eficiência, neutralidade e precisão.

Tais qualidades, assim, seriam perfeitas para resolução de problemas complexos, como o diagnóstico de doenças, o aprimoramento de ofertas aos consumidores no comércio e a otimização da prestação de serviços por parte do Estado (Fernandes; Resende, 2023).

Outrossim, o referido imaginário foi impulsionado pelas grandes corporações do ramo da tecnologia (Kremer; Nunes; Lima, 2023), bem como por discursos e criações da mídia *mainstream*, gerando grande especulação em torno da capacidade humana de transformar em realidade as - não tão irrealistas - tecnologias vistas nos filmes e livros de ficção científica.[9]

[8] "Um sistema de aprendizado de máquina "é um programa de computador que toma decisões baseado em experiências acumuladas através da solução bem sucedida de problemas anteriores". (Monard; Balanauskas, 2003, p. 39).

[9] No filme Missão Impossível - Nação Secreta, o quinto da franquia, o protagonista Ethan Hunt, estrelado por Tom Cruise, se depara com a necessidade de investigar o Sindicato, uma organização criminosa formada por agentes de inteligência desonestos. Em determinada cena, o agente se vale de um desenho feito à mão de uma mulher para que um sistema de reconhecimento facial identificasse seu paradeiro em tempo real. Embora inexistente um modelo de RF tão avançado na realidade, o emprego ficcional da tecnologia contribui para a formação de um imaginário quanto à capacidade de a tecnologia solucionar problemas considerados "impossíveis".

De fato, a partir do surgimento do algoritmo, tornou-se comum que usuários da internet tenham suas experiências digitais (preferências de pesquisa e conteúdo) antevistas pela própria máquina, em verdadeira prognose acerca do que o usuário provavelmente pensará e fará durante o uso. Como exemplo, não é difícil encontrar propagandas pré-direcionadas de produtos e serviços *on-line* a serem adquiridos por consumidores.

Essa materialização de cenários inimagináveis há alguns anos atrás também culminou na inauguração de uma nova fase do capitalismo, denominado por Zuboff (2020) como "capitalismo de vigilância".

A partir desse marco, foi possível notar uma densificação da retórica de presunção de "infalibilidade" e confiabilidade do aprendizado de máquina e das decisões dele decorrentes, o que é de grande interesse para os agentes capitalistas de vigilância - como *big techs* e desenvolvedores de IA. Afinal, tais empresas têm obtido grandes lucros com a aquisição e tratamento de dados[10], predominantemente pessoais, enquanto fonte de alimentação e treinamento de sistemas de inteligência artificial (Zuboff, 2020).

Nota-se, assim, que o processo de evolução da arquitetura dos processos automatizados de decisão baseados em dados tem se aproximado de uma visão utilitarista (com viés mercadológico e de poder) por trás de sua difusão na sociedade, na qual se encontra usurpado ou mitigado o controle por parte dos titulares de dados, que terão suas informações, por vezes, utilizadas pelos detentores da criação e manutenção das novas tecnologias para fins pouco claros. Há, assim, um desdobramento ético acerca do avanço digital que não pode ser ignorado.

Embora sistemas de inteligência artificial possam aparentar, num primeiro momento, certas vantagens relativamente à objetividade quando comparados com decisões humanas, a prática tem evidenciado uma série de erros e consequências por parte desses sistemas que geram questionamentos acerca da suposta imparcialidade e precisão pela mitigação do subjetivismo humano em seu processo decisório.

Nesse ponto, Wimmer e Doneda (2021, p. 383) asseveram que tais tecnologias não estão livres de adaptações durante treinamentos por parte de programadores, o que pode se traduzir num processo de ajustamento da IA a critérios utilitaristas ou instrumentalizados.[11]

[10] De acordo com o art. 5°, X, da Lei Geral de Proteção de Dados (Brasil, 2018), tratamento de dados é a "operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

[11] Tal apontamento se sintoniza com a ideia de Zuboff (2020, p. 23) a respeito do surgimento de um poder instrumentário na era do capitalismo de vigilância, que, por meio dos processos de aprendizado de máquina, "conhece e molda o comportamento humano em prol das finalidades de terceiros".

Assim, valem as dúvidas sobre a suposta inexistência de subjetivismo nas tecnologias guiadas por algoritmos.

Isso porque, considerando que a tradução de dados em decisões automatizadas por parte de algoritmos passa pelo aprendizado a partir de amostras de elementos de determinada realidade apresentada à máquina dotada de tal tecnologia, é possível concluir que os resultados poderão refletir, em alguma medida, problemas inerentes à própria sociedade que a utiliza[12]. Assim, "não haverá resultado sem viés ou livre de preconceitos em uma sociedade que se coloca, a todo o tempo, ao contrário disso" (Garcia; Duarte, 2021, p. 200).

É nesse quadro de expansão de formas complexas de tecnologia que emerge o reconhecimento facial. Não obstante sua importância na atualidade em diversas frentes, veremos, a partir da explanação sobre sua história e características, que o referido sistema possui uma dimensão problemática quando empregado na identificação biométrica em contexto de apuração de ilícitos penais.

1.2 Histórico, conceito e funcionamento do reconhecimento facial: erros de acurácia e enviesamento na tomada de decisões automatizadas

Cumpre dar contornos ao reconhecimento facial enquanto principal objeto de estudo, a fim de que, partindo de um panorama a respeito de seu limiar, funcionamento, finalidade, vantagens e riscos, seja possível entender melhor se sua utilização direcionada para a segurança pública no espaço público do metrô de São Paulo poderá culminar em uma intensificação da violação de direitos fundamentais no âmbito da persecução penal.

Considerando que as tecnologias baseadas em IA que emergiram na conjuntura da quarta revolução industrial possuem como característica principal a dependência de dados pessoais para o treinamento de algoritmos, destaca-se que, dentre tais tecnologias, algumas representam mais riscos aos direitos dos usuários. É o caso das que se valem de técnicas de processamento de dados pessoais sensíveis[13] para o aprendizado de máquina.

[12] Por essa razão, Tarcísio Silva (2022, p. 66) explica que, com as inovações tecnológicas, o racismo estrutural na sociedade ganhou uma nova camada: o racismo algorítmico. Esse, por sua vez, é compreendido como o "modo pelo qual a disposição de tecnologias e imaginários sociotécnicos em um mundo moldado pela supremacia branca realiza a ordenação algorítmica racializada de classificação social, recursos e violência em detrimento de grupos minorizados".

[13] De acordo com Ribeiro e Fermentão (2023), a distinção entre dados pessoais e dados pessoais sensíveis é relevante na medida em que estabelece o grau de proteção que as informações sobre determinada pessoa física devem ter de eventual legislação regulamentadora. No caso brasileiro, a LGPD distinguiu dados pessoais como toda informação relativa a uma pessoa física já identificada ou identificável (art. 5º, I), enquanto dado pessoal sensível é conceito específico, que envolve, sobretudo, informações atinentes à individualidade de cada pessoa

Merece atenção a utilização, nesse processo, da biometria. Trata-se de vertente de dado sensível que, sendo objeto de análise por parte de sistemas tecnológicos capazes de mensurar atributos biológicos, permite o reconhecimento de um sujeito (Duarte *et al*., 2021).

Tal verificação pode ser repartida em técnicas de naturezas variadas, a exemplo do recolhimento de material genético (DNA) em impressões digitais e o reconhecimento de voz, assinaturas, retina e da face, aspectos que possuem padrões únicos em cada ser humano (Pinho, 2024).

Dentre as técnicas supramencionadas, ganha destaque a análise facial automatizada por meio de tecnologia de reconhecimento facial. Trata-se de um *software* que, valendo-se de algoritmos matemáticos treinados com aprendizado de máquina, é capaz de detectar, classificar e identificar aspectos da face humana por meio do cruzamento de características biométricas obtidas com o uso de *hardwares*, como drones e câmeras de videomonitoramento CCTV (*Closed Circuit Television*), com um banco de dados (Buolamwini; Gebru, 2018; Paganoni, 2019).

Para Adjabi, *et al* (2020), diferentemente de outros vetores biométricos, a face humana possui vantagens que a tornam mais apropriada ao reconhecimento de identidades, uma vez que: a) imagens do rosto, em contraste com impressões digitais ou reconhecimento da íris, podem ser obtidas rapidamente e sem contato físico; e b) o reconhecimento facial requer menos assistência do usuário em comparação com os demais métodos, como o reconhecimento de voz, em que o sujeito precisa falar.

Nesse ponto, os dados sensíveis "que as tecnologias digitais e as respetivas bases (de dados) recolhem e arquivam são, cada vez mais, da ordem da imagem, com destaque para as imagens dos nossos rostos" (Melo; Serra, 2022, p. 210).

Embora o presente trabalho tenha partido de uma exposição sobre as novas tecnologias baseadas em IA no paradigma da quarta revolução industrial, importa dizer que o surgimento dos estudos em torno do reconhecimento facial nos remete para a década de 1960, período em que se deram as primeiras tentativas de automatização de procedimentos de análise da face humana.

Com o incentivo da CIA (*Central Intelligence Agency*), os pesquisadores norte-americanos Woodrow Bledsoe, Charles Bisson e Helen Wolf (à época, funcionários da *Panoramic Research*) foram pioneiros ao desenvolverem um método de visão

física, como origem étnica ou racial, opinião política, dados genéticos ou biométricos, dentre outros fatores (art. 5º, II).

computacional[14] que, por meio de um algoritmo treinando para realizar a medição das distâncias entre pontos faciais presentes em fotografias - largura da boca, distância entre os olhos, pupila, etc. -, realizava a associação de cada coordenada à fotografia de determinado indivíduo registrado em uma coleção de rostos de criminosos num banco de dados[15] (Nilsson, 2009; Gates, 2011).

Posteriormente, com financiamento por parte do Departamento de Defesa dos Estados Unidos, que visava o avanço científico-militar no contexto da guerra fria, novos estudos buscaram aprimorar os resultados até então obtidos (Gates, 2011). Contudo, o desenvolvimento esbarrou, por muitos anos, na limitada tecnologia informática disponível, bem como no fato de que o reconhecimento facial se baseava em uma quantidade limitada de fotos com padrão de angulação, expressão e iluminação que dificultavam a evolução do aprendizado de máquina (Nilsson, 2009).

A partir dos anos 1990, os sistemas protótipos começaram a tomar forma em razão de dois fatores principais. Primeiro, em razão do afastamento da produção da TRF para aplicações militares e de sua comercialização em *softwares* por empresas (Visionics, Viisage e Miros Inc.), e, segundo, pela ampliação do acesso a bancos de dados com fotografias mais extensos para servirem de referência para pesquisas, a exemplo do FERET (*Facial Recognition Technology*), desenvolvido pelo governo dos EUA em 1996.[16][17]

Em que pese o aumento na diversidade de conjuntos de dados, a permanência do método de visão computacional baseado em fotos de faces frontais ou de lado (Hirata Jr; Araújo; Abello, 2021) impediu que a precisão dos algoritmos de reconhecimento fosse otimizada no período.

Foi apenas com o advento da era da *big data* e a superação dos antigos métodos de visão computacional que um novo critério foi desenvolvido: o *DeepFace* (face profunda).

[14] "Área da inteligência artificial voltada a utilizar imagens, vídeos e sinais de sensores imagéticos para emular a capacidade de visão humana, realizando tarefas como reconhecer e detectar objetos, facilitar interação de sistemas com humanos e permitir a mobilidade e atuação de robôs". (Fernandes, *et a*l., 2024, p. 1).

[15]Nunes (2023, p. 38) associa o banco de dados utilizado pelos pesquisadores com os álbuns de suspeitos, hoje usados nas delegacias policiais do Brasil.

[16] O interesse do governo norte-americano pela face enquanto dado biométrico cresceu nesse período, levando-o a dar início ao financiamento de projetos de criação de bancos de dados, a exemplo do FERET, que serviu como fonte de referência para comparação entre algoritmos de reconhecimento facial e como forma de dar início à aplicação do aprendizado de máquina em visão computacional. O incentivo dos EUA ao desenvolvimento do reconhecimento facial perdura até os dias atuais por meio do *National Institute of Justice* (NIJ), vinculado ao Departamento de Justiça.

[17] Outra iniciativa do governo dos EUA foi a promoção do *Face Recognition Grand Challenge* (FRGC), uma grande competição realizada entre maio de 2004 e março de 2006 que reuniu diversos pesquisadores para a experimentação de protótipos de novas técnicas e sistemas de TRF. (Estados Unidos da América, 2024).

Criado em 2014 em consequência do trabalho de pesquisadores do *Facebook Research*, o *DeepFace* é um algoritmo baseado em redes neurais profundas[18], entendidas como unidades simples de processamento interconectadas (daí a associação com o "neurônio") que simulam a função cerebral humana e permitem o aprendizado autônomo de um computador (Gates, 2011, p. 50).

Uma vez que os criadores do *DeepFace* tinham à sua disposição um banco de dados gigantesco de fotos de usuários do *Facebook*,[19] tornou-se possível, enfim, um processo de modelagem em 3D das faces contidas nas imagens e de detecção de profundidade capaz de analisar, tridimensionalmente, características biométricas adicionais antes inviáveis, como contornos e dimensões (Hirata Jr; Araújo; Abello, 2021; Faceonlive, 2023). Assim, parâmetros como a precisão e a eficiência da tecnologia foram otimizados de forma nunca antes vista[20].

Delineado brevemente o estado da arte, cabe agora apresentar o funcionamento do reconhecimento facial, a fim de que possamos compreender melhor os fatores que tem despertado a preocupação de especialistas no tema a respeito de erros de reconhecimento, e, assim, dimensionar o seu impacto em situações reais e em garantias fundamentais.

Embora existam outras formas de classificação mais ou menos detalhadas, de modo geral, o sistema de reconhecimento facial pode ser dividido em quatro etapas principais, podendo cada uma delas ocorrerem de uma vez, ou não.

Tais fases podem ser definidas da seguinte maneira: a) detecção de rosto, passo em que uma imagem ou vídeo são obtidos pelo *hardware* (geralmente câmeras de vídeo) e o algoritmo analisa se existem faces humanas; b) normalização facial, que representa a padronização ou correção de pontos de referência da face em termos de tamanho, pose, iluminação, etc. em relação às imagens contidas num banco de dados; c) extração de recursos ou atributos, que se dá quando o algoritmo observa os componentes faciais possivelmente existentes no rosto detectado de modo a estabelecer um vetor (representação matemática)

[18] Podem ser entendidas como categoria do chamado *deep learning* (aprendizado profundo). Este, por sua vez, é definido como uma técnica pertencente à classe de *machine learning* (aprendizado de máquina): "*Deep learning, belonging to a machine learning class, employs successive hidden-layers of information processing levels, hierarchically organized for representation or pattern classification, and feature learning*" (Adjabi, *et al*., 2020, p. 22).

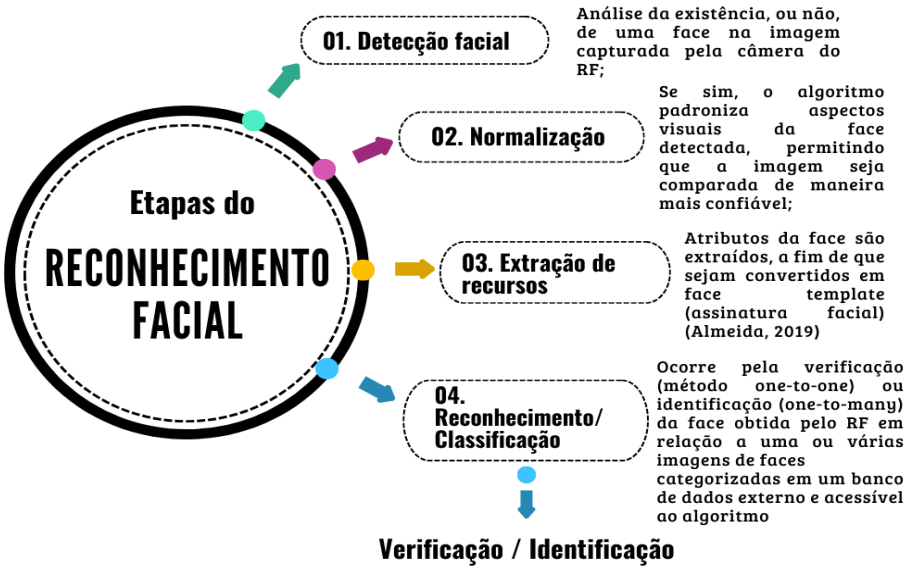
[19] Obtidas, inicialmente, sem o consentimento do usuário, o que só passou a ser solicitado após o ajuizamento de ação coletiva versando sobre violação da privacidade do usuário com o *DeepFace* (Paganoni, 2019).

[20] Cabe ressalvar, no entanto, que o aprimoramento do reconhecimento facial e aumento em taxas de acerto apresentadas atualmente são decorrentes, na maioria das vezes, de cenários ideais em testes controlados (Oliveira, *et al*., 2020), o que não afasta, como se demonstrará oportunamente com pesquisas sobre performance e exemplos reais, que a tecnologia ainda não foi capaz de atingir um patamar seguro para utilização em ambientes públicos, e, muito menos, para fins de segurança pública.

denominado assinatura facial (*face template*), baseado em individualidades do rosto que permitam o cotejo com outro; e d) reconhecimento ou classificação (Introna, Nissenbaum, 2009; Adjabi, *et al*., 2020; Almeida, 2022).

Essa última etapa pode se dar por meio de verificação[21], que é o exame da correspondência de uma face detectada pelo RF com uma outra, associada a informações sobre um indivíduo, em um banco de dados preexistente - *one-to-one*, ou identificação, forma mais comum de reconhecimento empregado para vigilância pública, que realiza a comparação da face com imagens de várias outras, também vinculadas a dados pessoais, e que gera possibilidades diversas para a localização da identidade do rosto sob análise - *one-to-many* (Lambert, 2021). A divisão pode ser ilustrada com base na Figura 1:

Figura 1: Etapas do reconhecimento facial.



Fonte: Elaborado pelo autor com base em Introna; Nissenbaum, 2009; Adjabi, *et al*., 2020; Almeida, 2022; e Lambert, 2021.

A arquitetura de funcionamento do reconhecimento revela, assim, um complexo conjunto de operações automatizadas que envolvem o tratamento de dados pessoais sensíveis relativos ao rosto humano.

O resultado dessas etapas culmina, por derradeiro, em resultados probabilísticos (em termos de porcentagem) em torno do grau de semelhança que determinadas características de uma assinatura facial possui com outras em bancos de dados externos a tal processo, de modo

[21] Um exemplo de verificação por reconhecimento facial é o Face ID dos smartphones da Apple, que compara a face do usuário em frente à câmera com aquela registrada no banco de dados do dispositivo.

que não há um resultado binário (sim ou não) acerca da correspondência entre a face capturada e as demais (Big Brother Watch, 2018).

Cabe dizer que, especificamente no caso do reconhecimento facial, o desenvolvedor realiza um treinamento supervisionado do algoritmo nele existente para que consiga identificar as informações de uma face, o que se dá "a partir da análise repetitiva de bases de dados pré-rotulados (i.e., milhões de exemplos de rostos humanos retirados de redes sociais)" (Duarte; Ceia, 2023, p. 18).

Dado o avanço em testes em ambientes controlados e o desenvolvimento de novos métodos de aprendizado de máquina, poder-se-ia presumir, com certa tranquilidade, que os resultados acerca da precisão e eficiência da tecnologia de RF, hoje disseminada em diversos aparelhos no universo da IoT, são seguros, e a "superioridade algorítmica" seria apenas um reflexo do sucesso científico (Silveira, 2020).

Quanto à confiabilidade de seu emprego na segurança pública, a visão de Relly Petrescu (2019) é no sentido de que a TRF mitiga criminosos nas ruas e previne crimes antes que tenham chance de acontecer. Isso porque, a possibilidade de se conferir a presença de um indivíduo numa lista de suspeitos ou procurados antes de medidas coercitivas poderia reduzir a discriminação de gênero, raça e idade, tornando mais transparente e objetiva a tomada de decisão sobre a oportunidade da intervenção.[22]

De fato, o algoritmo do reconhecimento facial não é capaz, por si, de abordar uma pessoa, e, tampouco, de instaurar processos de investigação ou denunciar alguém perante a justiça, deliberações que são eminentemente humanas e devem estar ancoradas na legislação que regulamenta procedimentos de natureza processual penal.

Contudo, em virtude do aprendizado de máquina, que permite padrões decisórios automatizados, a TRF pode chegar à determinada conclusão em torno da probabilidade de a face de um transeunte ser, ou não, a de um criminoso, contida em banco de informações. Essas informações, por sua vez, possuem o risco de estarem repletas de vieses (*bias*) discriminatórios e imprecisões derivadas do processo de aquisição e processamento dos dados pessoais sensíveis, o que pode direcionar ou induzir os agentes que terão em mãos as conclusões obtidas com a tecnologia.

[22] No entanto, a própria autora ressalva que, diferentemente de outros sistemas biométricos, o reconhecimento facial tem apresentado o maior número de falsos positivos/negativos, o que se dá por fatores técnicos, como iluminação, expressão, ruído de imagem, dentre outros aspectos que podem afetar o desempenho da tecnologia quando empregada, por exemplo, na segurança ferroviária e em aeroportos (Petrescu, 2019).

O mencionado risco de "contaminação" do reconhecimento facial não se trata de mera especulação.

Isso porque a acurácia do sistema de reconhecimento facial pode passar por fatores de distorção de duas naturezas: i) técnicos, como angulação, iluminação, ruídos de imagem, variações de pose da cabeça, etc., o que dificulta a localização das fases de detecção, normalização e extração de pontos de referência da face (Introna; Nissenbaum, 2009), ii) estruturais, que dizem respeito à fatores sociais e históricos preexistentes e que influenciam a fiabilidade do sistema. Nesse último caso, "a subjetividade do programador se expressa no funcionamento da tecnologia e essa interação pode reproduzir os preconceitos de classe, raça e gênero daquele" (Castro; Arguello; Cosate, 2022, p. 94).

