XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

CARLOS MARDEN CABRAL COUTINHO

JOSÉ RENATO GAZIERO CELLA

YURI NATHAN DA COSTA LANNES

D597

Direito, Governança e novas tecnologias I [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Carlos Marden Cabral Coutinho; José Renato Gaziero Cella; Yuri Nathan da Costa Lannes. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-813-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

No XXX Congresso Nacional do CONPEDI, realizado nos dias 15, 16 e 17 de novembro de 2023, o Grupo de Trabalho - GT "Direito, Governança e Novas Tecnologias I", que teve lugar na tarde de 15 de novembro de 2023, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados 23 (vinte e três) artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente na Faculdade de Direito do Centro Universitário Christus - UNICHRISTUS.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em cinco blocos, quais sejam a) temas de inteligência artificial; b) temas de liberdade de expressão e fake news; c) temas de proteção de dados pessoais; d) temas de cidadania, democracia, constituição e direitos; e e) temas de regulação.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema "Direito, Governança e Novas Tecnologias". Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. Carlos Marden Cabral Coutinho - Centro Universitário Christus

Prof. Dr. José Renato Gaziero Cella - Atitus Educação

Prof. Dr. Yuri Nathan da Costa Lannes - Faculdade de Direito de Franca

RECONHECIMENTO FACIAL: TECNOLOGIA DE VIGILÂNCIA ENVIESADA E DIRECIONADA

FACIAL RECOGNITION: BIASED AND TARGETED SURVEILLANCE TECHNOLOGY

Stephanny Resende De Melo
Roberta Hora Arcieri Barreto
Rayza Ribeiro Oliveira

Resumo

O uso de novas tecnologias como o reconhecimento facial pela segurança pública vem crescendo rapidamente nos últimos anos no Brasil, especialmente, em eventos e festas, com identificação pessoal em massa. Por esse motivo, é importante averiguar os riscos decorrentes dessa tecnologia, por servir de instrumento de vigilância da vida das pessoas, podendo ferir direitos, especialmente, a liberdade, ao serem utilizados algoritmos enviesados e banco de dados nem sempre bem tratados. Assim, questiona-se: o uso do reconhecimento facial pelas forças de segurança pública reforça a seletividade racial por meio de uma vigilância direcionada para as minorias, a ponto de gerar discriminações? Tem-se, portanto, como objetivo central analisar como o uso do reconhecimento facial pelas forças de segurança pública reforça a seletividade racial por meio de uma vigilância direcionada para as minorias, a ponto de gerar mais discriminações e exclusões. Para tanto, dividiu-se o desenvolvimento em tópicos interligados para se chegar ao pensamento final, em que, primeiro, aprofundou-se sobre como se desenvolvem o reconhecimento facial, o racismo institucionalizado nas polícias e as discriminações que a tecnologia gera; para só então tratar sobre a vigilância em massa que fere direitos mínimos, como a liberdade, em prol de um discurso ilusório de maior efetividade da segurança pública. A metodologia empregada para a pesquisa foi a partir de abordagem qualitativa do problema, baseando-se em pesquisa de natureza exploratória com procedimentos de pesquisa documental e bibliográfica.

Palavras-chave: Discriminação, Minoriais raciais, Reconhecimento facial, Novas tecnologias, Vigilância

Abstract/Resumen/Résumé

The use of new technologies as the facial recognition for public security has been growing rapidly in recent years in Brazil, especially at events and parties, with mass identification. For this reason, it is important to investigate the risks arising from this technology, as it serves as a basis for people's lives and can harm rights, especially freedom, when biased algorithms and databases that are not always well treated are used. Thus, the objective is to analyze how the use of facial recognition by public security forces reinforces racial selectivity through surveillance aimed at minorities, to the point of generating more discrimination and exclusions. To this end, the development was divided into interconnected topics to arrive at

the final thought, in which, first, we delved deeper into how facial recognition, institutionalized racism in the police and the discrimination that technology generates develop; and only then deal with mass surveillance that violates minimum rights, such as freedom, in favor of an illusory discourse of greater effectiveness of public security. The methodology used for the research was a qualitative approach to the problem, based on exploratory research with documentary and bibliographical research.

Keywords/Palabras-claves/Mots-clés: Discrimination, Facial recognition, New technologies, Racial minorities, Surveillance

1 INTRODUÇÃO[1]

O reconhecimento facial é uma tecnologia relativamente recente na área da segurança pública, mas que vem crescendo exponencialmente ao longo dos últimos anos, especialmente, em eventos e festas, sendo utilizado tanto pelos governos quanto pela iniciativa privada. Por se caracterizar como tecnologia que trata dados sensíveis, urge por análise e aprofundamento de sua aplicação, pois tem servido para guiar as pessoas em tomada de decisões que afetam a vida e os direitos de todos. Diante de sua formatação a partir de algoritmos e dos bancos de dados das mais diversas bases, como os geridos pelos órgãos de segurança pública, faz-se mister avaliar sua não-neutralidade e possíveis erros no processamento, no intuito de se garantir a efetivação do Estado Democrático de Direito.

No Brasil, a referida tecnologia tem sido empregada pela gestão estatal para identificação de supostos criminosos com mandados de prisão em aberto e para a abordagem de indivíduos com atitudes compreendidas como suspeitas; pelo Poder Judiciário, para prever a reincidência e sopesar as sentenças; e, nos setores privados, direcionadas ao consumidor por meio das redes sociais, entre outros. Nesse sentido, levantamento realizado, com vistas a mapear os estados brasileiros que estão utilizando ou possuem, em estágio de implementação, o reconhecimento facial na segurança pública, aponta para o quantitativo de 20 (vinte) estados[2], demonstrando o seu rápido avanço.

À vista disso, questiona-se: o uso do reconhecimento facial pelas forças de segurança pública reforça a seletividade racial por meio de uma vigilância direcionada para as minorias, a ponto de gerar discriminações? Considerando essa utilização crescente no âmbito estatal, justifica-se a necessidade de se empreender pesquisas que busquem compreender como se desenvolve essa tecnologia e, por conseguinte, analisar os motivos das suas falhas que geram, por vezes, humilhações e constrangimentos a indivíduos a ela submetidos, mas, principalmente, restrições à liberdade, à privacidade.

Desta feita, o objetivo do presente artigo é analisar como o uso do reconhecimento facial pelas forças de segurança pública reforça a seletividade racial por meio de uma vigilância direcionada para as minorias, a ponto de gerar discriminações.

[1] O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) – Código de Financiamento 001.

[2] Os Estados que já utilizam: Roraima, Pará, Ceará, Rio Grande do Norte, Bahia, Rio de Janeiro, São Paulo, Mato Grosso do Sul, Goiás, Santa Catarina. Os que estão em processo de implementação são: Amapá, Acre, Rondônia, Maranhão, Piauí, Paraíba, Pernambuco, Sergipe, Paraná e Rio Grande do Sul. Os que estão na fase de estudos: Mato Grosso, Minas Gerais, mais o Distrito Federal. (DAMASCENO; FERNANDES, 2021).

