PUCRS

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
DIREITO

GIULIANA GLASS DA SILVA

RECONHECIMENTO FACIAL AUTOMATIZADO E SUA APLICAÇÃO NA BAHIA: UM ESTUDO CRIMINOLÓGICO

Porto Alegre
2023

GRADUAÇÃO

Pontifícia Universidade Católica
do Rio Grande do Sul

RECONHECIMENTO FACIAL AUTOMATIZADO E SUA APLICAÇÃO NA BAHIA: UM ESTUDO CRIMINOLÓGICO

Giuliana Glass Glass da Silva[1]

Ricardo Jacobsen Gloeckner[2]

RESUMO

As técnicas de vigilância têm se aprimorado incluindo novas ferramentas e as câmeras de reconhecimento facial têm sido a grande promessa das instituições punitivas e repressivas do Estado. O presente artigo pretende analisar as ferramentas automatizadas de reconhecimento facial e sua aplicação na sociedade baiana, experiência destacada como de grande sucesso pelos gestores políticos. Para isso, iniciamos o artigo conceituando a sociedade de controle. Assim, estaremos aptos a entender como essa ferramenta se encaixa a ela. Depois, trataremos da tecnologia de reconhecimento facial, como ela funciona e é sistematizada através dos algoritmos, das bases dados, listas de observação e bancos de dados. Em seguida, destacamos as peculiaridades verificadas na sua implementação no Estado da Bahia e, por fim, realiza-se uma análise crítica da situação a luz dos achados da criminologia. Através da pesquisa realizada, foi possível verificarmos que o reconhecimento facial automatizado tem se ofertado como uma solução imbuída de neutralidade. Contudo, ao contrário do que se pensa, é uma ferramenta altamente enviesada, uma vez que construída por humanos. Na prática, foi possível constatar que o reconhecimento facial automatizado é, na verdade, uma continuação das práticas racistas e misóginas praticadas há séculos pelas instituições estatais punitivas e repressivas.
PALAVRAS-CHAVE: Reconhecimento Facial Automatizado – Criminologia - Bahia

ABSTRACT

Surveillance techniques have improved, including new tools, and facial recognition technology have been the great promise of the State's punitive and repressive institutions. This article intends to analyze automated facial recognition tools and their application in Bahia, an experience highlighted as being highly successful by political managers. To achieve this, we begin the article by conceptualizing the control society. Thus, we will be able to understand how this tool fits into it. Then, we will discuss facial recognition technology, how it works and is systematized through algorithms, databases, watchlists and data banks. Then, we highlight the peculiarities observed in its implementation in the State of Bahia. Finally, we will make a critical analysis of the situation based on criminology findings. Through the research realized, it was possible to verify that automated facial recognition has been offered as a solution imbued with neutrality. However, contrary to popular belief, it is a highly biased tool because it is built by humans. In practice, it was possible to verify that automated facial recognition is, in fact, a continuation of racist and misogynistic practices carried out for centuries by punitive and repressive state institutions.
KEYWORDS: Automated Facial Recognition – Criminology – Bahia

[1]Graduanda do curso de Direito da Pontifícia Universidade Católica do Rio Grande do Sul. E-mail: giuliana.silva @edu.pucrs.br.

[2]Professor de Direito da Pontifícia Universidade Católica do Rio Grande do Sul e Doutor em Direito pela Universidade Federal do Paraná. E-mail: ricardo.gloeckner@pucrs.br.

INTRODUÇÃO

O policiamento preditivo pode ser definido como o desenvolvimento de estratégias de segurança pública, realizadas através da vigilância, que visam dar previsibilidade à ocorrência de crimes (ARRUDA, 2022, p. 666-671). No âmbito do policiamento preditivo, a utilização do reconhecimento facial automatizado tem dado seus primeiros passos no país em razão de sua suposta neutralidade e eficiência. Por ser uma máquina, ferramenta matemática e científica, ele não estaria sujeito aos vieses racistas das práticas policiais. Contudo, os estudos sobre o tema nos têm demonstrado que ao contrário do que pensamos, essa nova tecnologia de reconhecimento de pessoas é altamente enviesada. No tópico 1, trataremos sobre a Sociedade do Controle, explicando como ela opera através da intensificação da vigilância por meio de ferramentas tecnológicas. No tópico 2, trataremos acerca do funcionamento da tecnologia de reconhecimento facial automatizado, explicando sua complexidade. No tópico 3, analisaremos a experiência baiana na sua aplicação e por fim, no tópico 4, passaremos a análise crítica do reconhecimento facial automatizado.