Buscando constatar a possibilidade de incidência das mencionadas distorções no reconhecimento facial, desde os anos 2000 o Departamento de Defesa dos EUA, em parceria com o *National Institute of Standards and Technology* (NIST), passou a realizar estudos e testes de acurácia[23] nos diversos programas de reconhecimento facial existentes naquele país (Nunes, 2022).

Trata-se do *Face Recognition Vendor Test* - FVRT (Teste de Fornecedores de Reconhecimento Facial), um programa do governo norte-americano, que financia pesquisas e o desenvolvimento de algoritmos, recebe projetos de desenvolvedores voluntários e avalia o desempenho das inovações por meio de um *feedback* (Estados Unidos da América, 2024).

Em testes controlados realizado em 2018, o NIST verificou que houve um aumento de qualidade nas taxas de erros no reconhecimento facial a partir de 2013, quando do surgimento do método de redes neurais convolucionais de aprendizagem profunda (*deep learning*), o que possibilitou a realização de correções mais avançadas em variações de brilho, ruído e outros aspectos nas imagens detectadas (Duarte, *et al.,* 2021).

Em que pese o aumento na precisão dos sistemas mais recentes, em 2019, no último teste realizado, o NIST avaliou o desempenho de 189 algoritmos, desenvolvidos por 99 desenvolvedores diferentes.

Na oportunidade, observou-se que as taxas de erro na verificação/identificação de faces apresentaram problemas quando levado em conta fatores demográficos, como raça, etnia, sexo e idade, sendo que as taxas de falsos positivos[24] para homens brancos e mulheres

[23] "Acurácia, em termos gerais, é a medida utilizada para avaliar o quão eficiente o *software* é em correlacionar corretamente a mesma face e de apontar quando as faces comparadas não pertencem a mesma pessoa. Chamamos esses casos de 'positivo verdadeiro' e 'negativo verdadeiro', respectivamente" (Nunes, 2021, p. 39).

[24] No contexto do reconhecimento facial, é relevante a explicação de Milanez (2024, p. 99) sobre os conceitos técnicos de falso negativo e falso positivo: "Um falso negativo ocorre quando o sistema não consegue realizar

negras variaram por fatores de 10 a mais de 100, ou seja, o algoritmo com desempenho mais baixo no reconhecimento de homens brancos poderia ser 100 vezes mais preciso do que em rostos de mulheres negras (Lambert, 2021).

Outra famosa análise de precisão de sistemas de RF é a de Joy Buolamwni, do MIT Media Lab, e Timnit Gebru, do Google Research[25]. Em 2020, as pesquisadoras criaram um banco de dados de referência (*Pilot Partiament Benchmark* - PPB) autônomo e balanceado[26] contendo imagens de parlamentares negros e brancos de seis países e que foram objeto de identificação por parte de sistemas de análises faciais de empresas como Amazon, Microsoft e Clarifai.

À semelhança dos testes do NIST - embora as autoras tenham utilizado um banco de dados mais diversificado em relação à raça e gênero - as maiores taxas de erro de identificação por parte dos classificadores também se direcionaram às mulheres negras, com índice de falsos positivos de até 34,7%, enquanto o índice para homens de pele mais clara foi de 0,8% do total (Buolamwini; Gebru, 2018).

É possível notar, assim, que mesmo em testes controlados e se valendo de novos métodos de aprendizado de máquina mais modernos e capazes de processar dados em quantidades cada vez maiores, os algoritmos de reconhecimento facial podem não ser tão neutros ou eficazes como se imagina. Nesse sentido, "para as tecnologias da informação e da comunicação também é preciso questionar se tudo o que é tecnicamente possível é socialmente e politicamente aceitável, eticamente admissível, juridicamente lícito" (Rodotà, 2008, p. 142).

Realizando releitura do estudo de Suresh e Guttag (2019), Ruback, Ávila e Cantero (2021) trouxeram ao debate quatro vertentes relevantes de vieses em aprendizado de máquina e que dão um panorama sobre as diversas frentes em que o processo de reconhecimento facial pode traduzir discriminação e violação de direitos.

---

um *match* entre um rosto e uma assinatura facial constante em um banco de imagens preexistente, apesar de tal rosto já estar em referida base (...). Já o falso positivo verifica-se quando o sistema associa um rosto a uma assinatura facial de uma base de imagens preexistentes de forma errônea. Isto é, apesar de o rosto não possuir uma correspondência no banco de imagens, o sistema acusa equivocadamente que sim, causando, por exemplo, a detenção de indivíduos inocentes".

[25] Para mais detalhes, recomenda-se o documentário "*Coded Bias*", produzido em 2021 pela Netflix com base no estudo das pesquisadoras.

[26] A construção de um bando de dados de referência para o teste que fosse mais representativo em aspectos fenotípicos e de sexo se deu em virtude da predominância, nos parâmetros de análise facial usualmente utilizados (como IJB-A e Adience), de faces de pessoas brancas, (79,6% para IJB-A e 86,2% para Adience) (Buolawmini, Gebru, 2018).

Na coleta de dados, em que são utilizados dados preexistentes para criação e treinamento do sistema, vieses históricos (i), como o racismo estrutural[27], podem repercutir na construção de bancos de dados para treinamento desbalanceados, o que, por conseguinte, desencadeia um desequilíbrio na representatividade (ii) da população de amostra, e, assim, maiores chances de erro no caso de grupos subrepresentados (Ruback; Ávila; Cantero, 2021).

Já no momento de teste do sistema da TRF, se o modelo é avaliado a partir de dados de teste ou referência geralmente não representativos, o resultado da análise tende a ter vieses de avaliação (iii), que, além disso, também são resultado da seleção de métricas que refletem, conforme a opinião ou crença do analista, melhores desempenhos, excluindo-se, assim, uma verificação dividida por grupos e crítica.[28]

Por fim, a interpretação humana (iv) do resultado obtido, como, por exemplo, a identificação de um suspeito, também pode infiltrar vieses no processo de tomada de decisão, o que se dá pela "incompatibilidade entre o problema que o modelo se propôs a resolver e a forma em que ele é usado na prática" (Ruback; Ávila; Cantero, 2021, p. 10).

Análises de precisão como as supracitadas têm revelado que nem mesmo a melhoria dos dispositivos de *hardware*, o surgimento de formas mais complexas de aprendizado de máquina (*deep learning*, etc.) e a criação de testes de avaliação - que, ainda que bem intencionados, podem não refletir a realidade - tem afastado os sistemas de reconhecimento facial de uma conclusão inexorável no cenário atual: o risco de projeção, em seu uso, de desigualdades sociais e violação de direitos fundamentais.

A seguir, veremos como a TRF tem sido implementada em espaços públicos no Brasil e no mundo para fins de segurança pública e em que medida seu uso despertou processos de discussão político-jurídica sobre uma regulação que mitigue seu uso indiscriminado.

1.3 Panorama internacional e nacional do reconhecimento facial em ambientes públicos: uma utilização que antecede o debate

[27] "O racismo é uma decorrência da própria estrutura social, ou seja, do modo "normal" com que se constituem as relações políticas, econômicas, jurídicas e até familiares, não sendo uma patologia social e nem um desarranjo institucional. O racismo é estrutural. Comportamentos individuais e processos institucionais são derivados de uma sociedade cujo racismo é regra e não exceção". (Almeida, 2019, p. 33).

[28] "Por exemplo, um modelo de reconhecimento facial pode ter uma precisão geral de 80%, mas se formos considerar a precisão dentro do grupo que inclui mulheres negras, a precisão cai para 60%, enquanto que a precisão dentro do grupo que corresponde a homens de pele clara, a precisão sobe para 90%" (Ruback, Ávila e Cantero, 2021, p. 10).

Como visto anteriormente, a utilização do reconhecimento facial vem tomando proporção global, sendo característica elementar, por exemplo, nos atuais modelos de *smartphones*, bem como em sistemas de autenticação bancários, localização de desaparecidos e publicidade direcionada *online* e predatória.[29]

Especificamente no caso de sistemas de RF para vigilância em espaços públicos para segurança e persecução penal, o avanço também foi considerável, o que tem levado vários países a buscar maneiras de conter a proliferação desenfreada da implementação da tecnologia sem balizas regulatórias e o aprofundamento da discussão entre gestores, empresas e a sociedade civil organizada, tudo com vistas a mitigar eventuais abusos e violações a direitos.

Dentre os casos de maior relevância se encontra a utilização, em vários departamentos de polícia no Reino Unido, do reconhecimento facial para vigilância enquanto instrumento auxiliar do patrulhamento ostensivo, o que tem ocorrido sem qualquer marco regulatório sobre o tema[30].

O uso da tecnologia no país suscitou uma série de manifestações de 26 organizações independentes de direito de minorias, igualdade racial e tecnologia em prol da suspensão imediata do uso do RF pela polícia, tendo em vista o alto potencial de impacto nos direitos de liberdade de expressão e presunção de inocência (Big Brother Watch, 2020).

Baseando-se em estatísticas fornecidas pela própria polícia, o *Big Brother Watch* - BBW (2020), uma das organizações envolvidas nas manifestações, publicou relatório sobre a precisão do reconhecimento facial da Polícia Metropolitana de Londres segundo o qual 93% das identificações foram imprecisas.

Recentemente, câmeras CCTV instaladas com a tecnologia no centro da cidade levaram a polícia a intervir em 71% dos casos de identificação errôneos e deter pessoas inocentes. Analisando o dado, o BBW apontou que o alto índice de atuação policial mesmo em casos de identificação falha pode estar ligado, justamente, à negligência quanto à existência de vieses influenciando o sistema de algoritmo, gerando, ao fim, uma presunção de veracidade que fundamentaria a intervenção policial (Big Brother Watch, 2020).

[29] Para aprofundamento na temática, ver: Zuboff, 2020, capítulo 7, I: O imperativo de predição; Silveira, 2020.
[30] Segundo a organização, embora o *The Protection of Freedoms Act 2012* tenha introduzido a possibilidade de uso de câmeras de vigilância em espaços públicos, não houve menção ao uso de reconhecimento facial em tais instrumentos, razão pela qual inexiste base legal para o uso da tecnologia pela polícia (Big Brother Watch, 2020).

No âmbito da União Europeia, ainda que os países integrantes tenham se movimentado e sido pioneiros na criação de um arcabouço normativo sobre proteção de dados pessoais (*General Data Protection Regulation* - GDPR, de 2016, e Diretiva nº 680/2016, que trata da proteção de dados no contexto da persecução penal), somente em março de 2024 houve a aprovação de uma lei pelo parlamento europeu versando especificamente sobre o uso de tecnologias de inteligência artificial que incluísse de alguma forma os sistemas de reconhecimento facial, o *AI Act*.

Na norma, seus autores buscaram estabelecer parâmetros mais claros sobre o reconhecimento facial enquanto sistema de IA.

Assim, foi estabelecido uma abordagem baseada em risco que categorizou sistemas de IA em proibidos, de alto risco, baixo risco ou risco limitado, enquadrando o reconhecimento facial, predominantemente, em aplicação de alto risco[31], sujeitando o seu uso a requisitos, como avaliações de impacto em direitos fundamentais antes de sua implementação, necessidade de consentimento prévio para uso e direito de explicação sobre uma decisão tomada pelo sistema (Zulehner, 2024).

A aprovação do *AI Act* representou um avanço na medida em que foi construído a partir de um debate sobre repercussões do uso de sistemas de IA em direitos e prerrogativas dos cidadãos europeus, embora ainda exista discussão sobre a pertinência, ou não, da regulamentação do RF em norma ainda mais específica de modo apartado.

Outro caso emblemático de uso desamparado de bases legais do reconhecimento facial com repercussões preocupantes sobre direitos fundamentais foi a utilização do RF na China.

Inicialmente implementada sem um marco regulatório ou diretrizes por parte da autoridade reguladora do governo, os sistemas de identificação facial passaram a ser massivamente utilizados por empresas e pelo estado para finalidades das mais variadas - até mesmo para ativação de dispensadores de papel higiênico em banheiros públicos (Aljazeera, 2023) [32].

Em 2023, diante de uma série de questionamentos sobre abusos e uso extremo do reconhecimento facial em várias cidades chinesas para controle social, a autoridade

[31] Embora o *AI Act* tenha listado setores de uso do sistema de IA em categorias, ressalvou-se a possibilidade de ampliar, restringir ou alterar o conteúdo da lista (artigo 7) com vistas a adaptar a norma às mudanças tecnológicas (Zulehner, 2024)

[32] Aljazeera. China drafts rules for facial recognition tech amid privacy complaints, **Aljazeera,** 8 ago 2023. Disponível em: https://www.aljazeera.com/economy/2023/8/8/china-drafts-rules-for-facial-recognition-tech-amid-privacy-complaints. Acesso em: 17 jul 2024.

reguladora (*Cyberspace Administration of China*) lançou iniciativa para colher a opinião pública acerca de medidas de regulamentação em torno do tema a nível nacional, quadro em que foram propostos requisitos acerca do consentimento dos indivíduos para coleta de dados sensíveis, finalidades mais delimitadas e medidas para coibir o acesso não autorizado ou o vazamento de dados (República Popular da China, 2023).

A medida também representou um importante avanço na medida em que, a um só tempo, incluiu a sociedade na discussão em torno dos problemas oriundos do vácuo normativo e visou à formação de um conjunto de regras que poderão servir como limites ao uso excessivo do RF no país.

Nos Estados Unidos, a ausência de normas federais regulamentando o tema fez a cidade de São Francisco abolir a tecnologia quando empregada para fins de segurança pública, medida que, posteriormente, foi efetivada por mais de uma dúzia de cidades em vários estados do país (Simonita, 2021).

O movimento também se deu em virtude de relatos de uso indiscriminado da tecnologia. Foi o caso de Robert Willians, homem negro que foi preso na frente de sua filha e de sua esposa acusado de roubo de artigos de luxo, o que se deu com base em reconhecimento falho feito por um *software* da polícia de Detroit quando da comparação de sua foto num banco de dados público com a imagem do real criminoso, obtida por meio de câmeras no local do crime (Brito, 2020).

Vê-se, assim, que, embora a tecnologia baseada em IA se torne cada vez mais difundida em diversas partes do mundo, existem movimentos e iniciativas governamentais, que, movidas pelos resultados de análises de precisão e relatos reais de erros, tem buscado maneiras de regulamentar ou até mesmo proibir seu uso quando direcionado para a segurança pública.

Embora os casos acima relatados sejam relevantes para entendermos que o reconhecimento facial empregado na segurança tem sido uma preocupação relevante a nível mundial, a repercussão sobre direitos fundamentais que o mencionado sistema biométrico pode acarretar em países constituídos a partir de processos históricos de exploração se torna ainda mais alarmante.

Particularmente no contexto latino-americano, os reflexos da colonialidade[33] enquanto elemento fundante das relações discriminatórias de poder (Quijano, 2009) se

[33] "A colonialidade é um dos elementos constitutivos e específicos do padrão mundial do poder capitalista. Sustenta-se na imposição de uma classificação racial/étnica da população do mundo como pedra angular do

desdobraram em variadas formas de mazelas sociais, gerando, assim, fenômenos como a segregação socioespacial dos marginalizados - negros, indígenas, imigrantes, etc., -, a formação de zonas de baixa renda e acesso escasso a riquezas, o crime organizado e a violência policial, dentre outros fatores que nos colocam em um plano de exercício precarizado da cidadania.

Nesse sentido, em que pese o avanço tecnológico e o acesso de países menos favorecidos a inovações como a IoT, a *big data* e demais fenômenos da era digital sejam cruciais para sua integração e desenvolvimento, merecem atenção as contingências acima referidas e em meio às quais o reconhecimento facial surge como "solução" para problemas eminentemente estruturais da sociedade[34], como é o caso da segurança pública e, em um passo adiante, do sistema penal.

A partir da problematização no caso da América Latina, vale citar um relatório divulgado em 2022 pelo Consórcio *Al Sur*. O documento apontou que, de 38 iniciativas de uso do RF em nove países (Argentina, Brasil, Costa Rica, Chile, Colômbia, México, Panamá, Paraguai e Peru), 31 empregam a tecnologia para vigilância de espaços públicos, sendo que, em mais de 60% dos casos, inexiste qualquer referência legal para apoiar a implementação (Al Sur, 2022).

No demais casos, o uso da tecnologia se ampara ou em exceções trazidas nos textos das leis gerais de proteção de dados pessoais, nos poucos países que a possuem,[35] ou em regulamentos obsoletos e não vinculantes relativos ao uso de outros tipos de câmeras de videovigilância (Franqueira, Hartmann, Silva, 2021). Assim, considerando que a sensação de insegurança demanda estratégias eficazes que contornem o problema da criminalidade, como o apelo para a utilização de sistemas de vigilância em ambientes públicos, torna-se relevante que o debate em torno da "aplicação dessa tecnologia seja acompanhada de preocupações éticas relacionadas aos possíveis processos discriminatórios e de estratificação do espaço urbano que podem surgir a partir da sua instalação" (Franqueira, Hartmann, Silva, 2021, 2021, p. 197).

---

referido padrão de poder e opera em cada um dos planos, meios e dimensões, materiais e subjectivos, da existência social quotidiana e da escala societal." (Quijano, 2009, p. 73).

[34] Vale mencionar a visão do Consórcio *Al Sur* (2020, p. 22) a respeito da utilização do RF como mecanismo de autenticação de identidade e condição para acesso a serviços públicos ou benefícios sociais, o que pode aumentar ainda mais as desigualdades estruturais na região latinoamericana: "*Finally, when implemented as identity authentication mechanisms to condition access to public services, facial recognition (as well as other biometric technologies) can represent a barrier to the exercise of economic and social rights. In addition, it implies that some people, mainly those dependent on social assistance, are subject to inferior guarantees in terms of the protection of their fundamental rights.*"

[35] Existem, até o momento, seis leis promulgadas, por exemplo, na Argentina, no Chile e na Colômbia (Magrani, 2018).

O Brasil, não diferentemente da maioria dos países, também viu crescer de maneira descontrolada os casos de implementação e testes da tecnologia para fins de segurança pública mesmo antes da evolução de uma discussão mais acurada e direcionada aos problemas decorrentes de tal fenômeno.

O primeiro relato de emprego do reconhecimento facial no país remonta ao ano de 2011: um projeto piloto na cidade de Ilhéus/BA e uso de câmeras com a tecnologia em veículos de transporte público visando identificar fraudes à gratuidade no sistema. (Igarapé, 2019).

No caso do emprego na segurança pública, os primeiros testes ocorreram durante eventos de grande porte ainda entre os anos de 2014 e 2016, como a Copa do Mundo e as Olimpíadas. A partir de 2019, contudo, com a edição da Portaria nº 793 do Ministério da Justiça e Segurança Pública, o governo federal passou a destinar verbas do Fundo Nacional de Segurança Pública para, dentre outras medidas, subsidiar a implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, o que propulsionou sua difusão em diversos estados e cidades (Franqueira; Hartmann; Silva, 2021).

Atualmente, de acordo com dados do O Panóptico, projeto de pesquisa do Centro de Estudos de Segurança e Cidadania (CESeC), hoje o Brasil possui 251 projetos em uso, teste ou processo de implementação que se valem da tecnologia em mais de 200 municípios e em quase todos os estados[36]. Outra pesquisa do CESeC apontou que 184 pessoas foram presas em seis estados com base no reconhecimento facial, sendo que, nos casos em que se conseguiu a informação sobre cor/raça do preso ou sobre a natureza dos crimes, 90% deles eram negros e, em sua maioria, suspeitos de crimes sem violência, como furtos e tráfico de drogas em pequenas quantidades (Nunes, 2023).

Para além da desproporção que o referido dado representa num país majoritariamente composto por pessoas negras (Brasil, 2023), os sistemas implantados no Brasil já apresentaram situações que reforçam as análises de precisão do NIST e de Buolamwini e Gebru no sentido de que a TRF tem apresentado vieses e sido usado de maneira pouco transparente.

É o caso de João Antônio Trindade, submetido ao constrangimento de ser detido por agentes da Polícia Militar em um estádio de futebol, com mais de 10 mil pessoas, enquanto acompanhava a final do Campeonato Sergipano. No caso, o homem, que é negro, foi levado para ser interrogado dentro de uma sala, após ter sido reconhecido por um

[36] Para mais detalhes, ver: Nunes, Pablo. Monitor de Novas Tecnologias na Segurança Pública do Brasil. 2024, Disponível em: https://www.opanoptico.com.br/#mapa. Acesso em: 18 jul 2024.

sistema de reconhecimento facial do governo instalado no local e que havia apontado que João seria um possível criminoso (G1, 2024). Após a verificação de que o sistema realizou identificação falha, o governo do estado suspendeu a utilização da tecnologia.

Outro estado que vem aplicando o reconhecimento facial em espaços públicos ao menos desde o ano de 2019 é o Rio de Janeiro. Mais recentemente, a partir da instalação de câmeras de reconhecimento facial no réveillon da capital, a Polícia Militar do estado passou a utilizar o sistema no projeto 190 Integrado, operado pelo Centro Integrado de Comando e Controle (CICC) da corporação (Sousa, 2024)[37]. Segundo dados da instituição, o emprego da TRF na segurança da cidade resultou na prisão de mais de 200 pessoas até junho de 2024 (PMERJ, 2024).

Meses antes da divulgação do dado, em abril de 2024, Natan de Oliveira, morador do Complexo do Alemão, foi preso pela PMERJ e levado até uma delegacia acusado de ser alvo de mandado de prisão em aberto, o que se deu com base em identificação por TRF no bairro de Bonsucesso. Diante da verificação de inexistência de qualquer medida judicial em seu desfavor, apesar do grande constrangimento, o jovem foi liberado (Millan, 2024).