Assim, o trabalho foi dividido em dois tópicos de desenvolvimento para consubstanciar o que se pretende demonstrar. Para tanto, no segundo capítulo, busca-se conceituar e explanar a respeito da tecnologia do reconhecimento facial, para uma compreensão quanto a sua efetividade na segurança pública. Além disso, verificam-se formas de utilização desses sistemas, considerando possíveis erros e falhas que podem ser cometidos, demonstrando sua relação com o racismo instituído nas forças policiais e em suas abordagens. No terceiro capítulo, discute-se se o uso desses *softwares* pode ocasionar uma sociedade de vigilância ainda mais discriminatória da que é imposta atualmente, ao ferir direitos básicos, o que resultaria na limitação da liberdade de todos de uma forma irreversível.

A metodologia empregada na pesquisa foi realizada por uma abordagem qualitativa do problema com foco em aprofundar subjetivamente acontecimentos sociais que impactam a vida das pessoas de um modo geral. Desta feita, baseia-se em uma pesquisa de natureza exploratória, no intuito de estreitar ligação com o problema, utilizando-se dos procedimentos metodológicos da pesquisa documental e bibliográfica.

Desse modo, realiza-se a pesquisa por intermédio da análise de documentos e textos científicos que guardam pertinência com o tema, como livros físicos e eletrônicos, blog de pesquisadores referências na área, artigos científicos selecionados a partir de descritores (tais como "vigilância e segurança pública", "direito e reconhecimento facial" e "algoritmos, vigilância e direito à liberdade") em bancos de dados como *Scielo* e *Google* acadêmico. Utiliza-se, especialmente, a opinião comprovada de pesquisadores e de seus levantamentos no intuito de buscar uma confirmação da hipótese suscitada e consubstanciar o discurso.

2 A IDENTIFICAÇÃO DA FACE COMO INSTRUMENTO DE DISCRIMINAÇÃO

O reconhecimento facial passa por alguns procedimentos até se chegar ao propósito final, dessa forma, primeiro, por meio de vídeo ou foto, a face de uma pessoa é capturada e armazenada para que o sistema, em um segundo momento, possa analisar e elaborar um padrão facial por meio da distância de alguns pontos, como olhos, boca e/ou testa. Só então, compara, de forma matemática, a um banco de dados preexistente. Neste momento, pode-se confrontar aquele padrão com um outro definido e único, que seria a verificação, ou pode equiparar efetivamente com um banco de dados para se fazer a identificação. (WECHSLER, 2007).

Para melhor compreensão dessa tecnologia, de modo mais técnico, Pablo Nunes conceitua que:

> O reconhecimento facial é uma forma de biometria, que é a ligação entre um elemento único do corpo humano de um indivíduo com uma unidade de registro. O elemento corporal utilizado pode ser a digital, a face, o modo de caminhar. As unidades de registro mais comuns são os cadastros, como o Registro Geral (RG), o número da Previdência Social ou a conta bancária. A parte do corpo utilizada na biometria, seja a digital ou a face, nunca é analisada por completo. Isto quer dizer que são escolhidos alguns pontos do rosto ou do dedo e, com base nas distâncias entre esses pontos, é calculada a probabilidade de aquela digital ou de aquela face ser da pessoa cadastrada no banco de dados. (NUNES, 2019, p. 67-68).

Importante é o levantamento realizado pelo Laboratório de Políticas Públicas e Internet (LAPIN) sobre quais empresas desenvolvedoras do reconhecimento facial os Estados e Municípios brasileiros estão realizando contratos e comprando tal tecnologia. A maioria delas, quase todas, são fornecedoras estrangeiras, especialmente, da China, Israel, Reino Unido e dos Estados Unidos. Países estes que não contém a diversidade racial como a do Brasil, desenvolvendo sistemas com base na sua sociedade, contribuindo para que os enviesamentos estejam presentes quando aplicadas neste país. (REIS; ALMEIDA; DA SILVA; DOURADO, 2021).

Outrossim, “os erros aumentam quando são analisadas imagens com resolução baixa e provenientes de segmentos de vídeo, assim como devido a variações na iluminação, fundo da imagem, pose, expressão facial, sombras e distância da câmera” (RODRIGUES, 2019). Também é fácil enganar as câmeras, modificando o rosto propositalmente, por meio de pinturas ou máscaras, pois há uma limitação de identificação no videomonitoramento, e isso foi o que efetivamente ocorreu em Hong Kong (NOVAK, 2019), ocasião em que manifestantes contra a implementação da tecnologia utilizaram-se dessas táticas para não serem reconhecidos.

A precisão de um sistema como esse é complexa, dependente de um banco de dados bem estruturado, que as imagens tenham um padrão mínimo de qualidade, treinamento dos algoritmos e dos parâmetros que serão considerados para a identificação. Se qualquer um desses pontos não corresponder ao desejado, falhas e/ou erros ocorrerão causando constrangimentos, humilhações ou ainda inutilizarão o sistema. (VENTURINI, 2021).

Além do que, pesquisa realizada pela organização *Consumentenbond* verificou que o uso do reconhecimento facial em *smartphones* de diversas marcas expressivas no âmbito internacional apresentam muitas falhas, como identificar uma fotografia correlacionando ao rosto de uma pessoa. (ZIZI, 2019). Ou seja, procedimentos simples continuamente manifestam incoerências e inexatidões que não deveriam ocorrer por simplesmente não serem de complicada utilização. Assim, é possível pensar que, se sistemas simples apresentam falhas

grotescas, quando complexos, como o reconhecimento facial na segurança pública, serão ainda piores.

Foi o que aconteceu, por exemplo, na implementação de tecnologias de reconhecimento facial na capital inglesa, em que foram reunidas fotos de mais de 2.400 suspeitos e geradas apenas 8 prisões. Ou, no caso do Brasil, durante seu uso na Micareta de Feira de Santana/BA, o sistema de videomonitoramento coletou 1,3 milhões, gerou 103 alertas, sendo identificados 18 foragidos e 15 foram efetivamente presos; sendo que o governo da Bahia investiu mais de R$ 18 milhões para sua implantação. (SILVA, 2021).

Segundo relatório produzido pelo Panóptico (NUNES, 2022), no Rio de Janeiro, em 2019, em uma implementação e posterior ampliação do número de câmeras com reconhecimento facial, em 10 (dez) dias, foram realizadas apenas 11 (onze) detenções, sendo que 07 (sete) eram alarmes falsos, com a utilização de 10 (dez) policiais para suprir a demanda e investimento de R$ 726.789,00 (setecentos vinte e seis mil setecentos e oitenta e nove reais) para esse deslocamento.