1. SOCIEDADE DO CONTROLE

Em seu texto “Post-scriptum sur les sociétés de contrôle”, Gilles Deleuze (1992, pp. 215-216) aponta que a sociedade do controle vem tomando o lugar da sociedade disciplinar. As sociedades de controle atuam por meio de máquinas informáticas e computadores, não sendo somente uma evolução tecnológica, mas também uma mutação do capitalismo. De acordo com o autor, as sociedades disciplinares enfrentam uma crise (DELEUZE, 1992, pp. 220-223). Hardt e Negri (2004, P. 42), ao contrário de Deleuze, acreditam que ao invés de substituir a sociedade disciplinar, a sociedade do controle apenas intensificou e generalizou os aparatos normalizadores disciplinares.

Atualmente, é possível verificarmos que três dispositivos de poder na sociedade — definidos por Foucault — atuam conjuntamente e se sobrepõem. São eles: o disciplinar, o da segurança e o que controla mentes. O primeiro dispositivo otimiza o corpo através de sistemas de recompensas objetivando condutas desejadas, de vigilância e corretivas. Dessa forma, se previne e corrige comportamentos não desejados. Ainda, podemos vê-los em instituições como escolas, empresas, prisões, manicômios e hospitais. O segundo dispositivo atua “na preservação e no cuidado da vida de uma população biologicamente determinada” exigindo a restrição de

suas liberdades, a obediência às suas regras e o pagamento de seus impostos como moeda de troca (BARACUHY; PEREIRA, 2013, 320). Diferente da disciplina, que é exercida em indivíduos pré-determinados, a segurança é exercida em toda uma população de indivíduos para o gerenciamento de suas vidas, saúde, psicologia e comportamentos (FOCAULT, 2013, n.p.). O terceiro dispositivo atua no controle de mentes, nas aspirações e desejos da população. Nas sociedades onde há o declínio do trabalho material e o aumento do trabalho imaterial, a indústria é substituída pelas empresas transnacionais, que podem ser virtuais — caso da Google. O controle de aspirações e desejos tem o objetivo de "dominar e controlar a arte do possível, delimitar as situações nas quais pensamos atuar livremente e assim por diante" (BARACUHY; PEREIRA, 2013, p. 320).

Os dispositivos disciplinares contemporâneos utilizam a vigilância de forma racional e normativa. Eles também usam o marketing, o cinema etc., para introjetar saberes que visam a eficiência do corpo — mais saúde, bem-estar, longevidade etc. — o que torna a vigilância algo desejado e não desprezado. O poder controlador se mantém e se instala naturalmente com base em sua grande astúcia. Como equivocadamente se vende como algo positivo e prazeroso, passa a ser desejado (BARACUHY; PEREIRA, 2013, p. 322). O poder produz o real, domínios de objetos e rituais de verdade. O indivíduo e seu conhecimento decorrem dessa produção:

> O indivíduo é, sem dúvida, o átomo fictício de uma representação «ideológica» da sociedade; mas é também uma realidade fabricada pela tecnologia específica de poder a que se chama «disciplina». Temos de deixar de descrever sempre os efeitos de poder em termos negativos: o poder «exclui», «reprime», «recalca», «censura», «abstrai», «mascara», «esconde». De facto, o poder produz; produz o real; produz domínios de objetos e rituais da verdade. O indivíduo e o conhecimento que dele se pode ter decorrem desta produção (FOUCAULT, 2013, n. p.).

O uso de tecnologias de vigilância, de forma privada e estatal, que nos monitoram — e.g.: monitoramento de aeroportos ou dispositivos que determinam nossas preferências em sites como a Amazon — são carregados de duplo sentido, negativo ou positivo, e de uma dimensão moral (2014, n.p.). Nesse sentido, Lyon aponta:

> Todo desenvolvimento tecnológico certamente é o produto de relações culturais, sociais e políticas. Tudo que chamamos de "tecnologia" é mais propriamente uma característica de relações "tecnossociais" ou "sociotécnicas". Nesse sentido, todos os dispositivos e sistemas exibem tendências morais; não um comportamento moral em si (em minha visão), mas uma direção moral (2014, n.p.).