Precursora no uso do reconhecimento facial para segurança pública, segundo Nunes, (2023, p. 9), a Bahia tem sido transformada num verdadeiro "laboratório" para a tecnologia.

Inicialmente empregado na micareta de Feira de Santana e no carnaval de Salvador, em 2019, o sistema de reconhecimento facial foi responsável por mais de 1.500 prisões desde aquele ano e vem se alastrando pelas cidades do interior, estando em processo de implementação em cerca de 80 municípios (Bahia, 2023).

Malgrado não terem sido encontrados dados sobre erros de acurácia e falso positivos no caso baiano, institutos[38] e parlamentares[39] têm questionado sua eficiência e difusão em um contexto de lacuna normativa e de poucas informações em torno da base de

[37] Integra o Sistema Integrado de Comando e Controla (SICC), criado em 2013 como forma de integrar e modernizar os sistemas de segurança pública no Brasil. "De modo mais específico, nos CICC estão os operadores da polícia, telas e computadores para monitoramento das imagens" (Nunes, Lima, Cruz, 2023, p. 9).

[38] "No Brasil, em maio de 2022, centenas de organizações de direitos digitais, ativistas e investigadores lançaram a campanha 'Tire o Meu Rosto da Sua Mira', que reivindica o banimento total das tecnologias digitais de reconhecimento facial na segurança pública, dado o potencial de abusos e violações de direitos" (Melo; Serra, 2022, p. 213).

[39] Em 2022, o deputado estadual Hilton Coelho (PSOL) apresentou o PL nº 24.579/2022, que dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado da Bahia" (Bahia, 2022). No mesmo ano, vereadores da cidade de São Paulo propuseram um projeto semelhante para restringir o uso da tecnologia no município (PL nº 419/2022) (São Paulo, 2022), que, atualmente, encontra-se em discussão na Comissão de Constituição e Justiça (CCJ) da Câmara Municipal.

dados utilizada (Banco de Mandado de Prisão e de Pessoas Desaparecidas) que apenas a Secretaria de Segurança Pública tem acesso (Reis, *et al*., 2021).

Diante do panorama apresentado, e sem a pretensão de esgotamento do universo de estudos, pesquisas, relatórios e notícias sobre os riscos do reconhecimento facial para direitos fundamentais e seu impacto amplificado no contexto brasileiro, pode-se verificar que sua implementação vem ocorrendo de modo precipitado e sem a devida cautela no que concerne ao estabelecimento de diretrizes, requisitos e responsabilização para utilização em espaços públicos.

Nesse sentido, embora tenha promulgado a LGPD, que disciplina "o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado" (Brasil, 2018), o Poder Legislativo brasileiro entendeu que a regulamentação do tratamento de dados pessoais na segurança pública e persecução penal seria tema a ser objeto de lei específica (art. 4º, III, 'a' e 'd'), ainda inexistente. De todo modo, é possível concluir que a regulamentação e o debate sobre como regulamentar o reconhecimento facial é uma demanda real e que deve ser encarada com urgência, sob pena de que seu uso imoderado potencialize cenários de injustiça sistêmica.

Nos casos reais expostos acima, as prisões efetuadas duraram apenas alguns dias ou horas.

Contudo, se determinado *software* de RF adquirido para a finalidade de vigilância possuir um sistema de algoritmo enviesado no decorrer do processo de aprendizado de máquina, ou mesmo se a interpretação humana acerca de uma identificação conferir presunção de eficiência e neutralidade à tecnologia, cabe indagar: até que ponto seu uso poderá ser levado em consideração para comprovar a necessidade de intervenção policial, ou mesmo de processamento e julgamento pela prática de um crime?

Ou seja, até que ponto a repercussão da conclusão obtida com seu uso se limitará a uma medida cautelar como a prisão? Ou, ainda, como o uso desmedido da tecnologia pode impactar a atividade jurisdicional em eventuais ações penais?

Essas e outras questões demandam, a partir de agora, um direcionamento da compreensão sobre o reconhecimento facial para fins de persecução penal a partir da ótica do processo penal, tendo em vista sua potencial contribuição, enquanto elemento probatório, para a ocorrência de erros judiciários.

Capítulo 2: A potencialização do erro judiciário pelo reconhecimento facial e a (im)possibilidade de sua utilização como meio de prova

> A seletividade, a reprodução da violência, a criação de condições para maiores condutas lesivas, a corrupção institucionalizada, a concentração de poder, a verticalização social e a destruição das relações horizontais ou comunitárias não são características conjunturais, mas estruturais do exercício de poder de todos os sistemas penais.
>
> - *Eugênio Raúl Zaffaroni, Em busca das penas perdidas.*

Neste segundo capítulo, foi realizada uma abordagem ainda pouco explorada acerca das possíveis repercussões da utilização do reconhecimento facial para as finalidades de segurança pública sobre o quadro de violações a direitos fundamentais e erros judiciários no processo penal.

Visou-se com isso, procurar entender se, à semelhança de outras formas de reconhecimento de suspeitos já existentes em nosso ordenamento, a aplicação desregrada de um instrumento tecnológico enviesado no contexto de vigilância de massas pode, se vier a ser utilizado como meio de prova na fase processual, exercer um efeito mitigador sobre direitos e garantias fundamentais em eventuais investigações e ações penais, como a presunção de inocência, o contraditório, a ampla defesa e a proteção de dados.

Para tanto, de início, foi feita uma breve explanação sobre o procedimento de reconhecimento de pessoas (art. 226 do CPP) enquanto meio de prova buscando distingui-lo do reconhecimento facial e destacando as críticas em torno dessa modalidade de reconhecimento quando realizado por meio de fotografia, o que tem gerado um cenário alarmante de prisões e condenações errôneas nos tribunais brasileiros.

Em seguida, reflete-se sobre a forma pela qual a inserção do reconhecimento facial na atuação investigativa e na fase judicial pode se manifestar como elemento potencializador de erros judiciários e servir como uma atualização instrumental de um exercício de poder abusivo que, no âmbito penal, carece de legitimidade. Nesse sentido, o uso da tecnologia tanto na prevenção de delitos, quanto na fase processual penal, pode afetar processos decisórios e apresentar resultados tão - ou mais - nocivos a direitos e prerrogativas do que aqueles já existentes no reconhecimento de pessoas presencial ou por meio fotográfico.

Por fim, foi realizada uma breve exposição sobre o atual estágio de compreensão em torno da legitimidade do reconhecimento facial como meio de prova no processo, ressaltando, ainda, as consequências negativas que o uso da TRF na persecução penal pode suscitar.

2.1. Problemas decorrentes da utilização de reconhecimento fotográfico no processo penal

Ao divagar sobre a construção da verdade no processo penal, Paulo Queiroz (2022) aponta que tal qualidade (verdade) não é objetiva, mas fruto de uma atribuição de sentido ou valor pessoal que os sujeitos conferem a determinado fato e com intenções variadas, o que depende, portanto, de uma interpretação construída a partir dos elementos probatórios admitidos e produzidos no processo. Nesse ponto, afirma que "tão importante quanto a prova da verdade é a legitimidade dos meios de prova da verdade" (Queiroz, 2022, p. 88).

Isso porque a busca pela veracidade em torno da existência de um fato típico, ilícito e culpável subsumível a um dispositivo legal incriminador perpassa, geralmente, por diferentes versões dos sujeitos envolvidos, direcionadas ao convencimento do magistrado que condenará, ou não, um acusado. "A verdade, assim, é contingencial, e a legitimação da decisão se dá por meio da estrita observância do contraditório e das regras do devido processo" (Lopes, 2021, p. 408), sob pena de que sejam flexibilizados direitos do investigado/acusado com a admissão e valoração de provas obtidas por meios ilícitos, o que é vedado a nível constitucional (art. 5º, LVI) e legal (art. 157 e parágrafos, CPP).

A ênfase na terminologia "meios" não é despropositada. Isso porque a doutrina realiza uma distinção pertinente entre meio de prova e meio de obtenção de prova. Enquanto o primeiro pode ser entendido como um instrumento direto de produção de provas (depoimentos, perícias, etc.) (Deus Garcia, 2022), o segundo pode ser entendido como uma ponte ou um "instrumento para colheita de elementos ou fontes de provas", de procura (Badaró, 2021, p. 270) (busca e apreensão domiciliar, interceptação telefônica, etc.).

Dentre os meios de prova existentes no Brasil e que devem estar submetidos a critérios legais de admissão e valoração, interessa, nesse ponto, o reconhecimento de pessoas, delimitado nos arts. 226 a 228 do CPP, e que difere substancialmente do reconhecimento facial até aqui estudado, embora tenha finalidades que se aproximam.

Trata-se de um procedimento que pode ocorrer tanto na fase investigativa quanto na fase processual, e visa a confirmação da identidade de uma pessoa supostamente envolvida

num crime a partir da análise, por parte da vítima ou de uma testemunha, das características físicas de sujeitos a ela apresentados presencialmente (Lopes Jr., 2021).

O reconhecimento em questão possui três fases e envolve a descrição da pessoa (art. 226, I); a comparação da pessoa com outras semelhantes (em sexo, idade, raça, etc.), que estarão lado a lado, se possível (art. 226, II); e, por fim, a indicação da pessoa que possivelmente praticou o injusto penal (art. 226, II, parte final), informação que constará em termo a ser lavrado em auto pormenorizado (art. 228). Se houver algum motivo para recear que a intimidação da pessoa a reconhecer os suspeitos comprometa a veracidade de sua declaração, a autoridade providenciará para que aquela não seja vista por esses (art. 226, III).

A doutrina processualista penal afirma que, embora inexista hierarquia entre os meios de prova (Pacelli 2021; Lopes, 2021), o reconhecimento de pessoas é apontado como o mais falho e precário, porquanto demanda a necessidade da estrita observância das fases supracitadas e depende das lembranças ou sentidos de quem é chamado a reconhecer, o que pode ser afetado por vários fatores, como o grau de violência do crime, a visibilidade, estereótipos culturais, a presença ou não de arma[40], estresse, dentre outros, o que pode comprometer a memória e culminar em reconhecimento errôneo (Badaró, 2018; Lopes Jr., 2021).

Diante da simplicidade da disciplina legal do referido meio de prova, seu sucesso dependerá da condução, pelas autoridades policiais e judiciárias, do procedimento positivado, que pode ser facilmente contaminado por preconceitos e falsas lembranças (Lopes Jr., 2021).

Tal panorama se tornou ainda mais preocupante na medida em que as delegacias de polícia no Brasil passaram a adotar, cada vez mais, técnicas informais de reconhecimento fotográfico[41] paralelas a do art. 226 do CPP, como o *show-up*, caso em que é apresentada a foto de um único suspeito, que deve ser identificado de forma positiva ou negativa, (Nunes, 2023), e o *line-up*, geralmente feito pela apresentação de álbuns de fotografias com a imagem de vários suspeitos.

[40] "O chamado *efeito foco na arma* é decisivo para que a vítima não se fixe nas feições do agressor, pois o fio condutor da relação de poder que ali se estabelece é a arma. Assim, tal variável deve ser considerada altamente prejudicial para um reconhecimento positivo, especialmente nos crimes de roubo, extorsão e outros delitos em que o contato agressor-vítima seja mediado pelo uso de arma de fogo". (Lopes Jr., 2021, p. 568).

[41] Corroborando a afirmação, observe-se trecho do voto do Ministro Rogério Schietti Cruz no HC nº 598.886/SC: "Mais ainda se revela frágil e perigosa a prova decorrente do reconhecimento pessoal quando se realiza por exibição ao reconhecedor de fotografia do suspeito, quase sempre escolhida previamente pela autoridade policial, quer por registros já existentes na unidade policial, quer por imagens obtidas pela internet ou em redes sociais. E, mesmo quando se procura seguir, com adaptações, o procedimento indicado no CPP para o reconhecimento presencial, não há como ignorar que o caráter estático, a qualidade da foto, a ausência de expressões e trejeitos corporais e a quase sempre visualização apenas do busto do suspeito comprometem a idoneidade e a confiabilidade do ato." (Brasil, 2020, p. 33).

Esse método se tornou praxe na persecução penal[42] e gerou um intenso debate a respeito de sua licitude, tendo em vista a ausência de transparência sobre quando e como as fotografias inseridas nos álbuns foram obtidas, o que é feito de maneira "obscura, e, comumente, ocorre com o auxílio de redes sociais" (Nunes, 2022, p. 35). Ademais, a menor precisão de informações físicas, como peso e altura, modo de andar, mudança de expressão, etc., (Badaró, 2018), bem como a sugestionabilidade no caso do *show-up* diante da inexistência de alternativas para comparação, também são aspectos que tem suscitado questionamentos quanto a sua compatibilidade com o procedimento previsto no art. 226 do CPP.

Na realidade brasileira, a difusão do reconhecimento fotográfico na atividade investigativa tem sido responsável por um alto número de erros judiciários em virtude da imposição de medidas cautelares e, até mesmo, condenações de pessoas inocentes - em sua maioria, negras e periféricas.

Em pesquisa divulgada no ano de 2022, a Defensoria Pública do Estado do Rio de Janeiro (DPERJ) apurou casos de prisões e condenações baseadas em reconhecimento fotográfico feito em sede policial e não confirmado em juízo que resultaram na absolvição dos acusados, seja pela fragilidade do reconhecimento, seja pela ausência de outras provas o corroborando. Em média, os acusados passaram 281 dias presos por crimes de roubo, furto ou homicídio ocorridos entre 2012 e 2020, sendo que, do total de casos analisados, 83% dos acusados eram negros (DPERJ, 2022).

Dentre diversos casos de abusos decorrentes do reconhecimento fotográfico que tomaram conta do noticiário recente, um deles chamou particular atenção: o do violoncelista Luiz Justino, jovem negro e morador de uma favela do Rio de Janeiro que foi preso em 2020 e denunciado pela suposta prática de um roubo ocorrido em 2017. Na ocasião, a polícia civil o informou de que teria sido reconhecido por meio de um álbum de fotografias existente em delegacia, mesmo sendo primário e sem registros de envolvimento com crimes. Ademais, relatos testemunhais apontaram que, no dia do fato, o jovem estava em outro local. Tal quadro levou o magistrado da causa a ordenar a retirada de sua fotografia do álbum de suspeitos e a absolvê-lo por ausência de provas (Rodas, 2021).

[42] Embora epistemologicamente diversos, o reconhecimento fotográfico e o reconhecimento facial são comumente confundidos em razão de as fotografias utilizadas para as identificações contidas nos álbuns de delegacias corresponderem a imagens do rosto dos suspeitos, de frente ou de lado. Vimos, contudo, que a tecnologia de reconhecimento facial se trata de um *software* composto por etapas complexas voltadas à verificação/identificação de faces obtidas, como regra, por meio de videomonitoramento em espaços públicos e que pode analisar de forma mais precisa as dimensões e a estrutura facial de um indivíduo.

Considerando esses e outros relatos, bem como a já apontada necessidade de lançar legitimidade aos meios pelos quais a polícia e o Judiciário buscam a veracidade acerca das imputações penal, o Superior Tribunal de Justiça (STJ) passou a se debruçar com mais cautela sobre a questão em diversos julgados.

No *Habeas Corpus* nº 598.886/SC, por exemplo, o STJ analisou de maneira paradigmática o caso de um acusado de roubo qualificado que foi condenado pelo tribunal local exclusivamente com base em reconhecimento fotográfico.

No caso, constatou-se diversas ilegalidades no procedimento, como a ausência de exibição de fotografias de outros suspeitos, a disparidade entre a altura relatada pela vítima (1,70m) e a altura do paciente (1,95m), o fato de que os reais envolvidos no delito estavam encapuzados - o que comprometeu a precisão da identificação -, a ausência de confirmação em juízo, dentre outras razões que conduziram à concessão da ordem e a absolvição do paciente (Brasil, 2020).

Na oportunidade, a Sexta Turma da Corte traçou importantes conclusões a respeito do reconhecimento de pessoas por exibição de fotos, entendendo que, embora tal modalidade deva seguir o mesmo procedimento do reconhecimento pessoal, há de ser vista como etapa antecedente deste. Assim, não deve servir como prova em ação penal, ainda que confirmada em juízo, dada sua precariedade e pouca fiabilidade (Brasil, 2020)[43].

Apesar do referido precedente, de acordo com levantamento realizado pelo gabinete do Ministro Rogério Schietti Cruz, do STJ, no ano de 2023, de 377 decisões que revogaram prisão preventiva ou absolveram réus em razão de falhas no reconhecimento do autor do delito, 74,6% tiveram como fundamento a existência de reconhecimento fotográfico errôneo. O alto índice de reversão na conclusão dos tribunais de origem se deu em virtude da interpretação, ainda contrária ao estabelecido no HC 598.886/SC, de que a observância do procedimento do art. 226 do CPP traria uma recomendação, e não uma vinculação legal (Brasil, 2024).

Outro marco relevante foi a conclusão do Grupo de Trabalho sobre Reconhecimento de pessoas, criado pelo Conselho Nacional de Justiça (CNJ), que culminou na edição da Resolução nº 484/CNJ/2022. Dentre as diretrizes estabelecidas, o CNJ delimitou a natureza do reconhecimento de pessoas como prova irrepetível[44] (art. 2º, §1º), a ser realizada por

[43] No mesmo sentido: AgRg no HC n. 462.030/SP, Rel. Ministro Ribeiro Dantas, 5ª T., DJe 13/3/2020.

[44] A prova irrepetível é, dada sua natureza, produzida uma única vez e sem contraditório, seja antecipado, seja em seu momento normal, seja diferido, razão pela qual possui força probante mitigada (Badaró, 2018). Por isso, com maior razão a necessidade de que a conclusão obtida com o reconhecimento seja sempre avaliada de forma conjunta, e nunca isolada, com outros elementos probatórios.

alinhamento de, no mínimo, quatro pessoas, ou de fotografias de pessoas não relacionadas ao fato investigado em igual número - o que afasta a possibilidade de *show-up* - (art. 8º, II), a necessidade de gravação integral do procedimento, a ser disponibilizadas para as partes (art. 5º, §1º) dentre outros parâmetros balizadores da utilização do referido meio de prova (Brasil, 2022).

Contudo, em novo relatório, ao analisar 109 inquéritos policiais instaurados entre a data de publicação da resolução e o final de 2023, a DPERJ constatou que: (i) mais de 80% das investigações estiveram baseadas unicamente em reconhecimento fotográfico, e (ii) não houve, na documentação, qualquer menção ou registro a respeito da Resolução nº 484/CNJ (DPERJ, 2024).

A conclusão, portanto, foi a de que a insistência da flexibilização de parâmetros legais e jurisprudenciais mínimos para o uso de um meio de prova sabidamente precário permanece contribuindo para a existência de uma rotina de erros judiciários no sistema penal brasileiro.

2.2. A perpetuação da perda da legitimidade do sistema penal por meio das novas tecnologias

O quadro exposto sobre o reconhecimento fotográfico revela uma busca incessante pela responsabilização ao arrepio das garantias e da legitimidade dos meios de prova. Essa distorção, por sua vez, apresenta-se como um dos fatores que ampliam uma crescente perda de legitimidade do sistema penal[45] (Zaffaroni, 2014), aqui compreendido pelos aparelhos policial, judicial e prisional voltados à operacionalidade do direito penal.

Segundo Zaffaroni (2014), a referida deslegitimação se relaciona ao fato de que o discurso jurídico-penal tem se tornado cada vez menos racional, pois se encontra em relação de contradição com sua fundamentação antropológica básica - o direito a serviço do homem, e não o homem a serviço do direito -, o que compromete sua veracidade ante a realidade social, e, consequentemente, o legítimo exercício de poder dos órgãos do sistema penal.

Esse exercício de poder, ademais, não se limita somente à atuação da agência judicial (sistema penal formal), mas abrange, antes, a atividade de agências executivas desse sistema, como a polícia, que também o exerce de modo abertamente contrário à legalidade e de forma

[45] Outros aspectos reveladores desse diagnóstico no caso brasileiro são a violência policial em periferias, a superlotação dos presídios e suas condições infraestruturais nefastas, o discurso de combate ao tráfico de drogas e o alto grau de exclusão social provocada pelo estigma do cárcere.

arbitrariamente seletiva (Zaffaroni, 2014). Isso provoca, ao fim, um ciclo de violações à legalidade no qual

> As agências executivas frequentemente atuam à margem dos critérios pautados para o exercício de poder pelos órgãos judiciais, de modo que, quando se produz a intervenção destes, já se consumaram efeitos punitivos irreversíveis sobre a pessoa selecionada (Zaffaroni, 2014, p. 28).

Essa lógica revela, ainda, a contradição de um discurso jurídico-penal que se pretende, especificamente no âmbito processual, alinhado ao sistema acusatório (art. 3-A do CPP) e garantidor das prerrogativas do acusado, mas que, como observado no recorte a respeito dos erros de reconhecimento, ainda flerta com a tendência inquisitiva de busca pela verdade real ao atropelo das mesmas prerrogativas.

Como visto, a tentativa de reconstrução da verdade acerca da autoria e materialidade de um delito, por vezes, é realizada a partir de procedimentos investigativos que reproduzem abuso, violência e opressão a inimigos predeterminados, e que, ao final, são validados pela agência judicial como se legítimos e racionais fossem.

Nesse sentido, em meio à crise que se revela pelo desbalanço entre o dever-ser e o ser do sistema penal brasileiro, bem como a cada erro desconcertante que enseja a absolvição de inocentes, o progresso científico-tecnológico esboçado no primeiro capítulo deste trabalho tem se apresentado como subterfúgio ou solução para os "pontuais" problemas.

Sob essa lógica, as novas tecnologias da era de *big data* e baseadas em inteligência artificial seriam as peças faltantes para o pleno funcionamento de um sistema penal eficaz e racional.