Os erros que esse sistema tecnológico tem causado são extremamente grosseiros de uma forma geral, causando humilhações, constrangimentos, prisões, traumas, entre tantos direitos feridos substancialmente. Não foi diferente quando um adolescente foi confundido com um traficante ao ser identificado por câmeras de segurança e abordado por policiais dentro do metrô. (SILVA, 2019). Ou quando um rapaz foi preso dentro da sua própria casa por ter sido identificado de forma equivocada por câmeras, permanecendo detido por mais de um dia, tendo efetuado pagamento de fiança. (HILL, 2020).

O grupo independente *Big Brother Watch* (DEARDEN, 2019), por meio de um pedido de liberdade de informação, obteve dados do uso do reconhecimento facial e apurou que, entre 2016 e 2018, a taxa de falsos positivos do software foi de 96% dos casos e que essa implementação tinha custado 222.000 libras para os cofres públicos.

Os Estados e Municípios brasileiros têm implementado a tecnologia sob o discurso de que há um grande custo-benefício envolvido, mas, em contrapartida, não fornecem dados suficientes para que tal afirmativa seja comprovada. Essa comprovação é necessária para que se tenha em mente se a coleta massiva de dados e a vigilância exacerbada efetivamente compensa em prol da segurança (REIS; ALMEIDA; DA SILVA; DOURADO, 2021, p. 17), especialmente, porque, apesar de não se terem dados públicos exatos, diversos setores da sociedade, como pesquisadores, têm-se utilizado de informações de um modo geral para comprovar que as discriminações advindas estão ocorrendo em larga escala.

À procura de um sistema de reconhecimento facial que surta efeito contra a criminalidade, os governos realizam testes sem se preocupar com as consequências que isso vai trazer para as pessoas. É como um pensamento de "vamos testar e ver no que dar". Um dos exemplos foi o que ocorreu no Rio de Janeiro em 2019 quando uma mulher foi detida ao ser identificada pela tecnologia como outra pessoa que já estava presa. Além de todos os problemas que o próprio reconhecimento facial traz, ainda surge o do banco de dados que muitas vezes está desatualizado, como foi o caso. (ALBUQUERQUE, 2019).

Os sistemas automatizados disfarçam as discriminações decorrentes, de forma a naturalizar as diversas exclusões, somente sendo percebida e forçado um debate pelas pessoas que frequentemente sofrem com essas tecnologias. (GILLIOM; MONAHAN, 2013).

Aquela ideia advinda do ditado popular "quem não deve, não teme", não pode ser utilizada para defender o uso do reconhecimento facial pela segurança pública, mesmo com um discurso de que ajudaria na diminuição da criminalidade no país, uma vez que o sistema comete muitos erros ao analisar o padrão de comportamento humano ou por algoritmos falhos, assim pessoas inocentes podem ser presas com grande frequência. (VICENTE, 2019).

Um sistema impreciso como esse facilita a atuação estatal no sentido de que retira o dever do Estado de provar que aquele suspeito é o criminoso, repassando essa obrigação para quem vai se defender, em uma real inversão da presunção de inocência.

Sob a justificativa de não haver tomada de decisão discriminatória, como ocorre nas condutas dos agentes de polícia, o reconhecimento facial tem sido utilizado com a máxima de garantir a segurança pública, ocorre que, não há transparência sobre os dados que são utilizados e a forma do seu tratamento, sequer sobre como deve ocorrer a correção da ocorrência de possíveis vieses. (BRAGA, 2020).

A maior parte dos bancos de dados utilizados pela polícia são os bancos de mandados de prisão em aberto ou de pessoas que já foram presas, assim, os lançamentos pretéritos servem para os novos registros, criando um ciclo de retroalimentação por serem repositórios enviesados em constante renovação interligada, perpetuando os preconceitos já existentes.

A polícia acaba por executar uma política criminal etiquetada (HASSEMER, 20005) em que a regra atribuída para as pessoas pretas segue um único fluxo, de invisibilidade e inexistência filtrada pelo sistema penal, seu único lugar de vinculação, a qual seu sentimento deve pertencer. Assim, "Em suma, os olhos que, geralmente, não nos enxergam são os mesmos olhos que nos veem tão somente para nos condenar". (DIAS, 2020, p. 351).

Demonstrou-se que em 2011, em São Paulo, para cada grupo de 100 mil habitantes negros, 1,4 foi morto pela polícia, ao passo que, para cada grupo de 100 mil habitantes brancos,

foi morto 0,5. Já no Rio de Janeiro, para a mesma quantidade de habitantes, 0,9 branco é morto pela polícia e 3,6 negros são mortos. Além disso, a vigilância policial também é organizada de forma racializada, ou seja, visam e suspeitam mais das pessoas negras ocasionando em prisões em flagrantes, diferente dos brancos que são menos vigiados. Nos estados de Minas Gerais e São Paulo, por exemplo, a taxa de flagrantes de negros são mais que o dobro da verificada para brancos. (SINHORETTO, 2014).

Conforme apontou o grupo de pesquisa, ao questionar oficiais e praças da Polícia Militar de São Paulo, Rio de Janeiro, Minas Gerais e Distrito Federal, todos negaram haver uma filtragem racial em suas atividades de policiamento, informando que são guiados pela fundada suspeita. Entretanto, quando tentam explicar quais elementos compõem essas desconfianças, fica claro que advém de um grupo social específico, caracterizado pelo estilo de vestir, andar e falar que remete a aspectos da cultura negra, ou, pelo menos, a estereótipos vinculados a essa raça. (SINHORETTO, 2014).

O problema do racismo não é somente das forças policiais, mas sim de toda sociedade brasileira, não devendo sua solução ser reduzida à tecnologia ou a outras de cunho rápido e simples. O racismo é um "problema social amplo o suficiente para que de sua solução dependa a própria possibilidade de nos considerarmos uma democracia". (BUENO; PACHECO; NASCIMENTO; MARQUES, 2022).

O uso do reconhecimento facial em massa também é atraído pela ideia de benefício no que diz respeito de evitar que mais discriminações sejam realizadas pelos policiais pelo fato de a polícia conseguir as informações das abordagens pela própria tecnologia, evitando que saiam de forma ostensiva pelas ruas. Ocorre que, não se pode perder de vista que os dados já obtidos nos bancos estão enviesados pelas operações pretéritas e pela própria construção dos dispositivos, como amplamente detalhado em seção específica.

Os casos de racismo no reconhecimento facial não fogem da regra do enviesamento nas tecnologias. Assim, caso os bancos de dados utilizados sejam os mandados de prisão em aberto, é ainda pior já que em sua maioria já prendem e suspeitam mais de pessoas negras, o que fará com que os algoritmos trabalhem nesse sentido, buscando mais negros, com policiais abordando ainda mais negros inocentes. O'Neil (2020, p. 173) relata que:

> A própria polícia gera novos dados, o que justifica mais policiamento. E nossos presídios se enchem de centenas de milhares de pessoas condenadas por crimes sem vítimas. A maioria delas vem de bairros empobrecidos, e a maioria é negra ou hispânica. Então mesmo que um modelo não enxergue a cor da pele, o resultado o faz. Em nossas cidades amplamente segregadas, a localização geográfica é um proxy altamente eficaz para raça.