A direção que se escolhe tomar e o sistema de pesos e balanças depende da sociedade, tendo em vista que pontos negativos e positivos sempre existirão (BAUMAN, 2014, n.p.). Quando Didier Bigo e Anastassia Tsoukala (2008, p. 5) discorrem sobre securitização, afirmam que os atores da (in)segurança não sabem o resultado dos movimentos que tomam, porque os

resultados dependem do campo de efeitos dos vários atores envolvidos na definição de quem é importante para a segurança e dos diferentes públicos passíveis de aceitar ou não essa definição. Contudo, não se pode negar que a vigilância excessiva, que provém de todos os setores, têm causado estragos. Ela não é regulada e dificilmente é percebida por quem é vigiado. Os riscos da vigilância são desconhecidos pelos seus alvos e o que mais preocupa, essas tecnologias têm sido aplicadas ao policiamento preditivo.

Podemos verificar que as ferramentas de predição e a normalização da exceção na sociedade do controle vêm se intensificado com base na política da intranquilidade — "*politics of unease"*. Essa intensificação pode ser constatada desde o ataque às torres gêmeas, em 11 de setembro de 2001, nos Estados Unidos da América (LYON, 2014, n.p.). Esse período de intensificação da securitização também pode ser chamado de Era pós-setembro 11 — "*post-September 11 era*" ou *"post 9/11"* (TSOUKALA, 2008, p. 50). Nos Estados Unidos, a tecnologia de reconhecimento facial foi implementada como ferramenta contra-terrorismo após a queda das Torres Gêmeas. Desde 2001, as câmeras fazem parte das paisagens naturais dos espaços públicos norte-americanos (KROENER; NEYLAND, 2012, p. 142).

De acordo com Bauman (2006, p. 8), o medo é mais assustador quando é indistinto, nos assombra, não possui explicação visível ou quando a ameaça está em todo o lugar e não podemos identificá-la. Para ele, medo é o nome que damos a nossa incerteza e a nossa ignorância da ameaça. A política da intranquilidade, presente na sociedade do controle, se assenta no medo. Depende dele. Contudo, para que o medo seja generalizado, é necessário um projeto político. Esse projeto é a política da intranquilidade.

2. ALGORITMOS, BASE DE DADOS E RECONHECIMENTO FACIAL NO POLICIAMENTO PREDITIVO

Antes de tratarmos do Reconhecimento Facial, importa destacar que esse método de reconhecimento é uma técnica utilizada no policiamento preditivo. O policiamento preditivo consiste na predição de crimes e pode ser aplicado tendo como objeto de análise a pessoa e o lugar. Por meio da análise de dados, se busca prever quais pessoas irão cometer crimes ou quais lugares terão maior criminalidade. O *profiling* é um método de policiamento preditivo que visa prever quem será o infrator, traçando o seu perfil comportamental (ARRUDA; RESENDE; FERNANDES, 2022, p. 671). Quando baseado em algoritmos, cataloga indivíduos de forma que o sistema de inteligência artificial passa a supor que determinados grupos de pessoas têm maiores chances de praticar crimes, informando às autoridades policiais quem merece maior

atenção. Se realizado por um observador humano, há a possibilidade de que se verifique critérios que preencham os elementos suficientes para auferir a culpabilidade do sujeito. Contudo, é importante fazermos um adendo: quando realizado por uma máquina, esses critérios de suficiência não são atendidos (GLESS, 2020, p. 5).

Ao contrário do que se pensa, as tecnologias de reconhecimento facial não oferecem alta precisão porque não são tecnologias fáceis de informatizar. Além do reconhecimento de faces, é necessário que seja trabalhado também o reconhecimento de expressões, que pode modificar drasticamente a identificação de um rosto (GATES, 2011, pp. 5-8). Ver é uma prática cultural e um processo fisiológico. Portanto, se as máquinas podem ver, elas necessariamente incorporam formas específicas de enxergar ao invés de possuírem uma visão universal, objetiva e incorpórea. Por serem informatizados, os sistemas de reconhecimento facial são vistos como mais precisos e objetivos. Logo, menos sujeitos aos preconceitos humanos. Contudo, as máquinas de reconhecimento facial são limitadas pelas intenções de seus idealizadores, seu design, sua implementação e seu uso (GATES, 2011, p. 10).