Assim, a utilização de *hardwares* e *softwares* avançados, como drones, *face tracking*[46] e mapas de criminalidade, permitiriam, dentre outras possibilidades, o alargamento dos meios de vigilância penal (Amaral, 2017), a mitigação do subjetivismo inerente às ações humanas no decorrer de procedimentos investigativos e decisórios, tendo em vista a maior imparcialidade e objetividade de métodos como o aprendizado de máquina, e a promoção da eficiência e celeridade inerentes a tais tecnologias, possibilitando a redução de pessoal e outras vantagens sobre o trabalho unicamente humano, tanto a nível investigativo, quanto a nível de prestação jurisdicional.

Nesse último caso, inclusive, vale mencionar a existência do *software* preditivo *COMPAS* (*Correctional Offender Management Profiling for Alternative Sanctions*), utilizado

[46] "O rastreamento facial (tradução livre de *face tracking*) se caracteriza como o uso policial de imagens de vídeo em tempo real ou gravações para rastrear um suspeito. A principal diferença entre as modalidades é a possibilidade de o rastreamento facial envolver informação de localização sobre determinado suspeito" (Oliveira, *et al*. 2022, p. 120)

pelos tribunais em Wisconsin, nos EUA. Tal sistema possui um algoritmo capaz de analisar o histórico criminal de determinado acusado, e, assim, apontar a probabilidade de reincidência, auxiliando a decisão do magistrado (Israni, 2017). O referido instrumento chegou a ser objeto de impugnação perante o Supremo Tribunal de Wisconsin sob o argumento de contrariedade ao devido processo legal, tendo em vista a ausência de transparência dos critérios aplicados em seu uso, contudo, a corte foi favorável à sua utilização em âmbito judicial[47] (Recent Cases, 2017).

Não obstante a empolgação de setores como a política[48] e a mídia[49] a respeito da "solução" que a inovação tecnológica representaria no âmbito do sistema penal, torna-se necessário compreender que seu uso faz permanecer, e até mesmo aprofunda, o problema da ratificação acrítica - ou predisposta à busca cega pela verdade real -, pelo Judiciário, de elementos de prova produzidos em procedimentos investigativos. Nesse sentido, "o progresso técnico-científico entra no mundo penal com legitimidade já formada" (Deus Garcia, 2015, p. 53).

Refletindo sobre o referido quadro, Rafael de Deus Garcia (2022) entende que o uso de tecnologias baseadas em algoritmos na investigação criminal sem a consolidação de um regramento legal específico ou construção doutrinária a seu respeito tem o potencial de mitigar, ou mesmo tornar obsoleto, qualquer avanço de cunho garantista recente no processo penal - como, por exemplo, as balizas sobre reconhecimento de pessoas por parte do CNJ e do STJ aqui explicitadas.

A referida incorporação, ademais, se aproxima do discurso utilitarista, segundo o qual uma ação é moralmente correta quando sua consequência é capaz de satisfazer a necessidade ou interesse de um ou alguns indivíduos (Magrani, 2017), como a manutenção de determinado *status* de poder ou de riqueza[50].

---

[47] No entanto, o tribunal também realizou algumas sugestões a respeito do uso da tecnologia no sentido de advertir os perigos da ausência de informações sobre seu funcionamento, o que é mantido como segredo comercial e pode estar sujeito a todo tipo de viés e imprecisão (Recent Cases. 2017).

[48] Em live publicada no Youtube pelo canal Cortes do Inteligência, o então candidato à prefeitura de São Paulo nas eleições de 2024, Pablo Marçal, respondeu a questionamentos a respeito do uso de métodos disruptivos para solucionar o problema da falta de segurança na cidade. Na ocasião, propôs um programa "pré-crime", voltado à análise preditiva acerca do comportamento de pessoas que, aparentemente, estivessem se preparando para cometer crimes, o que seria subsidiado por reconhecimento facial por meio de drones e câmeras instaladas nos distritos com maiores quantidades de ocorrências de ilícitos. (Youtube, 2024).

[49] Em tom propagandista, a revista Veja publicou matéria na qual ressaltou os benefícios do uso de reconhecimento facial em grandes cidades, como São Paulo, chegando a afirmar que apesar de as falhas "serem estatisticamente bem menores que as taxas de acerto, são esses casos que chamam atenção e alimentam a gritaria contra as máquinas, sobretudo nas redes sociais". (Freitas, 2024, *online*).

[50] "É possível afirmar que a aceitação tácita das tecnologias no processo penal é validada argumentativamente a partir de uma lógica utilitarista. O instrumento medido acaba sendo validado em termos de utilidade, e o critério

No contexto do capitalismo de vigilância, como visto, essa visão se traduz no interesse mercadológico de desenvolvedores que procuram o máximo lucro com a venda de seus produtos inovadores para o estado. Por sua vez, enquanto agente de poder que possui a prerrogativa de exercício do *ius puniendi*, o estado também passa a se valer de novos apetrechos para as políticas de combate à criminalidade, tendo por metas a eficiência e a celeridade, ainda que à míngua de reflexões básicas sobre a ética de tais meios quando sopesados com garantias fundamentais.

Tendo em mente as mazelas possivelmente perpetuadas ou atualizadas pela utilização de tecnologias na persecução penal, adentramos, nesse ponto, na análise do reconhecimento facial enquanto instrumento que guarda em si o potencial de sucessor das modalidades de reconhecimento de pessoas tradicionais, a subsidiar a atividade investigativa e probatória em eventual ação penal.

Torna-se relevante compreender se seu uso produz riscos iguais ou até maiores que as outras formas de reconhecimento para direitos fundamentais que o Brasil se comprometeu a salvaguardar, os quais vêm sendo violados à revelia de uma atividade probatória minimamente legítima na persecução penal.

2.3. Riscos do uso de reconhecimento facial para os direitos fundamentais na persecução penal

Vimos que o impacto do uso de reconhecimento fotográfico como meio de prova no processo penal tem sido contraproducente e responsável por um grande número de condenações viciadas por falhas neste procedimento decorrentes de sugestionabilidade, falsas memórias, racismo estrutural, etc., o que envolve, de maneira muito mais recorrente, indivíduos pertencentes a grupos vulneráveis.

Noutro giro, resgatando a exposição a respeito do reconhecimento facial no contexto da segurança pública, observamos que sua implementação tem sido precipitada e ignora o necessário debate sobre eventuais riscos para as prerrogativas dos mesmos sujeitos majoritariamente prejudicados pelo reconhecimento fotográfico, bem como sobre a existência de vieses algoritmos, falsos positivos e vigilância de massas, aspectos que recaem intensamente sobre os menos favorecidos socioeconomicamente.

---

para definir essa utilidade gira em torno de custos e celeridade, e não em termos de qualidade da prestação jurisdicional". (Deus Garcia, 2015, p. 59).

Nesse sentido, partindo do pressuposto de que a utilização de novas ferramentas tecnológicas no âmbito penal podem, paradoxalmente, potencializar e perpetuar antigos problemas, cabe entendermos que o reconhecimento facial, embora apresentado como forma de contornar o subjetivismo e a seletividade que hoje comprometem a legitimidade do reconhecimento fotográfico, em verdade tende a estimular os casos de erros judiciários já existentes, contrariando, por corolário, direitos fundamentais afetos ao devido processo legal (*due process of law*), como a presunção de inocência (não discriminação), a ampla defesa, o contraditório e a privacidade dados.

A Constituição Federal prevê em seu art. 5º, inciso LVII, que "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória"[51]. O referido preceito fundamental é a positivação do princípio da presunção de inocência.

Trata-se de uma presunção relativa (*juris tantum*) que parte da ideia de que determinado acusado ou investigado é inocente (Queiroz, 2022), o que só pode ser afastado caso o órgão acusador demonstre de maneira satisfatória, por meio do preenchimento de um *standard* probatório[52] mínimo, a sua vinculação com o ilícito. Comprovada a autoria e a materialidade nesses termos, o órgão julgador proverá uma decisão condenatória, que, a partir do trânsito em julgado, passará a produzir efeitos sobre o réu.

A doutrina aponta que o princípio denota duas[53] regras específicas distintas de eficácia, a saber: de tratamento, ponto em que o réu não deve ser submetido a tratamento incompatível com a condição de inocente na persecução penal - como queima de reputação por meios de comunicação que "sentenciam" precocemente, ou restrições cautelares infundadas -, e probatória, dimensão que assegura um ônus probatório sobre o acusador e que deve ser formado por provas lícitas (Pacelli 2022; Lopes Jr., 2021).

Tendo como premissa que a presunção ou estado de inocência se projeta em toda a atividade persecutória, desde o início da investigação até o termo final do processo penal, merece atenção o fato de que o emprego do reconhecimento facial como subsídio para a apuração de crimes pode restringir a sua eficácia a nível de tratamento e probatório.

---

[51] Já a Convenção Americana de Direitos Humanos prevê em seu artigo 8.2 que "Toda pessoa acusada de delito tem direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa. Durante o processo, toda pessoa tem direito, em plena igualdade, às seguintes garantias mínimas: (...)". (Organização dos Estados Americanos, 1969).

[52] Pode ser compreendido como os "critérios para aferir a suficiência probatória, o 'quanto' de prova é necessário para proferir uma decisão, o grau de confirmação da hipótese acusatória" (Lopes Jr., 2021, p. 410).

[53] Aury Lopes Júnior (2021, p. 109) também preleciona um caráter de norma de julgamento da presunção de inocência, perspectiva a partir da qual o referido princípio é "uma 'norma para o juízo', diretamente relacionada à definição e observância do standard probatório, atuando o nível de exigência de suficiência probatória para um decreto condenatório".

Luana Pinho (2024) afirma que esse problema ganha força sob a perspectiva da dimensão preditiva do reconhecimento facial, que reside na possibilidade de se identificar um suspeito que pode estar prestes a agir, ou mesmo que é procurado pela justiça em virtude de fatos remotos supostamente praticados.

Essa possibilidade em um contexto de vigilância de massas distorce o estado de inocência enquanto ponto de partida da atividade investigativa, uma vez que a coleta de dados faciais de todos os transeuntes de determinado local público pela TRF geraria, em verdade, um estado geral de suspeição, ponto em que "mesmo pessoas inocentes sentir-se-iam como criminosas ou potencialmente criminosas" (Pinho, 2024, p. 32).

À maneira de outras tecnologias de policiamento preditivo, a lógica de funcionamento do reconhecimento facial baseada em algoritmo e aprendizado de máquina também se mostra nociva ao devido processo legal sob a ótica da ampla defesa e do contraditório (art. 5º, LV, CF/88).

Numa primeira digressão a esse respeito, cabe rememorar que o emprego do reconhecimento facial para a finalidade aqui debatida está ancorado numa retórica com caráter utilitarista/consequencialista que interessa ao mercado de desenvolvedores, segundo a qual o uso de tal ferramenta representa o alcance da confiabilidade, da neutralidade e da eficiência que os meios tradicionais de reconhecimento não são capazes de atingir.

Contudo, presumir que os resultados aí obtidos são "infalíveis" por decorrerem de etapas (em tese) inteiramente baseadas em operações objetivas, ou que, em virtude de alegado baixo nível de imprecisão, merecem respaldo livre de censuras, é uma conjuntura capaz de gerar prejuízos gigantescos a aspectos imprescindíveis para o devido processo.

Nesse ponto, a opacidade (falta de transparência) a respeito do funcionamento da TRF aliada à "expectativa de neutralidade e objetividade dos processos algorítmicos, como se fossem capazes de suplantar os erros advindos da subjetividade" (Deus Garcia; Duarte, 2017, p. 2), são fatores que podem contaminar a tomada de decisão da autoridade judicial, principalmente caso se leve em conta eventual identificação biométrica por TRF não apenas como ato de investigação (elemento informativo), mas como meio de prova apto ao convencimento.

Esse quadro pode mitigar, assim, a paridade de armas no processo, o contraditório e a ampla defesa, pois "se esta tecnologia permanecer um mistério para o arguido, é-lhe renegado o direito a um julgamento justo" (Pinho, 2024, p. 34).[54]

Assim, a problematização do uso de reconhecimento facial ante tais princípios revela uma necessidade permanente de tomada de medidas de transparência e esclarecimento à pessoa que teve seus dados faciais coletados para fins de identificação, o que poderia se dar, em juízo, pelo parecer de um perito, por exemplo.

Ademais, embora se entenda que atos de investigação não demandam a estrita observância da publicidade e do contraditório (que poderia ser diferido ou postergado) (Lopes Jr., 2021), a transparência também é um princípio norteador da LGPD brasileira, e, sendo o reconhecimento facial uma tecnologia de tratamento de dados pessoais sensíveis, torna-se relevante destacar a incidência desse princípio geral como forma de se proporcionar ao máximo as informações técnicas e as possíveis consequências da identificação, ainda que direcionada para o subsídio de investigações criminais[55].

Por conseguinte, os direitos à privacidade[56] e à proteção de dados pessoais[57] também possuem proteção a nível constitucional e estão intimamente ligados ao problema ora trabalhado.

Como apontado na introdução deste trabalho, o dever estatal de manutenção da segurança pública revela a necessidade, por vezes, de ponderação entre liberdades individuais, como os direitos supracitados, e medidas ou estratégias de combate à criminalidade, o que coloca em evidência a necessidade de que os caminhos escolhidos pelo estado para a consecução de seus objetivos não contrariem tais direitos de modo inconsequente.

É justamente por isso que um meio de obtenção de prova como a gravação ambiental passa a ter caráter clandestino, e, portanto, ilícito, se realizada e posteriormente revelada sem o conhecimento de um dos interlocutores, uma vez que isso violaria o direito à intimidade/privacidade dos sujeitos envolvidos. Do mesmo modo, diversos outros meios ou

[54] Foi esse inclusive um dos argumentos levantados no caso *Winscosin v. Loomis* (2016), já visitado no subtópico anterior. Ao recorrer para o *Wisconsin Supreme Court* contra a sentença que se baseou na ferramenta de avaliação de risco *COMPAS* para condená-lo, Eric L. Loomis argumentou que a metodologia por trás da elaboração dos relatórios de risco pela ferramenta era um segredo comercial, e, portanto, uma decisão condenatória baseada nesse tipo de tecnologia preditiva teria um alto potencial de gerar conclusões discriminatórias, não individualizadas e não transparentes (Recent Cases, 2017).

[55] Compreendemos, contudo, que "o seu exercício nem sempre estará assegurado. Isso porque, por vezes, a tomada de consciência dos titulares acerca do tratamento dos dados pessoais pode prejudicar a própria investigação criminal ou instrução probatória" (Fernandes; Resende, 2023, p. 493).

[56] Art. 5º, X, CF/88: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

[57] Art. 5º, LXXIX, CF/88: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

métodos de prova, como a interceptação telefônica e de dados telemáticos, ou a quebra de sigilo fiscal e bancário, podem gerar situações de ilicitude ao incorrem na limitação da esfera individual.

No contexto do uso de sistemas de reconhecimento facial em tempo real para fins de segurança e vigilância, nota-se que, embora instalados, via de regra, em espaços públicos, sua principal finalidade culmina sempre no tratamento massivo de dados pessoais sensíveis (assinatura facial), pois direcionada, geralmente, para a realização de processos de identificação facial de pessoas perdidas, vítimas de crimes, e, principalmente, suspeitos do cometimento de crimes ou procurados pela justiça.

Desse modo, à maneira de outros meios de obtenção de prova ou meios de prova já estabelecidos em nosso ordenamento, o reconhecimento facial possui um caráter invasivo quanto à esfera privada dos indivíduos, tendo como um de seus objetivos a obtenção de dados biométricos de seus titulares. Nesse ponto, seu emprego no auxílio à persecução penal não pode ser exercido pelos órgãos estatais de modo arbitrário ou irrestrito.

Não se nega que tais direitos não são absolutos, sendo possível limitar a intimidade/privacidade na medida em que seu exercício contrarie interesses voltados a outros direitos igualmente garantidos em nível legal e constitucional.

Contudo, como forma de gerar o menor prejuízo possível à esfera de direitos dos indivíduos, as eventuais restrições só devem ser empreendidas, primeiro, se amparadas por alguma norma que regulamente o conflito e indique qual deve prevalecer, como é o caso da mitigação do direito ao sigilo de correspondência e de comunicações telefônicas em favor da persecução penal (art. 5º, XII, CF/88), ou, caso inexistente qualquer previsão legal, se amparadas por um juízo de ponderação de interesses guiado pela proporcionalidade (em sentido estrito) e razoabilidade da medida (Pacelli, 2022).

Considerando que o direito à intimidade ou privacidade se manifesta, no caso do uso do reconhecimento facial, como direito à proteção de dados pessoais[58], ganha relevância o fato de que a previsão do art. 5º, LXXIX, da CF/88 é norma de eficácia limitada[59], e, como tal, indica que a garantia deve ser assegurada na forma da lei. Ocorre que, como já ressaltado,

[58] Por esse prisma, como bem observado por Rafael de Deus Garcia (2022, p. 241), "o direito à privacidade deve significar muito mais do que ser "deixado só", respeito à propriedade privada e até mesmo autonomia sobre desenvolvimento pessoal. Deve significar também uma preocupação com a qualidade dos dados pessoais e transparência sobre todo o processo informacional, da coleta ao tratamento de dados".

[59] "Estas somente produzem os seus efeitos essenciais após um desenvolvimento normativo, a cargo dos poderes constituídos. A sua vocação de ordenação depende, para ser satisfeita nos seus efeitos básicos, da interpolação do legislador infraconstitucional. São normas, pois, incompletas, apresentando baixa densidade normativa" (Mendes; Branco, 2018, p. 105).

embora a LGPD tenha despertado seus efeitos, isso se deu de forma parcial, restando, ainda, a necessidade de seu pleno desenvolvimento no que tange ao tratamento de dados para fins de segurança pública e persecução penal, que ainda não foi regulamentado no país.

Outrossim, também vimos que o CPP possui, tão somente, disposições em nível não satisfatório a respeito do procedimento de reconhecimento de pessoas, que, nem mesmo aliadas aos balizamentos e detalhamentos realizados pela jurisprudência e pelo CNJ, se aproximam da lógica de funcionamento do reconhecimento facial, que é baseado em algoritmos e inteligência artificial e possui problemas específicos - vieses, opacidade, falhas técnicas, etc.

Assim, mais uma vez, vemos a necessidade de se estabelecer, efetivamente, um arcabouço normativo que condicione o uso de tecnologias no âmbito penal formado a partir do debate técnico e jurídico sobre o tema, o que será melhor discutido em momento posterior neste trabalho.

2.4. Repercussões do reconhecimento facial na atividade probatória

Do exposto, é possível verificar que a contenda entre direitos fundamentais caros ao devido processo legal, como os que aqui foram mencionados, e o uso de reconhecimento facial para vigilância de massas e persecução penal, representará um risco cada vez maior na medida em que essa ferramenta for incorporada em eventuais processos criminais sem balizas legais que orientem tal uso.

Partindo dessa lógica, Rafael de Deus Garcia (2022) entende que, a depender do contexto, as tecnologias baseadas em algoritmos como a em comento podem servir tanto como meio de prova, quanto como meio de obtenção de prova.

De fato, *softwares* de reconhecimento facial podem ser compreendidos como instrumentos que permitem a coleta e a extração de determinado dado (no caso, biométricos da face), seja para a formação de bancos de dados produzidos pelo próprio sistema, seja para a posterior verificação/identificação. Sob essa ótica, ele funcionaria como um meio de obtenção de prova.

Nada obstante, é também esse mesmo equipamento que, produzirá, por meio da comparação da assinatura facial de um indivíduo com outras faces constantes em bancos de

dados externos (ver Figura 1, capítulo 1), um resultado automatizado que indicará se tal sujeito é o responsável por uma infração penal ou um foragido.[60]

Nesse sentido, a sua compreensão como meio de prova (caso em que teria o potencial de subsidiar a formação da convicção do acusador, e, posteriormente, do julgador) possui o potencial de agravar o quadro de violações de garantias fundamentais já existente pelo uso desenfreado do reconhecimento fotográfico.

Embora a doutrina, o legislador e a jurisprudência ainda não tenham voltado suas atenções para esse ponto, encontramos algumas poucas visões sobre a repercussão dos perigos do reconhecimento facial enquanto prova no processo penal.

Sobre o assunto, Aury Lopes Jr. (2021) afirma que o reconhecimento facial é incapaz de solucionar os problemas do reconhecimento de pessoas ou fotográfico que culminam em erros judiciários, uma vez que se funda no pseudoargumento de que seria um novo meio de prova mais confiável e neutro do que os anteriores. Por essa razão, "pode ser um indício interessante, mas jamais uma prova e menos ainda decisiva" (Lopes Jr., 2021, p. 566).

Também Cani e Nunes (2022) se voltam para a temática apontando que o uso para fim de segurança pública tem o potencial de gerar efeitos no processo penal, pois, ainda que serviente, num primeiro momento, como elemento de investigação na fase pré-processual, também pode acabar sendo apresentado como prova em eventual ação penal.

Sob essa dimensão, as conclusões obtidas (que podem refletir um falso positivo) teriam o condão de serem apresentadas em forma de prova documental, como um relatório policial, ou mesmo serem erroneamente consideradas como prova antecipada, cautelar ou irrepetível (Cani; Nunes, 2022)[61]. Desse modo, considerando as dificuldades ainda existentes na superação do alto risco do reconhecimento facial[62], os autores também rechaçam a sua admissão como prova no processo penal.

Por fim, tendo como parâmetro o contexto do direito processual penal português, Luana Pinho (2024) também se debruça sobre a questão. Sob sua visão, o reconhecimento, no

[60] "Só dentro do reconhecimento facial, por exemplo, há várias possibilidades distintas de uso, cada uma com efeitos processuais também potencialmente diferentes. Há o simples *match*, o cruzamento entre o rosto de pessoa presente com sua foto em um documento; a busca, feita a partir de uma imagem existente de alguém que é procurada nos espaços urbanos vigiados; a coleta, para alimento de banco de dados e potencial identificação, feita a partir de imagens de um crime etc. Ou seja, a natureza jurídico-processual do reconhecimento facial é variável entre a identificação criminal, instrumento de autenticação, meio de prova e meio de obtenção de prova, e algo inteiramente novo, o que nos exige esforço de compreensão" (Deus Garcia, 2022, p. 147).