Corroborando tal pensamento, o levantamento da Rede de Observatórios da Segurança Pública, demonstrou que 90,5% das pessoas que foram presas a partir do uso do reconhecimento facial no setor de segurança pública no país eram negras. (NUNES, 2019). Além disso, o Anuário Brasileiro de Segurança Pública de 2022 (FBSP, 2022), aponta que 67,5% das pessoas encarceradas são negras, contra 29% brancas.

Nessa linha de raciocínio, ainda de acordo com o Anuário Brasileiro de Segurança Pública (2022), negros permanecem como as principais vítimas das mortes violentas intencionais (homicídios dolosos, latrocínios, lesões corporais seguidas de morte e mortes decorrentes de intervenções policiais), com 75,18%. Em uma sociedade que já prende e mata mais pessoas negras, é fácil perceber que com o uso indiscriminado de tecnologias de massa, a situação tende a piorar.

Enquanto isso, a Inteligência Artificial (IA) está sendo utilizada para prever pessoas e locais em que crimes de "ricos" são cometidos e que prejudicam sobremaneira a população como um todo, como por exemplo, crimes no sistema financeiro. Na verdade, "criminalizamos a pobreza, acreditando o tempo todo que nossas ferramentas não são apenas científicas, mas justas". (O'NEIL, 2020, p. 144).

Nesse sentido, a tecnologia tem contribuído para mais desigualdades sociais com seu uso sem transparência, refletindo sobremaneira estereótipos há muito tempo impregnado na sociedade, favorecendo o retrocesso de toda sociedade (MELO; MACHADO, 2022), pois se determinado agente público passa a ter sob seu escrutínio a validação de uma tecnologia que se entende neutra, não teria por que haver questionamento, consequentemente, o racismo vai aumentando de forma invisibilizada.

Em 2012, com a ajuda do FBI, um estudo verificou que os sistemas de reconhecimento facial tendem a ser menos eficazes em sua precisão com afro-americanos, por exemplo, quando comparados com pessoas brancas. (KLARE; BURGE; KLONTZ; BRUEGGE; JAIN, 2012). Consolidando, outro estudo fez uma simulação e verificou que o *software rekognition* identificou erroneamente 40% dos membros negros do congresso estadunidense sendo que apenas 20% da casa é composta pelos mesmos (SNOW, 2018), lembrando que são esses sistemas aqueles utilizados pelas polícias, com foco no policiamento, em parceria com as grandes empresas.

Outra situação ocorreu quando um membro do *Algorithm Watch* divulgou no *Twitter* um experimento demonstrando que o *Google Vision* identificou erroneamente uma pessoa negra com um termômetro na mão, como se estivesse com uma arma, ao contrário, uma pessoa branca na mesma posição com o mesmo objeto, este risco não foi percebido. (KAYSER-BRIL, 2020).

Soluções tidas como simples “É o que chamamos de solucionismo, um band-aid numa hemorragia. A gente precisa focar no racismo, entender como ele opera para verificar exatamente quais são os passos anteriores para discutir questões tecnológicas”. (GUIMARÃES, 2021). É pensar que a tecnologia deve ser utilizada em prol da população para que auxilie na sua evolução, em um mesmo compasso, e não fechar os olhos com a convicção, sem criticidade, de que contribuirá para a resolução de todos os problemas. (MELO; CRUZ; ANDRADE; JABORANDY, 2022).

Como foi demonstrado anteriormente, o Modelo *Face Detect* da *Microsoft* apresentou taxa de erro de 0% para homens de pele clara, enquanto teve uma taxa de erro de 20,8% para mulheres de pele escura (LESLIE, 2020, p. 17). O estudo realizado pelas cientistas de computação Joy Buolamwini e Gebru Timnit (BUOLAMWINI; GEBRU, 2018), revelou que a *Microsoft* tem uma taxa de erro em 12,9% em reconhecer sujeitos mais escuros e 0,7% em sujeitos mais claros. Quando analisada, a IBM possui uma taxa de erro ainda mais grave, em que é 7 vezes maior em peles mais escuras.

Além da discriminação estrutural que contribui para o enviesamento do dispositivo, a própria confiança absoluta dos agentes policiais na máquina, é o suficiente para não haver discussão, mantendo os resultados que ela produz, sem uma calibragem adequada para redirecionar a aprendizagem dos sistemas. A falta de compreensão de como a inteligência artificial em si funciona e como poderia ter chegado aquela solução também é um fator determinante para a perpetuação do preconceito, com uma naturalização geral dos erros ocasionados, em um ciclo destrutivo para os grupos alvos. (SMANIO, 2022).

Dessa forma, alguns questionamentos reflexivos são necessários para que se possa passar para o próximo capítulo do presente trabalho, quais sejam: a vigilância em massa, seria uma violadora de direitos? Ela estaria direcionada para grupos específicos ou atingiria qualquer cidadão? Mesmo que atingisse qualquer cidadão, esse é o futuro que se quer? Abdicar de direitos básicos é necessário? A segurança pública estaria garantida com o uso desenfreado dessa tecnologia?

3 DA VIGILÂNCIA DIRECIONADA A GRUPOS SOCIAIS

O reconhecimento facial é uma forma eficaz de garantir a vigilância onipresente das pessoas, pois opera sem intervalo e, frequentemente, sem ou com pouca supervisão humana, fazendo com que pessoas sejam vigiadas, etiquetadas, categorizadas, manipuladas, seus

comportamentos moldados, de modo que poucas manifestações contrárias ao seu uso são apresentadas por acreditar que estarão mais seguras.

Dessa maneira, a efetivação da segurança pública tem sido atrelada aos dispositivos de vigilância pois a violência e a criminalidade são dois fatores que fazem qualquer ser humano abdicar dos mais elementares direitos para conseguir erradicá-los, por isso dispositivos de segurança são frequentemente aceitos sem objeção, sendo encarados como uma solução em virtude dos vários discursos políticos envolvidos. Ocorre que, a segurança não necessariamente será garantida com o uso dessas tecnologias, e ainda se gera diversos outros problemas, como as discriminações, ferindo o estado democrático de direito. (RODOTÁ, 2003).

Necessário lembrar que o controle e a vigilância não são algo recente na sociedade ou tenha surgido com as novas tecnologias, na verdade, elas têm ganhado novos destaques e contornos de modo a alcançar mais pessoas, sem que geralmente elas saibam dessa situação. (FAUTH, BERLIM, 2020). Por isso, a importância de se debater cada vez mais o assunto para que medidas eficazes sejam tomadas, sem que os indivíduos percam sua liberdade a troco de interesses alheios à segurança.