[61] O que não faria sentido na medida em que o processo de identificação pelo *software*, ao menos em regra, não apresenta risco de perecimento ou dificuldade de repetição.

[62] "Mas não se cogita de uma via de acesso reformista que permita "ajustar" os algoritmos para que labutem melhor. Por um lado, é verdadeiro que se trata de uma tendência nas medidas securitárias que, possivelmente, se tornará preponderante nos próximos anos" (Cani; Nunes, 2022, p. 704).

atual estágio do estado da arte, não deve ser concebido como meio de prova, mas, apenas, como meio de obtenção de prova, o que ainda permitiria seu uso como elemento ou indício na investigação, e não como elemento de convicção para o magistrado.

Apesar disso, seu estudo apresenta, também, um otimismo quanto à possibilidade futura de coexistência entre o uso de reconhecimento facial como meio de prova e o respeito a princípios como a presunção de inocência e a ampla defesa, desde que orientado por um uso racional e crítico (Pinho, 2024)[63].

A breve revisão ora realizada revela que a aplicação do reconhecimento facial como potencial meio de (obtenção) de prova no processo penal chega a ser menos explorada que a também incipiente problematização de seu uso para fins de segurança pública enquanto política pública.

Ademais, pode-se concluir, ao menos no atual momento, que a existência de erros operacionais por fatores técnicos e demográficos ainda existentes e negligenciados por desenvolvedores e gestores que adquirem a tecnologia pode colocar em perigo a eficácia de direitos fundamentais quando utilizados na esfera de vigilância de massa, o que revela a necessidade de restrição de sua aplicação como meio de prova em meio ao cenário de incertezas e de lacuna normativa no caso brasileiro.

Nesse sentido, o ponto crucial a respeito do tema, independentemente do ângulo de que se parta, parece ser a regulamentação específica e o desenvolvimento do debate dogmático, o que poderá balizar o uso da TRF de diversas maneiras, englobando, inclusive, a definição de sua natureza e dos requisitos de sua aplicação para fins de investigação ou na fase de instrução.

Considerando que o reconhecimento facial já é uma realidade que ameaça e até mesmo fere as prerrogativas de cidadãos, que, com base nos relatos até aqui explicitados, pertencem a grupos vulneráveis socialmente, não é possível que se fique de "mãos atadas" observando que uma urgência real para a sociedade seja escamoteada do debate jurídico-político.

Feitas tais considerações, antes mesmo que a discussão sobre as repercussões negativas do reconhecimento facial atinja de forma mais concreta os direitos fundamentais no

[63] Nesse ponto, sugere ser "essencial que esta prova do reconhecimento facial seja apoiada por evidências adicionais; que intervenha um perito que esclareça o funcionamento daquela tecnologia; que o juiz perceba como o algoritmo chegou àquele resultado e que se obrigue a contradizer a tendência natural de confiar predominantemente na tecnologia, afigurando-se sempre necessária uma comunhão e corroboração de outros meios de prova, orientada para a transparência, a exatidão, a certeza; salvaguardando as garantias do arguido no processo penal" (Pinho, 2024, p. 62).

âmbito da persecução penal, surge a necessidade de que o estado brasileiro seja instado a se pronunciar sobre a questão ao nível que se espera.

Nesse sentido, uma via pertinente com o condão de impor limitações ao uso desmedido da tecnologia é a atuação do Poder Judiciário. Isso porque, visando mediar os conflitos oriundos do problema que se apresenta, poderá, por meio da prestação jurisdicional, contribuir com a formação de uma posição mais clara a respeito dele e de caminhos para sua superação.

Por outro lado, veremos, a partir das análises realizadas no capítulo seguinte, que também urge a já mencionada necessidade de debate e construção de um arcabouço legal específico voltado para a proteção de direitos nesse contexto e que sirva tanto para a atuação de gestores públicos no exercício de suas atividades, quanto para a atuação judicial dos tribunais.

Capítulo 3. A implementação de reconhecimento facial no Metrô de São Paulo e a necessidade de regulação específica para a salvaguarda de direitos fundamentais

A interação entre os novos meios de tecnologia baseados em inteligência artificial e o direito tem se revelado como um ponto de tensão entre um discurso de cunho utilitarista e empolgado com a otimização de resultados nas políticas públicas, por um lado, e as potenciais repercussões dessas inovações sobre direitos e garantias fundamentais, de outro.

Vimos que de todas as tecnologias baseadas no armazenamento massivo de dados (*big data*) oriundas do contexto da Revolução 4.0 (Schwab, 2016), o reconhecimento facial merece destaque enquanto possível mecanismo de perpetuação de relações de poder entre investigados/acusados criminalmente e o Estado quando no exercício da persecução penal. Isso porque, para além de aspectos ontológicos relativos ao seu funcionamento já verificados, como a falibilidade e a reprodução de vieses discriminatórios, seu uso na política de segurança pública de modo antecipado à formação de um conjunto de medidas legais que o limitem tende a aumentar o risco de eventuais abusos.

Com base nesses pressupostos, o presente trabalho se direciona, agora, para uma análise, sem a pretensão de esgotamento, a respeito da discussão sobre o projeto de implementação de um Sistema de Monitoramento Eletrônico (SME) dotado de *software* de reconhecimento facial para vigilância de massas em execução pela Companhia do Metropolitano de São Paulo (CMSP), empresa pública que opera as linhas de metrô da cidade de São Paulo.

O referido projeto é objeto de uma Ação Civil Pública (Processo nº 1010667-97.2022.8.26.0053) que tramita na 6ª Vara de Fazenda Pública do TJSP e que foi ajuizada em conjunto pela Defensoria Pública do Estado de São Paulo (DPESP), pela Defensoria Pública da União (DPU) e pelas entidades Artigo 19, Instituto de Defesa do Consumidor (IDEC) e do Coletivo Brasil de Comunicação Social (Intervozes), todas voltadas à causa da proteção de dados pessoais, do direito ao consumidor e demais liberdades civis.

Como o processo em questão não tramita sob sigilo ou segredo de justiça, a consulta ao seu teor foi realizada após solicitação de senha de acesso para terceiros (código: agfshn), concedida pelo cartório da vara por meio do e-mail sp6faz@tjsp.jus.br.

Outrossim, a escolha do referido caso se deu em razão de algumas razões que o tornam peculiar em relação aos mais de 250 projetos em fase de implementação ou em operação no Brasil (Nunes, 2024).

Primeiro, é sabido que a cidade de São Paulo possui um histórico de violência policial[64] direcionado às minorias étnicas e sociais da cidade, bem como uma grande população - majoritariamente composta por negros, imigrantes, periféricos e pobres[65] - residindo em sua região metropolitana e submetida ao transporte metroviário na movimentação pendular entre centro e periferia.[66] Considerando o dinamismo urbano e o recorte demográfico que o espaço do metrô apresenta, um sistema biométrico baseado em IA nesse local passa a representar um risco ainda maior para os direitos dos indivíduos que ali transitam.

Além disso, o projeto foi o primeiro a ser questionado judicialmente no Brasil visando instar o Poder Judiciário a se pronunciar sobre a legitimidade do uso da TRF no contexto de vigilância de massas.[67] Nesse ponto, inclusive, como forma de constatar o pioneirismo da ação e a ausência de discussões semelhantes na justiça brasileira, foram realizadas buscas nos bancos de jurisprudências do STF, do STJ, da jurisprudência unificada do Conselho da Justiça Federal (CJF), e dos 27 tribunais estaduais brasileiros com a palavra-chave "reconhecimento facial".

Após a pesquisa, viu-se que a menção ao termo só foi encontrada em processos que, de modo impreciso, utilizaram-no como sinônimo para o que se entende como reconhecimento fotográfico, ou, ainda, em outras situações distanciadas do assunto em comento, como é o caso da validade de contratos firmados por meio de assinatura facial.

Assim, considerando a dimensão que os efeitos da aplicação da TRF nesse cenário podem tomar, bem como a maior quantidade de informações que a judicialização do tema proporciona, nesse último capítulo será analisada a discussão no bojo da ACP para verificar se

---

[64] De acordo com o relatório Pele e alvo: a bala não erra o negro, do Observatório da Segurança Pública, embora São Paulo tenha melhorado os índices de letalidade policial nos últimos anos com políticas direcionadas a tal objetivo aliadas ao uso de *bodycam's*, em 2022, 108 das 157 vítimas de ações do estado eram negras, o maior número dentre os municípios do estado. (Ramos, *et al*., 2023).

[65] Segundo dados da pesquisa "Caracterização Socioeconômica do Passageiro e seus Hábitos de Viagem", publicada em 2018 pela CMSP, o perfil do usuário do metrô se caracteriza, dentre outros aspectos, por pessoas com renda média *per capita* de até 2,1 salários-mínimos (em 2018), majoritariamente residentes na região metropolitana ou na Zona Leste da capital e com nível de formação de ensino médio completo. (CMSP, 2024).

[66] Conforme o Censo Demográfico de 2022, promovido pelo IBGE, o município de São Paulo foi a cidade com o registro da maior população de pessoas pretas do Brasil. (Belandi; Gomes, 2023).

[67] Antes da Ação Civil Pública em questão, a DPESP e o IDEC moveram outra ação civil pública (1090663-42.2018.8.26.0100) contra a ViaQuatro, concessionária da Linha 4 (amarela) do metrô de São Paulo que utilizou um *software* de reconhecimento facial em painéis de publicidade no espaço para detecção facial de reações e emoções dos usuários. No caso, diante da ausência de consentimento ou autorização prévios dos usuários, e com base nos arts. 6º, II e IV, do Código de Defesa do Consumidor (Lei nº 8.078/1990) e do 11, I e II, da LGPD, o Juízo da 37ª Vara Cível da Comarca da Capital/SP julgou parcialmente procedente o pedido para condenar a ViaQuatro à obrigação de cessar a captação das imagens e ao pagamento de danos morais coletivos (Andréa; Gundim; Silva, 2022).

a eventual implementação do reconhecimento facial no metrô de São Paulo, previamente à regulamentação específica do assunto e nos termos propostos pelo Metrô, é um caso que pode contribuir para a ocorrência de erros judiciários no processo penal, potencializando o cenário de violação a direitos fundamentais já existente e relatado nos casos de reconhecimento de pessoas/fotográfico.

Visa-se, também, aferir em que medida a judicialização do uso de reconhecimento facial enquanto política de segurança envolveu a discussão sobre as repercussões desse sistema frente aos direitos fundamentais no âmbito da persecução penal, de modo a servir como ponto de partida para a formação posterior de entendimento jurisprudencial na medida em que violações sejam apresentadas perante o Judiciário e se elevem ao olhar dos tribunais superiores.

Para tanto, dado o grande volume de documentações no processo – que possui mais de três mil páginas –, foram analisadas as principais peças jurídicas[68] juntadas nos autos pelos litigantes, a saber, a petição inicial, a contestação e a réplica, as quais refletiram de modo satisfatório o cerne do problema.

Por fim, no segundo subtópico, foi feita uma breve análise das proposições legislativas voltadas à construção de um marco regulatório sobre o tema à luz das possíveis repercussões do uso dessa tecnologia como política de segurança pública em contextos como o analisado, apontando, ao final, algumas medidas que deverão ser disciplinadas e concretizadas nesse processo.

3.1. A proposta de implementação do reconhecimento facial no Metrô de São Paulo e a judicialização da questão: Ação Civil Pública nº 1010667-97.2022.8.26.0053/TJSP

O caso sob análise teve como ponto de partida o lançamento de um aviso de edital de licitação pública internacional (LPI nº 10014557), por parte da CMSP, para a criação de um novo Sistema de Monitoramento Eletrônico, a ser instalado nas Linhas 1 (azul), 2 (verde) e 3 (vermelha) do metrô.

Os consórcios *Engie Ineo Johnson* e IECIBR/IECISA entraram na disputa realizando propostas para a elaboração a execução do projeto, que, conforme divulgado no Diário Oficial

[68] Até a finalização do trabalho, o processo se encontrava em fase de saneamento e aguardava a realização de perícia judicial requerida pelas partes (São Paulo, 2024).

do Estado de São Paulo, acabou vencida pelo primeiro grupo, em contratação finalizada no montante total de R$ 58.618.282,54 (São Paulo, 2019).

A partir do resultado, o vencedor iniciou o processo de instalação de cerca de 5 mil unidades de câmeras que a empresa deveria fornecer. Ademais, foi estabelecido que cerca de 600 dos novos dispositivos seriam equipados com um *software* de reconhecimento facial.

Em 03 de março de 2022, visando o debate de mérito acerca do projeto, as legitimadas ajuizaram a Ação Civil Pública nº 1010667-97.2022.8.26.0053/TJSP pleiteando, liminarmente[69], a suspensão da instalação dos equipamentos por meio dos quais se promova tratamento de dados biométricos para reconhecimento facial no âmbito do SME, Etapa 3, bem como a abstenção, por parte da ré, em adotar qualquer *software* de reconhecimento facial até o trânsito em julgado da ação (São Paulo, 2024).

No mérito, as legitimadas requereram a condenação da ré e a confirmação dos pedidos liminares, além da condenação ao pagamento de indenização por danos morais coletivos em R$ 42.798.438,63 (valor do objeto contratado com o desconto dos tributos), a serem revertidos para o financiamento de projetos voltados à proteção de dados pessoais de usuários de serviços públicos, nos termos do artigo 42, §3º, 44 e 45 da LGPD.

As alegações de caráter fático das partes se basearam, majoritariamente, em duas fontes presentes nos autos, que são o documento de Concepção do Sistema CS-9.83.ME.XX/7XX.001 (fls. 977-1141), inicialmente constante nos anexos do edital de licitação e juntado ao processo com o inteiro teor de uma ação autônoma de produção de provas ajuizada previamente (Processo nº 1006616-14.2020.8.26.0053/TJSP)[70], e um parecer produzido pelo centro de pesquisas InternetLab a partir de questionamentos realizados pelas autoras (fls. 1652-1453) (São Paulo, 2024).

[69] Na decisão de fls. 1585-1587 da ACP nº 1010667-97.2022.8.26.0053, em 22 de março de 2022, a magistrada responsável pela causa, Cynthia Thome, chegou a deferir o pedido liminar das autoras, determinando a suspensão da execução do sistema de reconhecimento facial no sistema de monitoramento metroviário, admitindo, tão somente, a instalação dos dispositivos de videomonitoramento. Todavia, após interposição de agravo de instrumento (Processo nº 2079077-58.2022.8.26.0000), a 5ª Câmara de Direito Público do TJSP deu provimento ao recurso e reformou a decisão e derrubou a determinação nela exarada, em acórdão proferido em 10 de outubro de 2022 (São Paulo, 2022).

[70] Na ação autônoma as autoras realizaram pedidos de apresentação de provas por parte da CMSP, como, por exemplo, provas documentais sobre a existência de relatório de impacto de proteção de dados do uso da TRF no sistema, sobre a sua confiabilidade e eficiência, bem como sobre propostas de compartilhamento de dados com outros órgãos estatais ou empresas, pontos relevantes que, embora constassem nas atas de esclarecimento do processo licitatório nº 10014557, segundo as autoras, não estavam claros o suficiente. Após o deferimento do pedido pela 1ª Vara de Fazenda Pública do TJSP, a Companhia apresentou a documentação que embasou o processo licitatório e o processo foi extinto (São Paulo, 2024).

Em razão da extensão dos documentos e do conteúdo rigorosamente técnico que possuem, para fins da presente análise, optou-se pela observação das interpretações e menções das conclusões mais relevantes apontadas diretamente nas peças jurídicas.

Partindo da petição inicial (fls. 1-71), observou-se que as autoras da ACP problematizaram aspectos do projeto de implementação do reconhecimento facial no metrô paulistano e se valeram de uma linha argumentativa ampla. Nesse eixo, delinearam que a CMSP, ao instalar a tecnologia nas dependências do metrô, estará realizando tratamento de dados biométricos dos usuários em contrariedade aos direitos e deveres impostos pela Constituição e pela LGPD ao agente de tratamento[71] de dados, bem como às disposições legais e constitucionais que asseguram os direitos do consumidor, da criança e do adolescente, à vida privada (abrangendo a liberdade de expressão e política, de associação e de reunião), e a igualdade/não-discriminação. É possível sintetizar a argumentação da autora com base no seguinte esquema:

Tabela 1. Síntese da argumentação da parte autora na petição inicial da Ação Civil Pública n º 1010667-97.2022.8.26.0053

Direitos/deveres violados a partir da implementação	**Problemas identificados a respeito das características do sistema de reconhecimento facial**
Ausência de consentimento (art. 7º da LGPD)	Afirma que a própria ré admitiu, por ocasião da ação autônoma de produção de provas, que o tratamento de dados pessoais para tal fim não se baseará no consentimento (fl. 17);
Ausência de transparência e contrariedade à autodeterminação informativa a respeito das informações necessárias sobre o tratamento de dados (art. 9º da LGPD)	O projeto não descreve qual banco de dados será utilizado para treinamento do algoritmo do FaceX, se interno ou externo; além disso, existem problemas relacionados à governança, isto é, à forma e duração do tratamento de dados, à informação do controlador, incluído seu contato, às formas de compartilhamento com outros órgãos e responsabilidades dos agentes de tratamento de dados. (São Paulo, 2024, p. 22)
Ausência de adoção de medidas de avaliação e mitigação de riscos (art. 6º, VII, VIII e X, da LGPD; art. 6º, I c/c art. 8 e seguintes CDC)	A CMSP não apontou medidas para prevenir e remediar um dos principais riscos nesse tipo de tratamento de dados, que são os incidentes de segurança, como vazamento de dados massivos pelo compartilhamento ou invasão/roubo de dados por acessos não autorizados por pessoas não cadastradas para acessar as câmeras (São Paulo, 2024);
Ausência de proporcionalidade (adequação e necessidade) da medida (art. 6º, II e III)	Conforme vários estudos, a maior taxa de falsos positivos ocorre entre indivíduos de pele escura ou etnias que não estão devidamente representadas na base de dados. Assim, se esse conjunto de faces não estiver balanceado de modo a representar minimamente a diversidade étnica brasileira, utilizar o

[71] Lei nº 13.709/2018: Art. 5º Para os fins desta Lei considera-se:
(...)
IX - agentes de tratamento: o controlador e o operador;

	FaceX sobre uma média de 4 milhões de usuários por dia no metrô geraria um volume igualmente alto de falsos positivos, o que se mostra especialmente grave se seu objetivo for a identificação de criminosos (São Paulo, 2024).
Contrariedade às normas e princípios que asseguram os direitos da criança e do adolescente (art. 227 da Constituição; arts. 7º e 17 da Lei 8.069/1990; art. 14, §1º, da LGPD) e proíbem o tratamento discriminatório quanto à raça (art. 3º, III, 5º, caput, e XLI da Constituição Federal)	As violações massivas à privacidade promovidas por tecnologias de vigilância – como é o sistema de reconhecimento facial -, afetam de maneira desproporcional crianças e adolescentes, para os quais as políticas devem ser adotadas tendo em vista o seu melhor interesse (art. 6º do ECA); e as pessoas negras, promovendo discriminação racial (art. 5º, caput e XLI da CRFB). De igual forma, pessoas trans também sofrem discriminação algorítmica (São Paulo, 2024)
Contrariedade à privacidade, aos direitos à liberdade de expressão e à liberdade de associação e reunião (art. 5º, IV, X, LXXII da Constituição)	"A privacidade e a liberdade de expressão se reforçam mutuamente, tendo em vista que, para que alguém tenha espaço para pensar, falar e ter sua voz escutada, é um pré-requisito fundamental que não se esteja submetido(a) à vigilância constante (especialmente por parte do Estado) e que o direito à vida privada seja respeitado" (São Paulo, 2024, p. 53)
Contrariedade às normas de defesa do consumidor (art. 2º, VI, da LGPD; arts. 6º, 39, V, e 43 do CDC)	"Tem-se que as disposições do caso em comento violam o direito ao consumidor, em função de sua abusividade, falta de proporcionalidade, desrespeito ao direito de informação, autodeterminação, violação do princípio da vulnerabilidade e hipossuficiência, desconsideração do direito a cidade e direito ao consentimento livre e informado previsto tanto no CDC como na LGPD." (São Paulo, 2024, p. 47).

Fonte: elaborada pelo autor com base na petição inicial (São Paulo, 2024).

Diante da argumentação traçada pelas autoras, por ocasião da apresentação de contestação (fls. 1613-1645), a Companhia do Metropolitano preferiu esclarecer as características do sistema de reconhecimento facial por ela adquirido e os demais aspectos técnicos e jurídicos a respeito do sistema de monitoramento e vigilância a ser implementado no metrô (São Paulo, 2024).

No que interessa para a análise, a ré explicitou que o monitoramento no espaço do metrô era realizado, até então, por um circuito de câmeras analógicas e digitais parcialmente integradas aos seus Centros de Controle Operacional (CCO), sendo que a intenção com a contratação do consórcio *Engie Ineo Johnson* seria, dentre outras melhorias, substituir as câmeras antigas por novas, que transmitiriam informações ao CCO, onde se encontraria o *software* com funcionalidade de reconhecimento facial. Desse modo, ficariam viabilizados a identificação e o rastreio de pessoas desaparecidas ou suspeitas do cometimento de crimes (São Paulo, 2024).

O *software* em questão se chama *FaceX*/*SecurOS*[72], comercializado pela empresa ISS (*Intelligent Security Systems*), que integra o consórcio que venceu a licitação (São Paulo, 2024). Esse modelo de reconhecimento facial, de acordo com a CMSP, se vale do algoritmo da *Tevian*, uma desenvolvedora russa de inovações baseadas em redes neurais convolucionais capazes de armazenar e processar quantidades massivas de dados (São Paulo, 2024).