Em 1785, o filósofo e jurista inglês Jeremy Bentham idealizou o panóptico (BENTHAM, 2008), a partir da construção de um sistema prisional em que a vigilância era exercida de forma incessante, por meio de um prédio em formato redondo com uma torre no centro em que era possível visualizar todas as celas que estavam ao seu redor, aumentando o controle das pessoas encarceradas. Para Bentham (2008), “quanto mais constantemente as pessoas a serem inspecionadas estiverem sob a vista das pessoas que devem inspecioná-las, mais perfeitamente o propósito do estabelecimento terá sido alcançado”.

Posteriormente, atrelado à ideia de Bentham, Michel Foucault lançou seu livro “vigiar e punir: o nascimento das prisões” (FOUCAULT, 1999), publicado inicialmente em 1975, passando de uma interligação da vigilância com a disciplina, de modo que o tipo de construção proposta seria possível para esse controle. Para Foucault, o fato de simplesmente uma pessoa saber que está sendo observada, de alguma forma, nasce nela uma submissão automática.

A estrutura física do panóptico alcançaria um patamar mais elevado que não simplesmente adestrar e manipular, mas também exercer um poder sobre esses indivíduos de modo a “induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder”. (FOUCAULT, 1999, p. 224). Acrescentando, o autor expõe que o panóptico, no seu pensamento, possibilita uma tecnologia política, tornando-se um fator eficaz de discriminação e exclusão.

Outro fato importante para o uso exacerbado de controle, aprimorando os meios tecnológicos com tal finalidade, ocorreu a partir dos ataques terroristas do 11 de setembro nos Estados Unidos (EUA), momento em que o mundo, em total desespero, viu uma maior necessidade de vigilância, com a coleta de dados de forma massiva no intuito de criar perfis e diminuir as chances de mais desastres, sob discursos de que seria para o bem comum. (SOLOVE, 2011).

A luta contra o terrorismo passou a prevalecer a segurança em detrimento de qualquer outro direito previsto. (RODOTÁ, 2004). Assim, a disciplina e a segurança estão sendo melhor empregadas com as tecnologias digitais de vigilância que refletem os primeiros ideais exclusórios. (BAUMAN, 2013).

Mas não se deve deixar enganar com as declarações de que a luta contra o terrorismo abrange todos uma vez que a vigilância e as restrições à liberdade sempre existiram para grupos específicos, os históricos alvos da sociedade. Agora, os ataques terroristas apenas deram margem para que esse controle continue sendo exercido, só que de forma mais proativa e incisiva, como o uso de tecnologias, justificando a criação de perfis ameaçadores, afugentando seus movimentos. (BIGO, 2006, p. 63).

O panóptico digital é mais eficiente do que a sociedade disciplinar biopolítica de Foucault pois se apresenta como uma sociedade da transparência psicopolítica, capaz de interferir diretamente no processo psicológico das pessoas, influenciando e moldando pensamentos e comportamentos. Destarte, controlando a massa de fora para dentro, consegue alcançar o inconsciente coletivo em uma sujeição presente e futura, adquirindo formas totalitárias. (HAN, 2018a). E é mais eficiente do que o benthamiano pois naquele há a coleta e armazenamento ilimitado de dados dos indivíduos vigiados. (HAN, 2018b).

No digital, há uma falsa sensação de liberdade, pois as pessoas não se sentem controladas já que essa vigilância ocorre de forma quase invisível com coleta de dados nem sempre percebida ou aceita espontaneamente por seus detentores. Outro problema é que nem sempre o Estado detém o poder sobre esses indivíduos, empresas possuidoras das informações também possuem esse poder, visando o lucro (HAN, 2018a).

Destarte, como aponta Shoshana Zuboff (2020), impera-se o "capitalismo de vigilância"[3] em que as pessoas não são mais meras consumidoras, mas sim ações são

[3] O termo capitalismo de vigilância foi criado por Shoshana Zuboff, a qual complementa em seu livro que: "as reivindicações bem-sucedidas de liberdade e conhecimento da capitalismo de vigilância, sua independência estrutural em relação às pessoas, suas ambições coletivas e a indiferença radical que é necessária, possibilitada e sustentada por todos os três agora nos propelem rumo a uma sociedade na qual o capitalismo de vigilância não

antecipadas e controladas para serem moldadas ao interesse das empresas detentoras dos poderes. A liberdade e o conhecimento são contrapostos para acumulação de poder, definindo quem deve ser incluído e excluído.

Continua ao discorrer que se esse capitalismo de vigilância permanecer em implementação a liberdade de cada um será submetida e assimilada pela experiência do outro, em prol de lucros e poderes destinados a instituições específicas. Assim, pode-se afirmar que "o conhecimento é deles, mas a liberdade perdida pertence a nós". (ZUBOFF, 2020, p. 426).

Nessa perspectiva, Vera Malaguti (2016) expõe que "a indústria do controle do crime vai gerar uma nova economia, com seus medos, suas blindagens, suas câmeras, suas vigilâncias, sua arquitetura". A prisão física não necessariamente é mais necessária ou mais perquirida, pois articulou-se para um alcance ainda maior, mais destrutivo e lucrativo, por meio dos controles de vigilância.

A vigilância policial também é intensificada com o meio digital, como pelo uso do reconhecimento facial, que se tenta, de forma preventiva, evitar riscos para a sociedade, no intuito de diminuir a insegurança, em contrapartida os indivíduos renunciam à sua privacidade e liberdade (SMANIO, 2022), visando a uma suposta paz social.

Quando se pensa na vigilância dos algoritmos, há um diferencial mais destrutivo ao ser comparado à vigilância disciplinar uma vez que aquela, além de preocupar-se com números ou a identidade, também, e principalmente, tem como propósito a subjetividade das pessoas, traçando padrão de comportamento o que, por vezes, é descontextualizado. (NISSENBAUM, 2011). Assim, traça-se os objetivos, visões de mundo, incertezas e tantos outros comportamentos, mas com uma grande barreira, os sistemas pautam esses padrões conforme tem interesse e não como necessariamente deveria ser, com foco no que seria bom para o indivíduo.

A opacidade das vigilâncias em massa no espaço público representa um risco para os sujeitos que não sabem em que momento estão sendo vigiados e por qual motivo, gerando um estado de alerta constante, tirando a sua paz. (KOSKELA, 2000). É sob a premissa do anonimato em que as pessoas se desenvolvem e conseguem viver efetivamente de forma livre, como bem entender, dentro dos parâmetros legais, uma vez que se sentem acolhidos nos espaços

funciona como meio para instituições econômicas ou políticas inclusivas. Em vez disso, o capitalismo de vigilância deve ser considerado uma profunda força social antidemocrática" (ZUBOFF, 2020. p. 576).

públicos, de maneira a expressar sua opinião e suas vontades, como a "participação em manifestações"[4], por exemplo.

Em 2020, nos EUA, diante de diversas manifestações pacíficas contra o assassinato de George Floyd e a violência racial como um todo, levou o *Federal Bureau of Investigation* (FBI) a utilizar o reconhecimento facial para identificar as pessoas que estariam envolvidas nas reivindicações, trazendo danos irreparáveis à liberdade naquele momento e em ocasiões posteriores em que se torna perceptível o medo que pode causar do que acontecerá com a coleta dos seus dados sensíveis. (TARRASOV, 2020).

O novo tipo de controle vai além, as vozes são caladas e as visões antidemocráticas instauradas. A promessa da era do capitalismo informacional encantou a todos como uma forma possível de libertação e de justiça. (ZUBOFF, 2020).

Não é tão novo o monitoramento por parte do Estado, o presente trabalho não quer debater ou incutir a ideia de que toda essa vigilância é recente, pois há muito o rastreio das comunicações telefônicas e de computadores, por exemplo, já existe. Entretanto, com a internet e a ideia de obtenção de dados na era digital, o alcance e as ofensas alcançaram um patamar ainda mais maléfico com urgência em se discutir, especialmente, pela ausência de regulamentação e de proporcionalidade entre os direitos individuais pretendidos e feridos.

Os dados biométricos possuem uma infinidade de informações que sequer são conhecidas pelos seres e não se sabe onde são armazenadas ou por quanto tempo, dados esses, em sua maioria, sensíveis, que servem para definir aquele ser humano. Ainda pior, pensar que podem ser utilizadas não somente no momento da captação, mas por indeterminados períodos, para as mais diversas finalidades, inclusive no âmbito penal. (GILLIOM; MONAHAN, 2013).

A associação de diversos bancos de dados estatais e particulares com o uso do dispositivo de identificação acabam armazenando muitas informações sensíveis das pessoas a ponto de permitir uma vigilância desproporcional e serem maléficas o suficiente para a conferência de álibis pelas autoridades ou outro meio suficiente de controle não somente de prevenção criminal, mas de controle social. (SMANIO, 2022).

As pessoas não se sentem ofendidas quando ostensivamente em locais públicos percebem que existem câmeras de segurança filmando cada local, mas com certeza se preocupariam com seus direitos caso soubessem nitidamente que o foco da vigilância seria especificamente aquela pessoa. Com o reconhecimento facial é a mesma coisa. Criam uma

[4] "Via de regra, a liberdade pública volta-se enquanto obrigação negativa contra o Estado de impedir a liberdade de manifestação do pensar do indivíduo, por qualquer forma de comunicação desejada. Enquanto direito positivo, obriga o mesmo Estado a garantir os meios para que essa ideia possa se propagar" (SMANIO, 2022).

ilusão de que ninguém diretamente está sendo monitorado, até o dispositivo erroneamente o identificar e uma determinada pessoa se tornar o alvo ou como continuamente acontece pessoas de grupos determinados serem os alvos. (OLIVEIRA, 2021).

A vigilância proveniente do reconhecimento facial não é somente prevenção, mas também um meio para o exercício de poder investigatório, podendo gerar provas, não servindo apenas para identificação e buscas específicas. Os comportamentos potenciais são registrados e armazenados servindo para o presente e para o futuro. Assim, sua forma é ainda mais maléfica quando comparado as investigações tradicionais em que o investigado tem suas limitações apenas durante aquele lapso temporal e não de forma permanente, em um verdadeiro estado de exceção. (RODOTÁ, 2008).

Outro ponto importante são os desvios de finalidades dos dados obtidos, quando inicialmente era apenas para vigilância, como ocorreu em diversos locais que utilizaram o reconhecimento facial para fins menos agressivos. Em Londres, a tecnologia denominada *ShotSpotter*, que seriam microfones instalados ao longo da cidade no intuito de identificar sons de disparos de arma de fogo foram utilizados posteriormente para a captação de conversas ambientes e condenações criminais. (KELLEHER; TIERNEY, 2018).

Nesse sentido, diversos pesquisadores, como o professor Woodrow Hartzog (2018) defende uma regulamentação de banimento do reconhecimento facial antes que se torne comum na vida das pessoas a ponto de não poder mais voltar ao *status quo ante*. Tal defesa é explicada porque, segundo ele, é um dos mecanismos de vigilância mais perigoso do mundo por atingir sobremaneira a privacidade e com um custo-benefício totalmente desequilibrado.

Assim, imperioso questionar: "[...] A limitação de direitos e garantias será infinita? [...] Todos podem se tornar, se não inimigos, pelo menos suspeitos, legitimando todos os tipos de controle de multidões? Devemos nos resignar ao fato de que o próprio conceito de liberdade é modificado?" (RODOTÁ, 2003, p. 25), "[...]até que ponto realmente precisamos de novas técnicas e formas de vigilância e até que ponto temos sido meros consumidores dessa indústria, alimentados pela ilusão de segurança?". (OLIVEIRA, 2021).

Pelo que foi apresentado, compreende-se que a restrição à liberdade é um dos principais fatores que contribuem para repensar a proposta de vigilância por meio do reconhecimento facial pois as pessoas deixam de agir voluntariamente por saberem que estão sendo monitorados, moldando suas ações para os padrões preestabelecidos como corretos, em uma nítida robotização humana. A segurança é colocada em xeque em virtude dos próprios resultados e do seu confronto direto com aquele direito constitucional, além de contribuir para

o aumento de mais exclusões de indivíduos, ao se utilizar se uma tecnologia direcionada esses determinados grupos de minorias raciais.

4 CONSIDERAÇÕES FINAIS

O uso de inovações tecnológicas como resposta ao aumento da violência e da criminalidade tem gerado intensos discursos políticos sobre a necessidade da implementação do reconhecimento facial na segurança pública no intuito de cumprir mandados de prisão e prever comportamentos criminosos, sendo utilizado cada vez mais em ambientes públicos na ocorrência de eventos festivos ou até mesmo no dia a dia das pessoas, como em câmeras já instaladas para monitoramento do trânsito em cidades, por exemplo.

Essas implementações têm ocorrido mesmo sem estudo técnico de viabilidade, sem transparência nos dados, sem treinamento correto dos policiais e equipe que irá manusear os dispositivos. Tem ignorado todos os alertas de pesquisadores sobre os riscos que tecnologias podem trazer ao ser humano, especialmente, quando ligado ao videomonitoramento de forma massiva, na tentativa de identificação de qualquer pessoa e sem uma investigação prévia.

No presente artigo, discutiu-se a proposta de uso do reconhecimento facial na segurança pública, explanando de forma clara como funciona e como são criadas essa tecnologia, além de como as abordagens policiais racistas podem contribuir para que o preconceito aumente a partir de um ponto de vista do banco de dados, para só então trazer ocorrências comprovadas de enviesamento nesses sistemas e como isso tem contribuído para a seletividade penal.