A respeito da precisão do produto adquirido, a empresa ISS forneceu um relatório do NIST contendo as taxas de falsos positivos e falsos negativos obtidas a partir da participação em um dos testes de FVRT, que afere a qualidade dos algoritmos de reconhecimento facial existentes no mercado. Esse teste em específico tomou como referência fotos de passaporte para concluir que a probabilidade de falsos positivos estaria na faixa de 0,1% e de falsos negativos na média de 0,91%, variando minimamente a depender da idade e do sexo da pessoa a ser identificada (São Paulo, 2024).

A partir desse resultado, a CMSP ponderou que falsos positivos e falsos negativos são variáveis inerentes a todos os algoritmos de reconhecimento facial, e que, além de o teste ter revelado uma porcentagem baixa, após a fase de implantação, novos testes serão realizados no contexto do metrô (São Paulo, 2024), o que manteria a baixa ocorrência de identificações errôneas.

Embora a ré mencione os números para indicar a acurácia desse algoritmo, cabe lembrar que, de acordo com dados divulgados pela própria empresa, uma média de 4 milhões de pessoas usufruem do transporte público diariamente (CMSP, 2024). Nesse sentido, ainda que se considere faixas de falsos positivos menores que 1%, em virtude da utilização sobre uma massa populacional desse porte, o número de falsos positivos torna-se demasiadamente expressivo a depender do número de identificações biométricas a serem realizadas num período prolongado de tempo.

Além disso, como apontamos anteriormente, embora os testes de identificação facial (*one-to-many*) controlados do NIST demonstrem que os atuais modelos de algoritmos de reconhecimento facial conseguem contornar mais facilmente problemas de iluminação, variação de ângulos e outras questões técnicas, via de regra, eles não são realizados levando em consideração bases de dados balanceadas e representativas do ponto de vista étnico-racial e de gênero, abarcando pessoas negras e não-cisgênero. Esse ponto é crucial na medida em que a população de usuários do metrô é majoritariamente composta por residentes na periferia

[72] Uma demonstração do funcionamento do *FaceX/SecurOS* pode ser visualizada no seguinte vídeo, postado pelo canal da ISS no Youtube: **SecurOS FaceX Features.** Intelligent Security Systems. 19 abr. 2022. Disponível em**:** https://www.youtube.com/watch?v=8tPHZ49SlcI. Acesso em: 19 ago 2024.

da Grande São Paulo, em sua maioria negras, e nem sempre submetidas à heteronormatividade, o que pode reduzir a acurácia dessa ferramenta em condições de uso reais e violar o dever de não-discriminação.

Para além desse ponto, a CMSP também afirmou que as imagens de todos os usuários seriam armazenadas pelo prazo de 30 dias, período após o qual seriam sobrepostas por outras. Nesse sentido, o tratamento dos dados faciais não se voltaria à formação de um banco de dados permanente por parte do metrô, mas temporário (São Paulo, 2024).

Assim, a CMSP indicou que seria a controladora e operadora do sistema de reconhecimento facial por meio de seus servidores da área de segurança, e a consulta a essa base de imagens temporária para o fim de realizar a comparação de uma assinatura facial nela constante com um banco de dados externo se daria apenas mediante a celebração de convênio com os órgãos de segurança voltados à investigação e repressão da criminalidade (São Paulo, 2024).

De acordo com a ré, esse tratamento de dados para fins de segurança pública e/ou atividades de investigação e repressão a infrações penais estaria amparado pela Lei nº 6.149/1974, que determina que a segurança do transporte metroviário incumbe à pessoa jurídica que o execute (art. 1º)[73]. Essa imposição legal permitiria, sob essa ótica, o enquadramento da CMSP como órgão de segurança apto a ser a autoridade de tratamento de dados responsável pelo controle e operação do sistema de reconhecimento facial (São Paulo, 2024).

O problema dessa interpretação, contudo, vai de encontro ao fato de que, hoje, inexiste uma norma específica versando sobre o tratamento de dados para segurança pública e persecução penal delimitando quais órgãos poderiam ser entendidos como legitimados para serem autoridades de tratamento.

Assim, se nem mesmo os agentes e membros das forças de segurança mencionados no rol taxativo[74] do art. 144 da Constituição[75] possuem prerrogativa legal para o tratamento de dados pessoais sensíveis para tais finalidades, o que tem sido realizado em diversos outros

[73] Art 1º: A segurança do transporte metroviário incumbe a pessoa jurídica que o execute, observado o disposto nesta Lei, no regulamento do serviço e nas instruções de operações de tráfego.

[74] "Os Estados-membros, assim como Distrito Federal, devem seguir o modelo federal. O art. 144 da Constituição aponta os órgãos incumbidos do exercício da segurança pública. Entre eles não está o Departamento de Trânsito. Resta, pois, vedada aos Estados-membros a possibilidade de estender o rol que esta Corte já afirmou ser *numerus clausus*, para alcançar o Departamento de Trânsito" (Brasil, 2006).

[75] Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: I - polícia federal; II - polícia rodoviária federal; III - polícia ferroviária federal; IV - polícias civis; V - polícias militares e corpos de bombeiros militares. VI - polícias penais federal, estaduais e distrital.

casos no Brasil ao arrepio da legalidade e de garantias fundamentais,[76] tampouco a Companhia, que não é sequer um desses órgãos, pode ser compreendida como apta para o tratamento de dados pessoais para tal finalidade, sendo descabido o exercício da atividade de forma discricionária e sem comprovação de aptidão técnica necessária.

Ainda por ocasião da contestação, a ré mencionou que elaborou, já no contexto da ACP, um Relatório de Impacto de Proteção de Dados Pessoais (RIPDP) (São Paulo, 2024). Esse documento, de acordo com o art. 5º, XVII da LGPD, deve ser apresentado pelo controlador de dados pessoais contendo descrição dos processos de tratamento de dados pessoais nocivos às liberdades civis e aos direitos fundamentais, além de medidas e mecanismos de mitigação de risco.

O documento em questão foi colocado sob sigilo depois de um pedido da CMSP realizado na contestação, o que foi deferido pela magistrada competente. Por essa razão, não foi possível acessar o seu conteúdo, que ficou restrito às partes habilitadas nos autos. No entanto, segundo a Companhia, o relatório detalha os riscos e os classifica, além de sugerir medidas de redução de danos em casos de falhas (São Paulo, 2024).

Apesar da ausência de detalhes a respeito desse documento, as autoras afirmaram em réplica que o RIPDP juntado aos autos seria inválido, porquanto i) é extemporâneo e foi realizado especificamente para a ACP, enquanto deveria ter sido apresentado antes mesmo da realização da licitação para orientar a tomada de decisão a respeito da proporcionalidade e necessidade do investimento; ii) falha em descrever corretamente as operações de tratamento de dados; iii) e não analisa os principais riscos que ameaçam o usuário do transporte público e, portanto, não apresenta ações e medidas eficazes na sua prevenção (São Paulo, 2024).

As autoras observaram alguns riscos não identificados e, assim, carentes de medidas de mitigação, por parte do Relatório de Impacto apresentado no processo (São Paulo, 2024). Dentre eles, as autoras destacaram os constantes na tabela abaixo - elaborada a partir da réplica:

Tabela 2. Riscos não identificados e não avaliados pelo RIPDP apresentado na Ação Civil Pública n º 1010667-97.2022.8.26.0053

[76] Esse sintoma nos remete, sob o prisma do direito administrativo que rege o atuar dos gestores públicos, à lição de Hely Lopes Meirelles (p. 85, 1998) a respeito da legitimidade da atividade administrativa conferida pelo princípio da legalidade: “Na Administração Pública não há liberdade nem vontade pessoal. Enquanto na administração particular é lícito fazer tudo que a lei não proíbe, na Administração Pública só é permitido fazer o que a lei autoriza. A lei para o particular significa "pode fazer assim"; para o administrador público significa "deve fazer assim”’.

Riscos decorrentes do uso de reconhecimento facial pela CMSP não identificados e não avaliados no RIPDP
"As falhas consistentes em falsos positivos confessados pela própria Ré, porém não avaliados, por exemplo na: (i) Identificação equivocada, especialmente de cidadãos negros, de ambulantes ou pedintes; (ii) Identificação equivocada, especialmente de cidadãos negros, na busca por criminosos procurados pela justiça; (iii) Identificação equivocada de pessoas LGBTQIAP+, especialmente pessoas trans e não-binárias, potencializando a discriminação à qual elas já são submetidas, especialmente pela insuficiência da base de dados dessa população, o que aumenta chance de erros; (iv) Identificação equivocada a partir de critérios de idade e gênero" (São Paulo, 2024, pp. 2168-2169)
"A ocorrência de falsos positivos e o histórico de violência nas abordagens de segurança do metrô: aumento da violência sobre usuários do metrô - sejam eles pedintes, trabalhadores informais, ou pichadores" (São Paulo, 2024, p. 2169)
"A possibilidade de desvirtuamento do tratamento de dados, como já demonstrado por outras experiências: violação à liberdade de associação, perseguição de movimentos sociais e grupos organizados" (São Paulo, 2024, p. 2169)
"A possibilidade de identificar, seguir, destacar individualmente e rastrear passageiros específicos, via finalidade de estudo de fluxo origem e destino, conforme visto em outras empresas operadoras de sistemas de reconhecimento facial, onde funcionários utilizavam a ferramenta para perseguir pessoas específicas de seu interesse" (São Paulo, 2024, p. 2169)
A possibilidade de identificação biométrica das faces de crianças e adolescentes sem o consentimento qualificado exigido para lidar com esses dados (art. 14 *caput* e §1º da LGPD)

Fonte: elaborado pelo autor com base na réplica apresentada pelas autoras na ACP nº 1010667-97.2022.8.26.0053

Em suma, nota-se que se o Relatório de Impacto tivesse sido produzido em momento anterior e antevisto todos esses aspectos, provavelmente a conclusão oriunda de seu resultado seria a não aquisição e utilização da tecnologia, tendo em vista a nocividade que o uso em larga escala presenta a direitos fundamentais dos usuários, pedintes e ambulantes que transitam pelo espaço metroviário paulistano.

A partir da discussão promovida no âmbito do caso, uma limitação observada foi o fato de que a as partes não lançaram argumentos a respeito das possíveis repercussões desse uso indiscriminado e ilegal do reconhecimento facial na persecução penal, tampouco problematizou o uso de seus resultados como insumo probatório em investigações por parte da polícia ou para fins de julgamento.

No entanto, considerando que a Lei de Ação Civil Pública (Lei nº 7.347/1985) visa salvaguardar também se presta para a responsabilização por danos "a qualquer outro interesse difuso ou coletivo" (art. 1º, IV), a inserção dessa linha argumentativa na ação em questão

poderia ter reforçado a precariedade desse emprego da TRF no espaço do metrô de São Paulo e a nocividade dessa escolha de política de segurança pública para eventuais investigados e processados criminalmente. Além disso, esse ponto ainda poderá ser abordado por ocasião das decisões judiciais a serem proferidas no decorrer do processo.

De todo modo, foi possível notar, a partir da exposição a respeito das características da *FaceX/SecurOS* e das condições para seu uso na política de segurança pública do metrô, que a eventual implementação dessa ferramenta para a identificação de usuários previamente ao advento de norma regulamentadora que estabeleça balizas para esse fim poderá colocar em risco os direitos fundamentais voltados para a persecução penal. Essa projeção se baseia em algumas constatações.

No caso analisado, o *software* adquirido foi submetido a testes em ambientes controlados que não levam em consideração aspectos demográficos, ficando prejudicadas as porcentagens de falsos positivos e falsos negativos apresentadas. Cabe relembrar, no particular, que ainda que os métodos de aprendizado de máquina tenham avançado nos últimos anos, o processo de treinamento dos algoritmos de reconhecimento facial segue marcado pela ausência de representatividade e diversidade no momento em que são alimentados por dados faciais. Assim, se a TRF do caso do metrô foi desenvolvida em um contexto desse tipo (hipótese que não foi afastada), é bem provável que o processo de identificação biométrica a partir da comparação entre a assinatura facial e algum banco de dados de suspeitos e foragidos da justiça ocorra de modo mais impreciso no caso de atributos faciais menos familiares para o seu algoritmo.

Além disso, seu uso sobre milhões de indivíduos que frequentam o espaço metroviário diariamente também é fator que amplia o universo de potencialmente atingidos pelos erros decorrentes de vieses discriminatórios.

Por conseguinte, a CMSP não apresentou em momento adequado o relatório de impacto à proteção de dados pessoais, o qual, segundo as autoras do processo, também careceu de uma análise suficiente a respeito dos riscos e das correlatas ações mitigadoras.

Viu-se, também que, atualmente, inexiste norma específica que confira à CMSP a competência para ser autoridade de tratamento de dados, ou seja, para controlar ou operar os bancos de imagens formados com a finalidade de realizar a identificação biométrica dos indivíduos nesse espaço. Ademais, o argumento de que a empresa teria prerrogativa para exercer atividades de segurança pública é insuficiente, uma vez que nem mesmo os órgãos de persecução penal a possuem.

Isso porque o art. 4º, III, excepciona, em suas alíneas ‘a’ e ‘d’, a incidência plena da LGPD ao tratamento de dados pessoais para fins de segurança pública e atividades de investigação e repressão de infrações penais (Brasil, 2018), o que torna claro que, em nenhum momento, a lei autoriza de forma expressa ou direta esse tipo de tratamento de dados pessoais atualmente. Pelo contrário, quando menciona o tratamento de dados para esse fim, ou a norma emana condições, ou faz vedações.

Faz condicionamentos no §1º do art. 4º na medida em que prevê que, a partir da edição da lei específica autorizando o uso de tratamento de dados na segurança pública e na repressão penal, as atividades a partir dali iniciadas só podem ocorrer de forma proporcional e respeitando seus princípios gerais e os direitos do titular já existentes (Brasil, 2018). Esse ponto, como vimos, foi abordado pelas Defensorias e pelas entidades legitimadas na ACP.

Além disso, nos §§2º e 4º do art. 4º, a LGPD veda esse modo de tratamento de dados pessoais por pessoa de direito privado, o que só estaria autorizado no caso daquelas constituídas integralmente constituído pelo poder público - empresas públicas. Contudo, em todo caso, esses procedimentos só poderiam ocorrer sob tutela de pessoa jurídica de direito público e serem informados de modo específico à autoridade nacional de proteção de dados. Por fim, o §3º da lei também impõe à ANPD o dever de emitir opiniões técnicas ou recomendações a respeito desse tratamento excepcional e solicitar aos responsáveis os relatórios de impacto à proteção de dados pessoais.

Sob qualquer ângulo, a conclusão inexorável é a de que esses condicionamentos e vedações demandam a edição de norma de amplitude nacional que indique competências e atribuições quanto ao tratamento de dados para fins de segurança e persecução penal.

Esse aspecto, inclusive, está ligado ao fato de que a intenção da CMSP retratada na contestação é o compartilhamento de dados com órgãos policiais para o subsídio de investigações. Contudo, isso também traz consigo a possibilidade de um reconhecimento facial errôneo ser utilizado - ilicitamente, como apontado na discussão no capítulo anterior -, como meio de prova em eventual processo penal para apuração da autoria e materialidade de um crime.

Em arremate, cabe refletir que a aplicação do reconhecimento facial para a finalidade em questão tem maior probabilidade de acontecer em espaços urbanos como o do metrô paulistano, fazendo com que suas consequências repercutam com maior intensidade sobre os chamados “crimes de rua”, como tráfico de drogas, roubos e furtos (Lopes; Furtado; Júnior, 2021). Nesse sentido, “a tecnologia de reconhecimento facial corrobora para o mapeamento

estigmatizante de ‘territórios de risco’, onde habitam os ‘sujeitos potencialmente criminosos’” (Lopes; Furtado; Júnior, 2021, p. 231-232) – como pedintes, artistas de rua e ambulantes - havendo, assim um processo de estratificação de espaços urbanos com seu uso (Franqueira; Hartmann; Silva, 2021).

Por todas essas razões, o caso revela a necessidade de que as preocupações em torno do direito geral à proteção de dados se estendam ao manejo das novas tecnologias baseadas em inteligência artificial no âmbito penal, o que deve se guiar pelos princípios mais basilares do devido processo[77] e por uma visão garantista (Souza, 2022), sob pena de que esses instrumentos sirvam para a atualização de velhos enredos protagonizados seletivamente pelos mais vulneráveis na sociedade.

3.2. A superação da lacuna normativa sobre tratamento de dados pessoais na segurança pública e na persecução penal: regulação como ponto de partida

Apesar de toda a problematização até aqui realizada, faz-se necessário admitir que a interação entre tecnologias de IA no contexto da segurança pública e, consequentemente, da persecução penal, é, provavelmente, um caminho sem volta, sendo uma tendência que já possui dimensão relevante considerando o número de projetos e de relatos a respeito dessa prática no Brasil. Apesar disso, todas essas iniciativas atualmente existentes contrariam o nosso ordenamento pela ausência de norma autorizando o tratamento de dados nesse âmbito, bem como pela contrariedade aos princípios fundamentais constitucionalmente previstos[78].

Diante disso, e tendo em mente o caso analisado, fica claro que não há mais espaço para inércia - deliberada ou não - a respeito do estado de lacuna normativa[79] em que nos encontramos, sendo imperativa a adoção de medidas e parâmetros legais que, a um só tempo, limitem transgressões a prerrogativas nas ações estatais voltadas para o exercício do poder punitivo e deem plena efetivação ao direito fundamental à proteção de dados pessoais previsto no art. 5º, LXXIX, da CF/88.

---

[77] Como a presunção de inocência a ampla defesa e o contraditório, a privacidade dos dados pessoais ante procedimentos de obtenção de provas, e a não-discriminação.

[78] Em sentido contrário, Milanez (2024) sugere que a ausência de regime legal evidencia uma autorização tácita geral para essa atividade.

[79] Kremer e Silva (2023, p. 181) afirmam que a “A previsão do Art. 4º, III, da LGPD denota uma lacuna regulatória, mas jamais um vazio regulatório. Apesar de a Lei não tratar diretamente sobre proteção de dados e segurança pública por vedação expressa no seu Art. 4º, ela apresenta uma série de parâmetros e garantias que devem ser observados. Tais como incidência dos princípios gerais e aspectos de responsabilidade, segurança e boas práticas no tratamento de dados pelo poder público, sem prejuízo de aplicabilidade do ordenamento jurídico pátrio e legislações setoriais concernentes ao tema”.

Assim sendo, tendo "na LGPD o ponto de partida para construir mecanismos e instrumentos eficazes para o uso legítimo das TRFs" (Milanez, 2024, p. 122), os atores envolvidos no processo de regulação da temática devem se atentar a alguns pontos entendidos como imprescindíveis para minimizar os efeitos do uso dessa ferramenta.

Atualmente, o Congresso Nacional vem deliberando acerca de alguns projetos de lei que versam em alguma medida sobre proteção de dados e inteligência artificial. Dentre as propostas mais promissoras estão o PL nº 1.515/2022, de autoria do deputado federal Coronel Armando (PL-SC), um Anteprojeto de Lei elaborado por uma comissão de juristas criada especificamente para esse fim na Câmara dos Deputados, e o PL nº 2.338/2023, que visa regulamentar a inteligência artificial no Brasil, de autoria do Senador Rodrigo Pacheco (PSD-MG).

O primeiro projeto tem enfoque na garantia da proteção de dados pessoais na segurança pública e na persecução penal e tem sido informalmente chamado de "LGPD Penal". Apesar de ter sua estrutura embasada no APL elaborado pelo grupo de juristas convocado pela Câmara dos Deputados, esse texto sofreu críticas diante da supressão de conceitos e princípios da proteção de dados em prol da ampliação de autorizações mais amplas para o tratamento de dados pessoais, o que poderia ocorrer, segundo o projeto, nos casos de segurança pública, investigação criminal e repressão de infrações penais, atividades de defesa nacional, segurança de Estado e, também, de inteligência, o que abriria maior margem para abusos (Azevedo, *et al*., 2022).

Analisando o texto, vê-se que a única medida expressamente voltada para a transparência, por exemplo, é a delegação, à Autoridade Nacional de Proteção de Dados (ANPD), da discricionariedade de dispor sobre acesso a dados e tempo de guarda de registros (art. 35).

Seu conteúdo também é bastante genérico quanto ao problema da discriminação algorítmica em decisões automatizadas, questão em que se limita a vedar definições de perfis que conduzam à discriminação de titulares de dados e indicar que esses sistemas devem ser auditáveis (art. 21, §§ 1º e 2º).

Por fim, o art. 14 do projeto autoriza o tratamento e o compartilhamento de dados pessoais (inclusive sensíveis) para a investigação e repressão de infrações penais, não estabelecendo, no entanto, qualquer procedimento específico para tanto ao dispor: "observada a legislação processual penal vigente no que couber" (Brasil, 2022, p. 9). O problema dessa delegação é que a atual legislação processual penal se encontra obsoleta no que tange às novas

técnicas de apuração de delitos[80], e, no caso dos dados sensíveis obtidos a partir de reconhecimento facial, não há qualquer procedimento aplicável existente ou indicação de que essa técnica de identificação é um elemento de prova válido. Essa estratégia de se valer da legislação processual, ainda que extremamente lacunosa, para se furtar ao dever de disciplinar as garantias necessárias à proteção de dados, é vista em outros pontos do texto[81].

Diante desses problemas, embora esse projeto já esteja aguardando a criação de comissão temporária pela Mesa da Câmara, o Laboratório de Pesquisa em Políticas Públicas e Internet (LAPIN) chegou a recomendar o arquivamento da proposição (Azevedo, *et al*., 2022).