O reconhecimento facial, ferramenta com inteligência artificial, utiliza-se da captura e armazenamento massivo de informações de rostos para que o sistema elabore um padrão facial por meio de técnicas, como a distância entre olhos, por exemplo. Após, compara-se aquele resultado a um banco de dados previamente estabelecido. Ocorre que, são diversas as falhas e erros que podem ser cometidas uma vez que as faces podem mudar ao longo do tempo por meio de cirurgias ou de forma natural, muitas pessoas são parecidas entre si, além do fato desses dispositivos serem desenvolvidos em outros países, com diversidade étnica totalmente incongruente com o Brasil. Ainda, elas tendem a aumentar quando são analisadas imagens com baixa resolução, variação de luminosidade e expressões faciais.

A polícia historicamente prende e suspeita mais das pessoas negras, assim, levantamentos pretéritos servem para novos registros, criando uma retroalimentação. Os estereótipos refletem as ações da própria polícia que respinga para os bancos de dados. Nesse contexto, o racismo vai sendo consolidado ainda mais no âmbito da segurança pública e da área

penal com policiais abordando mais pessoas negras por estas terem sido identificadas por uma tecnologia que representa uma suposta neutralidade.

Buscou-se, num segundo momento, apresentar como a sociedade vai lidar com o reconhecimento facial no que diz respeito à vigilância onipresente que é causada. A vigilância não é algo recente ou implementado pela tecnologia, pois desde as teorias apresentadas por Bentham e Foucault, muito se falava em monitoramento constante para que as pessoas assumam postura passiva e o objetivo proposto seja alcançado, mas pode aumentar sobremaneira seu alcance destrutivo com esses *softwares*.

Percebe-se que os discursos nos quais a efetividade da segurança pública será garantida única e exclusivamente se adotado o reconhecimento facial, vem ganhando força, concebendo uma ideia que remonta as origens do monitoramento em massa, que são discriminatórios e exclusórios, não somente de controle. Por isso, a importância de se analisar crítica e cientificamente os referidos discursos, no intuito de, por meio da pesquisa, identificar acertos e falhas.

Diante do que foi exposto, percebe-se que o uso do reconhecimento facial pelas forças policiais apenas cria uma ilusão de que a criminalidade e violência serão acentuadas, fazendo com que os indivíduos abdiquem dos mais elementares direitos a propósito de uma falsa sensação de liberdade. O que se tem como resultado é: pessoas tendo seus comportamentos moldados, perdendo seus direitos, renunciando à sua dignidade em prol de governos e empresas, ao passo que a criminalidade e a violência permanecem intactos.

Vale lembrar que, se não há transparência, não há previsibilidade, sendo esta necessária para compreensão das responsabilidades e dos resultados, além de sensação de garantia maior para a segurança e confiança no sistema, principalmente, em ambientes públicos, visando a efetivar o Estado Democrático de Direito. A vigilância em massa continuará servindo apenas para que as minorias continuem sendo excluídas, enquanto o discurso valida a sua não discriminação em meio às afirmações de neutralidade da tecnologia.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, Ana Luiza. Em fase de testes, reconhecimento facial no Rio falha no 2° dia. **Folha de São Paulo**, 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/07/em-fase-de-testes-reconhecimento-facial-no-rio-falha-no-2o-dia.shtml. Acesso em: 30 ago. 2022.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BENTHAM, Jeremy. O panóptico ou a casa de inspeção. In: SILVA, Tomaz Tadeu da (org.). **O panóptico**. 2. ed. Belo Horizonte: Autêntica, 2008.

BIGO, DIdier. Security, exception, ban and surveillance. In: LYON, David (org.). Theorizing Surveillance. **The panopticon and beyond.** Portland: Willan Publishing, 2006. p. 63.

BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). **Inteligência artificial e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters, 2. ed., 2020.

BUENO, Samira; PACHECO, Dennis; NASCIMENTO, Talita; MARQUES, David. Letalidade policial cai, mas mortalidade de negros se acentua em 2021. p. 81. In: **Anuário Brasileiro de Segurança Pública**, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/06/anuario-2022.pdf?v=5. Acesso em: 02 set. 2022.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades:** Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR, n. 81, p. 77-91. 2018. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 20 ago. 2022.

DEARDEN, Lizzie. Facial recognition wrongly identifies public as potential criminals 96% of time, figures reveal. **Independent**, 2019. Disponível em: https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html. Acesso em: 31 ago. 2022.

DIAS, Camila Cassiano. Olhos que condenam: uma análise etnográfica do reconhecimento fotográfico no processo penal. **Revista da AJURIS**, Porto Alegre, v. 47, n. 148, p. 329-356, jun. 2020. p. 351.

FAUTH, Pedro; BERLIM, Camila. Vigilância e segurança pública: preconceito e segregação ampliados pela suposta neutralidade digital. **Emancipação**, Ponta Grossa, v. 20, p. 1-22. 2020. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7998401. Acesso em: 05 abr. 2023.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2022**. São Paulo: Fórum Brasileiro de Segurança Pública, 2022. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/06/anuario-2022.pdf?v=15. Acesso em: 27 de fev. 2023.

FOUCAULT, Michel. **Vigiar e punir:** nascimento da prisão. 20. ed. Petrópolis: Vozes, 1999.

GILLIOM, John; MONAHAN, Torin. **Supervision**: An introduction to the surveillance society. Chicago: The University of Chicago Press, 2013.

GUIMARÃES, Hellen. Nos erros de reconhecimento facial, um “caso isolado” atrás do outro. **Folha de São Paulo**, 2021. Disponível em: https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/. Acesso em: 15 set. 2022.

HAN, Byung-Chul. **No enxame:** perspectivas do digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018a.

HAN, Byung-Chul. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018b.

HARTZOG, Woodrow. Facial Recognition Is the Perfect Tool for Oppression. **Medium**, 2018. Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66. Acesso em: 15 set. 2022.

HASSEMER, Winfried. **Introdução aos fundamentos do direito penal.** Tradução de Pablo Rodrigo Aflen da Silva. Porto Alegre: Sergio Antonio Fabris, 2005.

HILL, Kashmir. Wrongfully Accused by an Algorithm. **NY Times**, 2020. Disponível em: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.htrnl. Acesso em: 30 out. 2021.

KAYSER-BRIL, Nicolas. Google Apologizes After Its Vision AI Produced Racist Results. **Algorithm Watch**, 2020. Disponível em: https://algorithmwatch.org/en/story/google-vision-racism/. Acesso em: 30 out. 2021.

KELLEHER, John D.; TIERNEY, Brendan. Data Science. Cambridge: The MIT Press, 2018.

KLARE, Brendan F.; BURGE, Mark J.; KLONTZ, Joshua C.; BRUEGGE, Richard W. Vorder; JAIN, Anil K. **IEE transactions on information forensics and security**, vol. 7, n. 6, 2012. Disponível em: https://s3.documentcloud.org/documents/2850196/Face-Recognition-Performance-Role-of-Demographic.pdf. Acesso em: 12 jul. 2022.

KOSKELA, H. The gaze without eyes: video-surveillance and the changing nature of urban space. **Progress in Human Geography**, v. 24, n. 2, p. 243-265. 2000.