Por outro lado, o anteprojeto se apresentou mais adequado para dar efetividade às disposições da LGPD[82] e avançar na regulação do assunto (Azevedo, *et al*., 2022), uma vez que, além de adotar vários dos princípios de proteção de dados previstos naquela norma, também acrescenta como fundamentos os princípios do respeito à vida privada e à intimidade (art. 2º, III), da presunção de inocência (art. 2º, V), e da garantia do devido processo legal sob a ótica da ampla defesa, do contraditório, da motivação e da reserva legal (art. 2º, VII), abrangendo todos aqueles que ressaltamos ao longo do segundo capítulo como de observância obrigatória para evitar um aumento de erros judiciários a partir dos resultados obtidos pela TRF.

Interessante a abordagem regulatória prevista nos arts. 23 a 26 do projeto, que indica possibilidade de um conjunto de ações antidiscriminatórias e de minimização de vieses por parte do órgão de controle da atividade, que, nesse projeto é apontada como sendo o CNJ, e não a ANPD.

Nesse sentido, o texto prevê que as decisões tomadas com base no tratamento automatizado de dados, como medidas coercitivas ou restritivas de direitos, devem ser precedidas de autorização pelo CNJ e autorizadas por lei.

---

[80] Cabe lembrar que o Decreto-Lei que introduziu o CPP no ordenamento jurídico foi decretado em 1941 pelo então presidente Getúlio Vargas, enquanto o projeto de lei mais promissor no Congresso Nacional (PL nº 8045/2010) foi elaborado há mais de uma década, razão pela qual seu capítulo que disciplina as provas digitais (arts. 298 a 310) carece de revisão no sentido de inserir seu conteúdo no contexto das inovações baseadas em inteligência artificial e do tratamento de dados pessoais.

[81] Por exemplo, ao invés de disciplinar diretamente o direito de acesso à informação do titular de dados sobre compartilhamento dessas informações pessoais para fins de investigação e repressão penal, o texto também afirma que o exercício desse direito se dará na forma da legislação processual penal (art. 29), embora essa regulação inexista no atual CPP (Azevedo, *et al*., 2022).

[82] A exposição de motivos do APL indica que seu texto foi elaborado a partir de inspirações na LGPD (Lei nº 13.709/2018) e na Diretiva 680/2016 da União Europeia, que regula o tratamento de dados para fins de segurança pública e persecução penal de forma apartada do Regulamento Geral de Proteção de Dados (GDPR) (Brasil, 2019).

Ademais o órgão ficaria incumbido de solicitar e examinar relatórios de impacto de proteção de dados pessoais e decidir quanto à possibilidade da atividade a partir de auditorias para verificar a precisão do algoritmo, a existência de vieses e o grau de precisão e acurácia, ficando afastadas restrições em razão de segredo industrial e comercial.

Esse conjunto de medidas poderia ser complementado, via emenda, por disposições[83] a respeito das características mínimas que as tecnologias baseadas em IA devem possuir para serem utilizadas, como, por exemplo, a necessidade de que tenham sido desenvolvidas por meio de amostras representativas para o treinamento de máquina e adequadas ao contexto demográfico em que serão aplicadas, ou mesmo de que as empresas ou órgãos desenvolvedores adotem políticas internas de diversificação de gênero, raça etnia, e outros referenciais nas equipes de pesquisadores e criadores de soluções, o que pode mitigar os vieses apontados por Ruback, Ávila e Cantero (2021) no primeiro capítulo.

O APL também estabelece critérios gerais para avaliação de risco das tecnologias de monitoramento ou tratamento de dados à direitos e garantias dos titulares (art. 42, §1º), todavia, não enquadra cada modalidade de tecnologia por níveis de risco.

Essa classificação, no entanto, pode ser encontrada no Projeto de Lei nº 2.338/22[84]. Baseando-se na categorização por grau de risco do *AI Act* europeu[85], o PL determina que sistemas de IA devem ser submetidos à avaliação preliminar de risco que determine se ele é alto ou excessivo.

No caso, o projeto classifica os sistemas de identificação biométrica à distância, em tempo real e em espaços públicos como de risco excessivo, o que ensejaria sua proibição.

[83] No Brasil, a Resolução nº 332/2020 do CNJ, que regulamentou a produção e o uso de IA no Poder Judiciário, já possui alguns dispositivos que condicionam a criação de novas tecnologias no âmbito dos tribunais a essas medidas. Nesse sentido, seus artigos 6º: "Quando o desenvolvimento e treinamento de modelos de Inteligência exigir a utilização de dados, as amostras devem ser representativas e observar as cautelas necessárias quanto aos dados pessoais sensíveis e ao segredo de justiça" (Brasil, 2020, p. 4), e 20: "A composição de equipes para pesquisa, desenvolvimento e implantação das soluções computacionais que se utilizem de Inteligência Artificial será orientada pela busca da diversidade em seu mais amplo espectro, incluindo gênero, raça, etnia, cor, orientação sexual, pessoas com deficiência, geração e demais características individuais" (Brasil, 2020, p. 8).

[84] O texto foi aprovado em 29 de setembro de 2021 pela Câmara dos Deputados e posteriormente encaminhado ao Senado, contudo, até o momento, não há indicativo de que a análise e votação ocorrerá dentro de um prazo definido.

[85] O *AI Act* condicionou o uso de sistemas de IA a três categorias de risco: primeiro, sistemas proibidos, entendidos como aqueles que geram um risco inaceitável a direitos; segundo, aplicações de alto risco, e, por fim, sistemas que não foram explicitamente proibidas ou classificados como de alto risco, que foram deixados sem regulamentação específica quanto ao uso (Future of Life Institute, 2024). No caso do reconhecimento facial, Rui Pereira (2022) explica que a norma classificou como sendo um sistema de alto risco e estabeleceu que seu uso só poderia ocorrer em três hipóteses: a busca direcionada de potenciais vítimas específicas de crime, incluindo crianças desaparecidas; a prevenção de uma ameaça específica substancial e iminente à vida, como ataque terrorista; e para a detecção e identificação de um suspeito pelo cometimento de um crime grave, entendido como um daqueles constantes na Decisão-Quadro do Mandado de Detenção Europeu, de rol taxativo.

Contudo, uma emenda acrescentada pelo Senador relator, Eduardo Gomes (SDD-TO), excepcionou seu uso para i) instrução de inquéritos ou processos criminais, quando a prova não puder ser feita por outros meios disponíveis; ii) busca de vítimas de crimes e pessoas desaparecidas; iii) flagrante delito de crimes punidos com pena privativa de liberdade superior a 2 (dois) anos e iv) recaptura de réus evadidos e cumprimentos de mandados de prisão (Brasil, 2024, p. 46).

Vê-se, assim, que as exceções desse PL esvaziam a categorização e criam uma brecha direta para que a identificação biométrica por TRF passe a ser utilizada como meio de prova, o que demanda a exclusão, especialmente, da primeira, terceira e quarta exceções.

Noutro giro, uma disposição que, ao menos em tese, asseguraria maior transparência e tornaria o eventual uso dessa tecnologia na persecução penal algo menos problemático, caso autorizado, foi encontrada no PL nº 3069/2022,[86] que "Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências" (Brasil, 2022, p. 1). A proposta assegura que ações ou diligências policiais de restrição da liberdade não devem ser efetuadas somente a partir do reconhecimento facial, devendo haver uma associação da informação obtida com medidas de identificação multibiométrica e a revisão por um perito papiloscopista especializado em identificação facial (art. 5º, parágrafo único) (Brasil, 2022).

Esse cotejo do reconhecimento facial com outros procedimentos de identificação somado à revisão humana por um especialista parece relevante para uma futura legislação que estabeleça procedimentos e balize eventual permissão de uso da TRF como elemento probatório. Isso porque, se positivado, pode contribuir tanto para a minimização de falhas, quanto para eventual exercício da ampla defesa e do contraditório, que tem como pressuposto uma explicação qualificada e que permita a compreensão, por parte dos indivíduos investigados ou acusados criminalmente, sobre o funcionamento do reconhecimento facial e de suas implicações.

Nesse sentido, e à guisa de conclusão, é possível elencar como inegociáveis na disciplina da matéria os seguintes parâmetros: a) estratégias ou ações antidiscriminatórias e de minimização de vieses ou erros de acurácia a partir de uma abordagem regulatória, envolvendo a atuação de uma autoridade nacional de proteção de dados; b) classificação de risco autorizando, limitando ou proibido o uso da tecnologia, a depender do cenário em que aplicado; c) definição a respeito da pertinência ou não do compartilhamento dos dados para

[86] Proposta elaborada por Petterson Vitorino de Morais, Especialista em Análise Facial – Papiloscopista Policial - II/DPT/PCDF, e apresentada pelo deputado federal Gonzaga (PSD-MG).

uso como elemento probatório na persecução penal, com a criação de um procedimento detalhado, caso admitido; d) iniciativas de transparência/*accountability* e de revisão humana (auditorias, direito à informação e à explicação, etc.) e e) análise preliminar de proporcionalidade e realização de relatórios de impacto à proteção de dados.

As iniciativas para resolução dessas e outras demandas, portanto, devem ter como pressuposto a realidade brasileira, marcada pelos reflexos sociais da colonialidade afeita ao contexto latino-americano (Quijano, 2009), e, principalmente, por um sistema penal caracterizado pela violência institucional, pela difusão do "nós contra eles" no senso comum pelas mídias voltado à justificação da vigilância e do controle social[87], pelo quadro de erros judiciários nos tribunais decorrentes de arbitrariedades processuais contra inocentes, dentre outros elementos que tornam ainda mais temerosa a instrumentalização das novas tecnologias nesse âmbito[88].

[87] Aqui mencionado no sentido preconizado por Zaffaroni (2014) de "poder configurador positivo", que transcende a mera repressão de imputações penais legalmente criminalizadas e atinge um nível de projeção muito maior sobre o comportamento social. Nesse sentido, "praticamente, não existe conduta - nem mesmo as ações mais privadas - que não seja objeto de vigilância por parte dos órgãos do sistema penal ou daqueles que se valem de sua executividade para realizar ou reforçar seu controle, embora mostrem-se mais vulneráveis às ações realizadas em público, o que acentua a seletividade da vigilância em razão da divisão do espaço urbano que confere menores oportunidades de privacidade aos segmentos mais carentes" (Zaffaroni, 2014, p. 25).

[88] Cabe alertar, no entanto, que não se trata de uma "demonização" da intersecção das novas tecnologias e o âmbito da prevenção/repressão de delitos, mas, tão somente, de explicitar o alto risco que elas possuem quando empregados para essas finalidades sem condições legais mínimas. Afinal, esses instrumentos também podem ter efeitos positivos, como quando as *bodycam's* contribuem para a mitigação de arbitrariedades da atuação policial, e, consequentemente, para um processo penal que não viole direitos fundamentais, ou mesmo quando o reconhecimento facial permite a identificação de desaparecidos ou vítimas de delitos como o sequestro (art. 148, CP).

CONCLUSÃO

O aprimoramento da capacidade e da funcionalidade dos artefatos tecnológicos que hoje compõem a era digital trouxe consigo a otimização de atividades humanas e uma série de outros benefícios, mas, também, novos dilemas.

Dentro desse contexto, o reconhecimento facial, enquanto espécie de tecnologia voltada à verificação/identificação biométrica de dados pessoais sensíveis (atributos faciais), tem se mostrado uma ferramenta nociva para direitos fundamentais de populações historicamente submetidas a relações de poder, podendo mitigar, especialmente, as prerrogativas de investigados e acusados criminalmente.

Nesse sentido, seu emprego nas políticas de segurança pública com vistas à vigilância em espaços urbanos tem sido amplamente difundido no Brasil e no mundo, o que surge acompanhado por uma compreensão, propagada pelas grandes corporações que desenvolvem tais tecnologias e pela mídia, de que a celeridade, a imparcialidade e a precisão da atuação dos agentes envolvidos na prevenção e repressão de delitos seriam fatores alcançados a partir desse "tecnosolucionismo".

Ainda sob essa lógica, no âmbito da persecução penal, a TRF tem sido apresentada como um meio de minimização de erros em eventual apuração de delitos que, atualmente, se dão, em grande parte, pela falibilidade inerente ao reconhecimento de pessoas ou por fotografia.

No entanto, embora imbuído de atributos que o tornam mais eficaz em relação à mente humana, o reconhecimento facial, ao contrário do que se faz crer, não se encontra afastado da dita falibilidade, especialmente quando analisado seu grau de acurácia relativamente à diversidade étnico-racial e de gênero, ponto em que se mostra vulnerável ao reproduzir vieses discriminatórios presentes na sociedade. Por essa razão, considerando as mazelas socioeconômicas que permeiam a história brasileira e que se potencializam num sistema penal seletivo, estigmatizante e voltado ao controle social das massas, seu emprego como elemento probatório no âmbito processual penal não tem sido recomendado.

De todo modo, o arranjo de utilização da TRF na segurança pública com desdobramentos sobre a atividade de persecução penal é um fenômeno real em nosso país, havendo relatos de milhares de prisões realizadas com base nesse tipo de tecnologia, algumas, inclusive, reconhecidamente errôneas em razão de falha de identificação. Esse cenário, ademais, passou a ser propulsionado pelo próprio estado brasileiro, que, fomentando o

investimento nesse tipo de tecnologia, contribuiu para sua difusão a nível estadual e municipal em um cenário de aparente legalidade. Afinal, a implementação ou não desse tipo de tecnologia estaria submetida à discricionariedade do gestor no atendimento às demandas da sociedade quanto à segurança pública.

No entanto, conforme abordado do presente trabalho, essa aplicação desenfreada da TRF tem ocorrido previamente à construção de um marco regulatório específico, uma vez que as disposições atualmente existentes contidas na LGPD não se apresentam como suficientes e não autorizam o tratamento de dados pessoais para essa finalidade.

A partir desse panorama, a partir da identificação de um quadro ainda incipiente de discussão a nível judicial dos casos de implantação da TRF para fins de segurança e vigilância em espaços públicos, realizou-se a análise do projeto de implementação desse instrumento no Sistema de Monitoramento Eletrônico do metrô de São Paulo, primeiro caso judicializado no país, a fim de se verificar os possíveis riscos dele decorrentes para direitos fundamentais no âmbito da persecução penal.

A partir do debate promovido pelas partes na ACP, viu-se que essa repercussão em específico não se fez presente como foco central na discussão, a qual esteve voltada para a problematização do uso de reconhecimento facial sobre direitos relativos à proteção do consumidor, da criança e do adolescente, de liberdades civis – reunião, associação, livre pensamento, etc. -, e, à luz do atual regramento da LGPD, da proteção de dados pessoais. Nada impede, contudo, que a questão seja abordada pelas decisões judiciais a serem proferidas no processo, o que contribuirá para o surgimento de um entendimento inicial acerca do tema.

Ainda assim, levando-se em conta as características do *software FaceX/SecurOS*, adquirido para a política de segurança do metrô, bem como as condições em que possivelmente funcionará caso a instalação se concretize, seu uso nesse espaço poderá colocar em risco os direitos fundamentais voltados para a persecução penal.

Isso porque: a) o *software* não foi submetido a um teste balanceado do ponto de vista demográfico e voltado para a constatação, ou não, de vieses, o que prejudicou as taxas de falsos positivos e falsos negativos apresentadas pela empresa contratante; b) o metrô de São Paulo é espaço frequentado por cerca de 4 milhões de pessoas todos os dias, fato que amplia o universo de potencialmente atingidos pelos erros decorrentes de eventuais distorções; c) a apresentação do relatório de impacto à proteção de dados pessoais ocorreu de modo circunstancial – apenas em razão da judicialização – e careceu de uma análise suficiente sobre

riscos e ações mitigadoras; d) inexiste norma que confira à CMSP uma competência para ser autoridade de tratamento de dados no contexto da segurança pública, a qual nem mesmo os órgãos de segurança possuem, razão pela qual o compartilhamento dos dados obtidos entre a Companhia e esses órgãos também seria realizado de forma precarizada; e) a ferramenta poderia colaborar para o mapeamento de indivíduos estigmatizados na localidade instalada, atingindo, além da população periférica usuária das linhas metroviárias, os pedintes, artistas de rua e ambulantes.

A partir da análise contextual do caso escolhido, que permitiu uma constatação a nível prático dos problemas apontados ao longo do trabalho, viu-se que a superação da atual lacuna normativa acerca da regulação do tratamento de dados pessoais para fins de segurança pública e persecução penal é uma necessidade premente e deverá ser composta por medidas que minimizem de maneira eficaz os riscos identificados, como as que foram elencadas ao final do último subtópico.

Sob essa ótica, considerando que "o homem não existe em razão da lei, mas a lei existe em razão do homem" (Marx, 2010, p. 50), a edição de uma regulação da atividade de tratamento de dados pessoais na seara em comento deverá ser compatível com a realidade de nossa região, orientada pela busca da concretização de direitos humanos e fundamentais na atividade investigativa e no processo penal, bem como atenta à tendência utilitarista do emprego da tecnologia nesse âmbito, a fim de que abusos de direito e erros judiciários não se intensifiquem enquanto sintomas da operatividade de nosso sistema penal.

REFERÊNCIAS

ADJABI, Insaf, *et al*. **Past, Present, and Future of Face Recognition: A Review.** Electronics. 2020, 9, 1188; doi:10.3390/electronics9081188. Disponível em: file:///C:/Users/mathe/Downloads/FaceRecognition_23-07_2020.pdf. Acesso em: 15 jul. 2024.

AI-HLEG, High-Level Expert Group on Artificial Intelligence (2019). **A definition of AI: Main capabilities and scientific disciplines.** 2019. Disponível em: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf. Acesso em: 12 jul. 2024.

ALJAZEERA. **China drafts rules for facial recognition tech amid privacy complaints**, Aljazeera, 8 ago 2023. Disponível em: https://www.aljazeera.com/economy/2023/8/8/china-drafts-rules-for-facial-recognition-tech-amid-privacy-complaints. Acesso em: 17 jul 2024.

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. **Revista Brasileira de Segurança Pública**. São Paulo v. 16, n. 2, 264-283, fev/mar., 2022.

ALMEIDA, Silvio Luiz de. **Racismo estrutural**. São Paulo: Sueli Carneiro, Pólen, 2019.

AMARAL, Augusto Jobim do. A governamentalidade em tempos securitários. *In:* **Direito, risco e sustentabilidade: abordagens interdisciplinares.** Caxias do Sul: EDUCS, 2017, p. 162.

ANDRÉA, G. F. M.; GUNDIM, W. W. D.; SILVA, D. **Tecnologia de reconhecimento facial como política de segurança pública**: o caso do metrô de São Paulo. Revista da Faculdade de Direito do Sul de Minas, v. 38, p. 279-298, 2022.

AZEVEDO, Cynthia Picolo Gonzaga de; *et. al*. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022.** Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Disponível em: https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf. Acesso em: 19 ago. 2024.

BADARÓ, Gustavo Henrique. **Processo penal [livro eletrônico].** 9. ed. rev., atual. e ampl., São Paulo: Thomson Reuters Brasil, 2021.

BAHIA. **326 presos pelo Reconhecimento Facial e queda de mortes violentas são destaques no primeiro semestre de 2023**. Governo do Estado da Bahia, 2023. Disponível em: https://www.ba.gov.br/policiatecnica/noticia/2024-04/900/326-presos-pelo-reconhecimento-facial-e-queda-de-mortes-violentas-sao-destaques, Acesso em 18 jul 2024.

BELANDI, Caio; GOMES, Irene. **Censo 2022:** pela primeira vez, desde 1991, a maior parte da população do Brasil se declara parda. Agência IBGE Notícias. 22 de dezembro de 2023. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38719-censo-2022-pela-primeira-vez-desde-1991-a-maior-parte-da-

populacao-do-brasil-se-declara-parda#:~:text=O%20munic%C3%ADpio%20de%20S%C3%A3o%20Paulo,%2C%20com%2052%2C8%25. Acesso em: 1 jun. 2024. Acesso em: 18 ago. 2024.

BIG BROTHER WATCH. **Big Brother Watch Briefing on facial reecognition surveillance.** Big Brother Watch, 2020a. Disponível em: Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf (bigbrotherwatch.org.uk). Aceso em: 15 jul. 2024.

BIG BROTHER WATCH. **Face off:** The Lawless growth of facial recognition in UK policing. Big Brother Watch, 2018. Disponível em: Face-Off-final-digital-1.pdf (bigbrotherwatch.org.uk). Acesso em: 15 jul. 2024.

BIONI, Bruno Ricardo**. Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Habeas Corpus nº 462.030/SP**. 5ª Turma, rel. Min. Ribeiro Dantas, DJe: 13 de marco de 2020.

BRASIL, Superior Tribunal de Justiça. **Habeas Corpus nº 598.886/SC.** 6ª Turma, rel. Min. Rogerio Schietti, data de julgamento: 27.10.2020, 2020.

BRASIL. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal.** Brasília: Câmara dos Deputados, 2019. Disponível em: https://escola.mpu.mp.br/a-escola/comunicacao/noticias/especialistas-discutem-anteprojeto-da-lgpd-penal/anteprojeto-lgpd-penal.pdf/view. Acesso em: 19 ago. 2024.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515, de 07 de junho de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Câmara dos Deputados, Brasília, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022. Acesso em: 19 ago. 2024.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 3.069, de 22 de dezembro de 2022.** Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2228103&filename=PL%203069/2022. Acesso em 18 ago. 2024.

BRASIL. Câmara dos deputados. **Projeto de Lei nº 8.045, de 22 de dezembro de 2010.** Código de Processo Penal. Brasília, 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263. Acesso em: 20 ago. 2024.

BRASIL. Conselho Nacional de Justiça. **Resolução nº 332, de 21 de agosto de 2020.** Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Brasília, 2020. Disponível em:

https://atos.cnj.jus.br/files/original191707202008255f4563b35f8e8.pdf. Acesso em: 20 ago. 2024.