LESLIE, David. **Understanding bias in facial recognition technologies**: an explainer. The Alan Turing Institute, 2020. p. 17. Disponível em: https://arxiv.org/ftp/arxiv/papers/2010/2010.07023.pdf. Acesso em: 28 ago. 2022.

MALAGUTI, Vera. **A questão criminal no Brasil contemporâneo**. Comunicação apresentada no 2o Fórum Nacional de Alternativas Penais: "Audiências de Custódia e a Desconstrução da Cultura do Encarceramento em Massa". Salvador, 2016. Disponível em: https://issuu.com/amilcarpacker/docs/caderno_oip_vera_malaguti. Acesso em: 04 abr. 2023.

MELO, Stephanny Resende de; MACHADO, Carlos Augusto Alcântara. Algoritmos raciais e o retrocesso do ODS 10: o princípio da fraternidade como uma solução possível. In: VERONESE, Josiane Rose Petry; FONSECA, Reynaldo Soares da (Coord.). **Sociedade Digital:** desafios para a fraternidade. v. 1. Caruaru: Editora Asces, p. 88-103. 2022.

MELO, Stephanny Resende de; CRUZ, Letícia Feliciana dos Santos; ANDRADE, Diogo Calasans Melo; JABORANDY, Clara Cardoso Machado. Algoritmos raciais e a sua ocorrência no reconhecimento facial na segurança pública como entrave aos direitos humanos. In: BRAGA, Daniel L. S. (Org.). **Pesquisas e Inovações em Ciências Humanas e**

Sociais: produções científicas multidisciplinares no século XXI. v. 2. 1. ed. Florianópolis: Instituto Scientia, p. 181-194. 2022.

NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Journal of the American Academy of Arts & Sciences,** v. 4, n. 140, 2011. Disponível em: https://nissenbaum.tech.cornell.edu/papers/Contextual%20Approach%20to%20Privacy%20Online.pdf. Acesso em: 20 jul. 2022.

NOVAK, Matt. Hong Kong proíbe máscaras e pinturas faciais que ajudam manifestantes a evitarem reconhecimento facial. **Uol**, 2019. Disponível em: https://gizmodo.uol.com.br/hong-kong-proibe-mascaras-pinturas-faciais-reconhecimento-facial/. Acesso em: 15 jul. 2022.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. In: RAMOS, Silvia at al. **Retratos da violência: cinco meses de monitoramento, análises e descobertas.** Rede de Observatórios da Segurança. Rio de Janeiro: CESeC, 2019. p.67-68 Disponível em: https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf. Acesso em: 30 jan. 2022.

NUNES, Pablo (coord.). Projetos de lei em todo Brasil pedem o banimento do reconhecimento facial em espaços públicos. **O panóptico**, 2022. Disponível em: https://opanoptico.com.br/projetos-de-lei-em-todo-brasil-pedem-o-banimento-do-reconhecimento-facial-em-espacos-publicos/. Acesso em: 12 set. 2022.

OLIVEIRA, Samuel R. de. **Sorria, você está sendo filmado!**: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

O'NEIL, Cathy. **Algoritmos de destruição em massa:** como o big data aumenta a desigualdade e ameaça a democracia. Trad. Rafael Abraham. 1. ed. Santo André: Rua do Sabão, 2020. p. 173.

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. Disponível em: http://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/. Acesso em: 20 mar. 2023.

RODOTÁ, Stefano. Democracia y protección de datos. **Cuadernos de Derecho Público,** Madrid**,** Maio/dez., 2003. Disponível em: https://revistasonline.inap.es/index.php/CDP/article/view/690/745. Acesso em: 30 mar. 2023.

RODOTÁ, Stefano. Transformações do corpo. **Revista Trimestral de Direito Civil**, v. 19, n. 5, 2004.

RODRIGUES, Gustavo. Reconhecimento Facial na Segurança Pública: Controvérsias, riscos e regulamentação. **Blog do Instituto de Referência em Internet e Sociedade**, 2019. Disponível em: https://irisbh.com.br/reconhecimento-facial-na-seguranca-publica-controversias-riscos-e-regulamentacao/. Acesso em 15 jun. 2022.

SILVA, Tarcízio. Colonialismo de dados é fruto e arma da supremacia branca. **Blog do Tarcízio Silva**, 2021. Disponível em: https://tarciziosilva.com.br/blog/colonialismo-de-dados-e-fruto-e-arma-da-supremacia-branca/. Acesso em: 28 ago. 2022.

SILVA, Tarcízio. Linha do Tempo do Racismo Algorítmico. **Blog do Tarcízio Silva**, 2019. Disponível em: https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo. Acesso em: 28 ago. 2022.

SINHORETTO, Jacqueline et al. A filtragem racial na seleção policial de suspeitos: segurança pública e relações raciais. In: **Segurança Pública e direitos humanos:** temas transversais. Cristiane do Socorro Loureiro Lima et al. (Org.). Brasília: Ministério da Justiça, 2014. Disponível em: https://www.patriciamagno.com.br/wp-content/uploads/2018/03/Filtragem-Racial-na-Sele%C3%A7%C3%A3o-de-Suspeitos.pdf. Acesso em: 03 set. 2022.

SMANIO, Gianluca Martins. **Vigilância policial em meio digital:** entre o garantismo e a eficiência. Curitiba: Juruá, 2022.

SNOW, Jacob. Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots. **ACLU**, 2018. Disponível em: https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28. Acesso em: 15 set. 2022.

SOLOVE, Daniel J. **Nothing to ride:** the false tradeoff between privacy and security. New Haven: Yale University Press, 2011.

TARRASOV, Katie. As protests over the killing of George Floyd continue, here's how police use powerful surveillance tech to track them. **CNBC**, 2020. Disponível em: https://www.cnbc.com/2020/06/18/heres-how-police-use-powerful-surveillance-tech-to-track-protestors.html. Acesso em: 04 abr. 2023.

VENTURINI, Jamila; GARAY, Vladimir. **Reconhecimento facial na América Latina**: tendências na implementação de uma tecnologia perversa. Alsur, 2021. Disponível em: https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_PR_Final.pdf. Acesso em: 29 ago. 2022.

VICENTE, João Paulo. Reconhecimento facial erra muito, e você deveria se preocupar com isso. **UOL Notícias**, 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/05/27/tecnicas-de-vigilancia-como-identificacao-facial-ainda-sao-falhas.htm?cmpid=copiaecola. Acesso em: 03 set. 2022.

WECHSLER, H. **Reliable face recognition methods**: system design, implementation and evaluation. Berlim: Springer, 2007.

ZIZI, Martin. The flaws and dangers of facial recognition. **Security Today**, 2019. Disponível em: https://securitytoday.com/articles/2019/03/01/the-flaws-and-dangers-of-facial-recognition.aspx. Acesso em: 15 jun. 2022.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrínseca, 2020. p. 426.