BRASIL. Conselho Nacional de Justiça**. Resolução nº 484, de 19 dezembro de 2022**. Estabelece diretrizes para a realização do reconhecimento de pessoas em procedimentos e processos criminais e sua avaliação no âmbito do Poder Judiciário. Brasília, 2022. Disponível em: https://atos.cnj.jus.br/files/original211837202212276 3ab612da6997.pdf. Acesso em: 8 ago 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 2024. Disponível em: http://www.planalto.gov.br/ccivil_03/ Constituicao/Constituiçao.htm. Acesso em: 15 jun. 2024.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal).** Disponível em: < https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm>. Acesso em: 15 mai. 2024.

BRASIL**. Lei n° 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD)**.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 mai. 2024.

BRASIL**. Lei nº 7.347, de 24 de julho de 1985**. Disciplina a ação civil pública de responsabilidade por danos causados ao meio ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm. Acesso em: 22 ago. 2024.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm.Acesso em: 19 ago. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 19 ago. 2024.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023.** Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 18 ago. 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 1.182.** Rel. Min. Eros Grau, data de julgamento: 24-11-2005, publicado no Diário de Justiça de 10-03-2006.

BRITO, Carina. **Sistema de reconhecimento facial erra, e homem negro é preso por engano.** Tilt Uol. 25 jun 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/06/25/homem-e-preso-apos-erro-de-tecnologia-de-reconhecimento-facial-nos-eua.htm. Acesso em: 18 jul 2024.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades:** Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 81:1-15,

2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 15 jul. 2024.

CANI, L. E.; NUNES, J. A. Erros judiciários em tempos de digital surveillance: os algoritmos de reconhecimento facial em questão. **Revista Brasileira de Direito Processual Penal**, v. 8, n. 2, p. 679–712, maio 2022. Disponível em: https://doi.org/10.22197/rbdpp.v8i2.720. Acesso em. 15 jun 2024.

CANTO, Mariana. Made in Surveillance: A regulação da importação e do uso de tecnologias de vigilância estrangeiras e a relativização dos direitos fundamentais e da soberania estatal. Surveillance in Latin America. 2019. *In:* **VI Simpósio Internacional Lavits**, 2019. Anais... Salvador, 2019, p. 3 ss.

CAPPI, Ricardo. A "teorização fundamentada nos dados": um método possível na pesquisa empírica em Direito, p. 397. *In.* MACHADO, Maíra Rocha (Org.). **Pesquisar empiricamente o direito.** São Paulo: Rede de Estudos Empíricos em Direito, 2017. 428 p.

CASTELLS, Manuel. **A sociedade em rede.** Tradução: Roneide Venâncio. 6. ed. (A era da informação: economia, sociedade e cultura, v.1) São Paulo: Paz e terra, 1999.

CASTRO, Bruna Azevedo de; ARGUELLO, Katie Silene Cáceres; COSATE, Tatiana Moraes. Capitalismo de vigilância e racismo: o reconhecimento facial automatizado como técnica de controle sobre o corpo negro. São Paulo, **Revista jurídica direito e paz.** Ano XVI, n. 47, 2º Semestre, 2022, pp. 79-101.

CMSP. **Pesquisa de Caracterização Socioeconômica do Passageiro e seus Hábitos de Viagem**. 2018, Disponível em: https://transparencia.metrosp.com.br/dataset/pesquisa-de-caracteriza%C3%A7%C3%A3o-socioecon%C3%B4mica-do-usu%C3%A1rio-e-seus-h%C3%A1bitos-de-viagem. Acesso em: 17 ago. 2024.

COELHO, Ana. **Programa de monitoramento da Prefeitura de SP começa com 200 câmeras instaladas.** CNN Brasil, 27 de outubro de 2023. Disponível em: https://www.cnnbrasil.com.br/nacional/programa-de-monitoramento-da-prefeitura-de-sp-comeca-com-200-cameras-instaladas/. Acesso em: 18 jun 2024.

CONSÓRCIO AL SUR. **Reconocimiento facial en América Latina:** Tendencias en la implementación de una tecnología perversa. 2021. Disponível em: https://estudio.reconocimientofacial.info/reports/ALSUR-Reconocimiento_facial_en_Latam-ES.pdf. Acesso em: 18 jul 2024.

DEUS GARCIA, R. **O uso da tecnologia e a atualização do modelo inquisitorial:** gestão da prova e violação de direitos fundamentais na investigação policial na política de drogas. Dissertação (Mestrado em Direito) Universidade de Brasília, Brasília, 2015. 222 p.

DEUS GARCIA, R. **Processo penal e algoritmos o direito à privacidade aplicável ao uso de algoritmos no policiamento.** (Doutorado em Direito) – Faculdade de Direito, Universidade de Brasília. Brasília, 2022. Disponível em: http://icts.unb.br/jspui/bitstream/10482/44902/1/2022_RafaeldeDeusGarcia.pdf. Acesso em: 13 jul 2024.

DPERJ. **Reconhecimento de pessoas:** delegacias não cumprem resolução do CNJ. 2024. Disponível em: https://defensoria.rj.def.br/noticia/detalhes/29549-Reconhecimento-de-pessoas-delegacias-nao-cumprem-resolucao-do-CNJ. Acesso em: 29 jul 2024.

DPERJ. **Relatório sobre reconhecimento fotográfico em sede policial.** Diretoria de Estudos e Pesquisas de Acesso à Justiça. 2020. Disponível em: https://www.defensoria.rj.def.br/uploads/arquivos/54f8edabb6d0456698a068a65053420c.pdf. Acesso em: 30 jul. 2024.

DUARTE, Daniel Edler; CEIA, Eleonora Mesquita. **Tecnologia, Segurança e Direitos:** Os usos e riscos de sistemas de reconhecimento facial no Brasil. Organização: Daniel Edler Duarte e Eleonora Mesquita Ceia. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (pdf). Disponível em: https://www.kas.de/documents/265553/0/Tecnologia%2C+Seguran%C3%A7a+e+Direitos+VF.pdf/8c70ec5a-1adf-69a8-39fb-f7afb1f76e91?version=1.0&t=1696517977110. Acesso em: 15 ago. 2024.

DUARTE, Evandro Piza; GARCIA, Rafael de Deus. O uso de novas tecnologias de comunicação no sistema de justiça criminal: tensões entre propostas de eficiência da justiça e a maximização dos efeitos negativos do sistema penal. **Revista de Processo**, v. 261, nov. 2016, p. 445-464.

DUARTE, Renata, *et al*. Aplicação dos Sistemas Biométricos de Reconhecimento Facial na Segurança Pública. **Brazilian Journal of Forensic Sciences, Medical Law and Bioethics.** v. 11, n. 1, p. 1-21, 2021. Disponível em https://www.ipebj.com.br/bjfs/index.php/bjfs/article/view/848. Acesso em: 14 jul 2024.

ESTADOS UNIDOS DA AMÉRICA. **Face Recognition Vendor Test (FRVT).** National Institute of Standard and Tecnology. 2024 Disponível em: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt, 2024. Acesso em: 20 jul. 2024.

FACEONLIVE**, History of Facial Recognition:** Evolution & Insights, 2023. Disponível em: https://faceonlive.com/history-of-facial-recognition-evolution-insights/. Acesso em: 15 jul 2024.

FERNANDES, Fernando Andrade; RESENDE, Ana Paula Bougleux Andrade. Regulamentação do tratamento automatizado de dados pessoais em matéria penal. **Suprema: revista de estudos constitucionais,** Brasília, v. 3, n. 1, p. 471-500, jan./jun. 2023. DOI: https://doi.org/10.53798/suprema.2023.v3.n1.a207.

FOCAULT, Michael. **Vigiar e punir:** nascimento da prisão. Tradução: Raquel Ramalhete. 42ª ed., Petrópolis Rio de Janeiro: Vozes, 2014.

FREITAS, Hyndara. **Câmeras de reconhecimento facial se multiplicam em São Paulo:** Medida é aposta do governo estadual e da prefeitura para a área da segurança pública. Veja, 2024. Disponível em: https://vejasp.abril.com.br/cidades/cameras-reconhecimento-facial-sp/. Acesso em: 17 jul 2024.

FUTURE OF LIFE INSTITUTE**. The EU Artificial Intelligence Act. Up-to-date developments and analyses of the EU AI**, 2024. Disponível em: https://artificialintelligenceact.eu/. Acesso em: 20 ago 2024.

G1. **'Medo, frustrado e constrangido', diz homem detido por engano em estádio após erro do sistema de reconhecimento facial**. G1. 21/04/2024. 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: 18 jul 2024.

GATES, Kelly. **Our biometric future: facial recognition technology and the culture of surveillance. (e-book)**, 2011. Disponível em: https://eholgersson.wordpress.com/wp-content/uploads/2019/08/our-biometric-future-facial-recognition-technology-and-the-culture-of-surveillance.pdf. Acesso em: 15 jul 2024.

HIRATA JR., R.; ARAÚJO, Rafael Will M. de; ABELLO. Antonio A. **Parecer Internet Lab**. Março 2021. Disponível em: https://internetlab.org.br/wp-content/uploads/2022/03/Parecer-Metro-de-Sao-Paulo.-Reconhecimento-facial.pdf. Acesso em: 12 ago. 2024.

INSTITUTO IGARAPÉ. **Desde 2011 vem sendo utilizado o Reconhecimento Facial no Brasil**. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/#:~:text=O%20primeiro%20caso%20reportado%2C%20ainda,intuito%20de%20controlar%20evas%C3%A3o%20escolar. Acesso em: 16 de maio de 2024.

ISRANI, Ellora Thadaney. **When an Algorithm Helps Send You to Prison**. 2017. Disponível em: https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html. Acesso em: 19 jul 2024.

KREMER, Bianca, NUNES, Pablo, LIMA, Thallita, G.L. **Racismo algorítmico [livro eletrônico].** Rio de Janeiro: CESeC, 2023.

KREMER, Bianca; SILVA, Fernanda dos Santos Rodrigues. A LGPD Penal e a lacuna regulatória no tratamento de dados pessoais sensíveis por profissionais de segurança. *In:* **Tecnologia, Segurança e Direitos: Os usos e riscos de sistemas de reconhecimento facial no Brasil**. Organização Daniel Edler Duarte e Eleonora Mesquita Ceia. Rio de Janeiro: Konrad Adenauer Stiftung, 2022. Dados eletrônicos (pdf). Disponível em: file:///C:/Users/mathe/Downloads/TecnologiaSeguranaeDireitosVF.pdf. Acesso em: 14 ago 2024.

LAMBERT, Warren (org**.). Issues with facial recognition technology:** Technology in a globalizing world. New York, NY: Nova Science Publishers, Inc, 2021.

LOPES JR., Aury. **Direito Processual Penal**. 19ª ed., São Paulo: SaraivaJur, 2022.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da Hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MARQUES, Ana. **China testa "robotáxis" autônomos nas ruas de Shenzhen**. Tecnoblog, 2021. Disponível em: https://tecnoblog.net/noticias/china-testa-robotaxis-autonomos-nas-ruas-de-shenzhen/. Acesso em: 10 jul. 2024.

MARX, Karl. **Crítica da filosofia do direito de Hegel**. Tradução de Rubens Enderle e Leonardo de Deus; [supervisão e notas Marcelo Backes]. 2.ed revista. São Paulo: Boitempo, 2010.

MEIRELLES, Hely Lopes: **Direito Administrativo Brasileiro.** 23ª ed., São Paulo, Editora RT, 1998.

MELO, Paulo Victor; SERRA, Paulo. **Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. Comunicação e sociedade [Online]**, ed. 42, 2022. Disponível em: http://journals.openedition.org/cs/8111. Acesso em; 16 jul. 2024.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 13. ed. rev. e atual. – São Paulo: Saraiva Educação, 2018. – (Série IDP).

MILANEZ, Giovana. A utilização de tecnologias de reconhecimento facial para fins de segurança pública e persecução penal no Brasil: mapeando discussões e possíveis caminhos regulatórios, pp. 91-126. *In:* **Constituição, direito penal e novas tecnologias.** coordenação: Gilmar Ferreira Mendes; Matheus Pimenta de Freitas, São Paulo: Almedina, 2023.

MILLAN, Samantha. **Morador do Alemão é abordado por policiais em Bonsucesso devido a erro de reconhecimento facial**. Vozes da Comunidade, 19 abr. 2024. Disponível em: https://vozdascomunidades.com.br/casos-de-policia/morador-do-alemao-e-abordado-por-policiais-em-bonsucesso-devido-a-erro-de-reconhecimento-facial/. Acesso em: 18 jul. 2024.

MONARD, M.C.; BARANAUSKAS, J.A. Conceitos de aprendizado de máquina. *In:* REZENDE, S.O. **Sistemas inteligentes:** fundamentos e aplicações. São Carlos: Manole, 2003.

NILSSON, Nils J. **The Quest for Artificial Intelligence.** Cambridge University Press. ISBN 978-1-139-64282-8 (e-book), 2009. Disponível em: https://ai.stanford.edu/~nilsson/QAI/qai.pdf. Acesso em: 10 jul 2024.

NISSENBAUM, Helen; INTRONA, Lucas. **Facial Recognition Technology A Survey of Policy and Implementation Issues.** The Center for Catastrophe Preparedness & Response, New York University, 2009.

NUNES, Pablo; LIMA, Thallita Gabriele Lopes; CRUZ, Thaís Gonçalves. **O sertão vai virar mar: Expansão do reconhecimento facial na Bahia**. Rio de Janeiro: CESeC.

NUNES, Pablo. **Coleção Panorama: Reconhecimento Facial**. Rio de Janeiro: CESeC, 2023.

NUNES, Pablo. **Monitor de Novas Tecnologias na Segurança Pública do Brasil**. 2024, Disponível em: https://www.opanoptico.com.br/#mapa. Acesso em: 18 jul 2024.

OLIVEIRA, L.V. *et al*. **Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil.** Rev. Tecnol. Soc., Curitiba, v. 18, n. 50, p.114-135, jan./mar., 2022. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/12968. Acesso em: 15 jul 2024.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Convenção Americana de Direitos Humanos ("Pacto de San José de Costa Rica")**, 1969. Disponível em: https://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm. Acesso em: 17 jul. 2024.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

PACELLI, Eugênio. **Curso de Processo Penal**. 26ª ed., rev. atual. e ampl. São Paulo: Editora Juspodivm, 2022.

PAGANONI, Maria Cristina. ***Ethical Concerns over Facial Recognition Technology***. Anglistica AION an Interdisciplinary Journal, v. 23, n. 1, p. 83-92, 2019, p. 83 ss. Disponível em: http://www.serena.unina.it/index.php/anglistica-aion/article/view/8616. Acesso em: 14 jul. 2024.

PEREIRA, Rui Soares. Sobre o uso de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) para fins de segurança pública e de aplicação coerciva da lei: reflexões a propósito do da proposta de regulamento europeu sobre a inteligência artificial. **Revista da Faculdade de Direito da Universidade de Lisboa,** n. 63 (1/2), 2022, pp. 839-865. Disponível em https://www.fd.ulisboa.pt/wpcontent/uploads/2022/12/Rui-Soares-Pereira.pdf. Acesso em: 20 ago. 2024.

PETRESCU, Relly Victoria Virgil. **Face Recognition as a Biometric Application. Journal of Mechatronics and Robotics**. 2019, Volume 3: pp. 237-257. Disponível em: https://thescipub.com/pdf/jmrsp.2019.237.257.pdf. Acesso em: 17 jul 2024.

PINHO, Luana C. P. da Rocha. **Reconhecimento Facial e Justiça Penal Facial:** Uma análise à luz das propostas de regulamento da União Europeia sobre a Inteligência Artificial e o direito português. Dissertação (Mestrado no 2º Ciclo de Estudos em Ciências Jurídico-Forenses), Faculdade de Direito da Universidade de Coimbra, Coimbra, 2024.

PMERJ. **Polícia militar atinge marca de 200 prisões com auxílio do sistema de reconhecimento facial.** Rio de Janeiro, 2024. Disponível em: https://sepm.rj.gov.br/2024/06/policia-militar-atinge-marca-de-200-prisoes-com-auxilio-do-sistema-de-reconhecimento-facial/. Acesso em: 18 jul 2024.

QUEIROZ, Paulo de Souza. **Direito Processual Penal – Introdução**. 3. Ed. rev. atual. e ampl. São Paulo: Editora JusPodivm, 2022.

QUIJANO, Aníbal. Colonialidade do Poder e Classificação Social. **Epistemologias do Sul.** org. Boaventura de Sousa Santos, Maria Paula Meneses. – (CES), 2009.

RAMOS, Silvia, *et al*. **Pele alvo: a bala não erra o negro**. Rio de Janeiro: CESeC, 2023. Disponível em:

https://drive.google.com/file/d/1kypOaUP0ZgSAAu2NfU8xuZEOeKkbjMAe/view. Acesso em: 1 jul 2024.

RECENT CASES, Criminal Law – Sentencing Guidelines – State v.
Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing, **Harvard Law Review** 130, 2017, pp. 1531, 1534. Disponível em: https://harvardlawreview.org/print/vol-130/state-v-loomis/. Acesso em: 10 ago. 2024.

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

REPÚBLICA POPULAR DA CHINA. **China mulls first nationwide comprehensive guidelines for use of facial recognition technology.** 08 ago 2023. Ministry of Justice of the People's Republic of China. Disponível em: http://en.moj.gov.cn/2023-08/10/c_909702.htm. Acesso em: 17 jul 2024.

RIBEIRO, Micaela Mayara; FERMENTÃO, Cleide A. G. R**. Proteção de dados pessoais na era do capitalismo de vigilância em defesa dos direitos personalíssimos da pessoa**: uma possibilidade ou mero devaneio? VirtuaJus, Belo Horizonte, v. 8, n. 15, p. 245-252, 2o sem. 2023 – ISSN 1678-3425.

RODAS Sérgio. **Justiça do Rio absolve músico preso com base em reconhecimento por foto**. Consultor Jurídico. 10 de junho de 2021. Disponível em: https://www.conjur.com.br/2021-jun-10/musico-preso-base-reconhecimento-foto-absolvido/, Acesso em: 10 jul 2024.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 142.

RUBACK, Lívia; AVILA, Sandra; CANTERO, Lucia. Vieses no Aprendizado de Máquina e suas Implicações Sociais: Um Estudo de Caso no Reconhecimento Facial. *In:* **Workshop sobre as implicações da computação na sociedade (wics).** 2021, Evento Online. Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 90-101. Disponível em: https://sol.sbc.org.br/index.php/wics/article/view/15967. Acesso em: 26 ago 2024.

SÃO PAULO. Tribunal de Justiça de São Paulo**. Ação Civil Pública nº 1010667-97.2022.8.26.0053**, 6ª Vara de Fazenda Pública. Juiz(a): Cynthia Thome, Data de distribuição: 03 de março de 2024, 2024. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=1H000LRDS0000&processo.foro=53&processo.numero=1010667-97.2022.8.26.0053. Acesso em: 17 ago. 2024.

SCHWAB, Klaus. **A quarta revolução industrial.** Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SILVA, Tarcízio. **Racismo algorítmico**: inteligência artificial e discriminação nas redes digitais. São Paulo: Edições Sesc São Paulo, 2022.

SILVEIRA, Sérgio Amadeu da. Discursos sobre regulação e governança algorítmica. **Revista Estudos de sociologia**. Araraquara/SP, v.25, n.48, p.63-85 jan.-jun. 2020. Disponível em: Discursos sobre regulação e governança algorítmica | Semantic Scholar. Acesso em: 18 jul. 2024.

SIMONITA, Tom. **Face Recognition Is Being Banned—but It's Still Everywhere: Two dozen cities and states prohibit use of the tech. But it's on phones and is increasingly used in airports and in banks.** Wired. 22 dez 2021. Disponível em: https://www.wired.com/story/face-recognition-banned-but-everywhere/. Acesso em: 19 jul 2024.

SOUSA, Aléxia. **Mulher é solta após ser detida por erro no sistema de reconhecimento facial no Rio.** Uol, 2024. https://www1.folha.uol.com.br/cotidiano/2024/01/mulher-e-solta-apos-ser-detida-por-erro-no-sistema-de-reconhecimento-facial-no-rio.shtml. Acesso em: 18 jul 2024.

SOUZA, Ricardo Calmona. A Emenda Constitucional nº 115 e o direito de proteção de dados na persecução penal: a (des)preocupação com a necessidade de uma "LGPD Penal". **Revista de Direito da Defensoria Pública do Estado do Rio de Janeiro**, nº 32, 2022, pp. 109-122.

WIMMER, Miriam; DONEDA, Danilo. **"Falhas de IA" e a Intervenção Humana em Decisões Automatizadas: Parâmetros para a Legitimação pela Humanização**. Dossiê – Inteligência Artificial, Ética e Epistemologia. RDP, Brasília, Volume 18, n. 100, 374-406, out./dez. 2021.

YOUTUBE. **Anti-crime? Kim Kataguiri faz perguntas ao Pablo Marçal sobre planos para segurança de São Paulo!** Cortes do Inteligência. 2024. Disponível em: https://www.youtube.com/watch?v=Cz-Va8HMq9c. Acesso em: 10 ago 2024.

YOUTUBE. **SecurOS FaceX Features. Intelligent Security Systems**. 19 abr. 2022. Disponível em: https://www.youtube.com/watch?v=8tPHZ49SlcI. Acesso em: 19 ago 2024.

ZAFFARONI, Eugenio Raul. **Em busca das penas perdidas**: a perda da legitimidade do sistema penal. Tradução: Vania Romano Pedrosa, Almir Lopez da Conceição. Rio de Janeiro: Revan, 2014.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

ZULEHNER, Bruno. EU Artificial Intelligence Act: Regulating the Use of Facial Recognition Technologies in Publicly Accessible Spaces, **EU Law Working Papers,** nº. 91, Stanford-Vienna Transatlantic Technology Law Forum, 2024.