Os algoritmos de reconhecimento facial não têm se mostrado bons reconhecendo alguns tipos de rostos. Apesar disso, sua comercialização não foi impedida. A tecnologia de Reconhecimento Facial pode ser operada por dois algoritmos: o *Automated facial recognition technology* — AFR — ou pelo *Automated facial expression analysis* — AFE (GATES, 2011, p. 8). Os algoritmos AFR são desenvolvidos para localizar uma face em uma imagem, medir as características geométricas do rosto — distância entre os olhos, nariz, boca, entre outros — e combinar com uma foto previamente armazenada em um banco de dados ou em listas de observação a partir da forte correlação entre características geométricas (PURSHOUSE; CAMPBELL, 2021, p.1). O AFR trata o rosto como um índice de identidade, ignorando sua capacidade de se expressar e de se comunicar em interações sociais. O objetivo dele é usar a iconicidade das imagens faciais como uma forma de estabelecer sua indexicalidade, ou seja, sua efetiva conexão com pessoas humanas e reais. Por sua vez, o AFE busca controlar aquilo que o AFR não consegue: os diversos significados que uma face individual pode expressar. O AFE trata as dimensões afetivas como objetos de medição e cálculo. Contudo, o modo como os humanos interpretam faces não pode ser reduzido a uma série de processos técnicos (GATES, 2011, p. 8). A possibilidade da visão dos sistemas computacionais depende da fusão técnica de sistemas projetada para simular essas formas inter-relacionadas de percepção visual. Não existem sistemas de reconhecimentos que possuam o AFR e o AFE, por isso, a ciência da

computação tem se dedicado a desenvolver sistemas que podem desempenhar as duas funções a que esses algoritmos se propõem: reconhecer rostos e expressões (GATES, 2011, p. 9).

Para Gates (2011, pp. 12-14), assim como as impressões digitais ópticas, o escaneamento da íris e o reconhecimento de vozes, o reconhecimento facial é mais uma das formas tecnológicas em desenvolvimento que "desincorpora identidades" ou a existência de representações visuais e textuais que circulam independentemente dos corpos físicos que as representam. Digitalizando representações visuais do corpo, se poderá expô-lo e vinculá-lo diretamente a redes de informações. O reconhecimento facial teria, portanto, o mesmo propósito de identificação que o DNA — contudo, é preciso salientar que, ao contrário do reconhecimento facial, o DNA não depende de códigos.

As tecnologias biométricas prometem organizar a ambiguidade das identidades quando reivindicam uma ligação direta aos corpos. Contudo, para que isso ocorra, há um complexo processo de mediação. Na aplicação dos sistemas de identificação, os objetivos do reconhecimento facial são: mediar processos de conexão de reconhecimento facial com identidades e permitir a distribuição dessas identidades através de redes informáticas. Assim, é possível a institucionalização de um regime de individualização em massa mais funcional do que a identificação documental (GATES, 2011, p. 15), o que supostamente geraria resultados altamente satisfatórios para a segurança pública quando aplicado no policiamento preditivo. Além disso, a tecnologia de reconhecimento facial promete identificar pessoas à distância, tanto em termos de distância entre câmeras e pessoas, como também de alcance — alcance alargado em redes que cobrem áreas distantes. O grande problema é que automatizar o reconhecimento não estabiliza a identidade, não importando a qualidade do algoritmo e da base de dados (GATES, 2011, p. 16).

Um rosto é capaz de mudar por diversos motivos, tais como: os seus próprios movimentos, o envelhecimento, traumatismos, procedimentos cirúrgicos, estéticos, maquiagens ou em razão da iluminação. Naturalmente, os rostos mudam com o tempo e a qualidade das imagens capturadas de uma face pode variar. Isso traz dificuldades na aplicação do AFR. Faces podem ser detectadas em imagens, extraídas do contexto e normalizadas para se adequarem a um formato padrão. O processo de combinação resulta em uma série de possíveis combinações, dependendo de um limite de correspondência. Um alto limite de correspondência potencializa as chances de perder uma correspondência positiva enquanto um baixo limite de correspondência pode gerar um grande número de falsos positivos (GATES, 2011, p. 17).

Existem dois tipos gerais de reconhecimento facial: aqueles que usam imagens estáticas do rosto e aqueles que analisam imagens de rostos em vídeos (GATES APUD, 2011, p. 18). Os reconhecimentos também podem ser diferenciados de acordo com seus objetivos: podem servir para verificar identidades ou para identificar a identidade de pessoas desconhecidas. No primeiro caso, é necessária uma comparação de imagem facial "um por um" — *"one-to-one"*. No segundo caso, o processo é mais exigente e de informação intensiva. Compara-se a imagem do rosto da pessoa desconhecida com um banco de dados de imagens faciais (GATES, 2011, p. 18).

Os esforços no sistema de reconhecimento facial têm ido na seguinte direção: identificar indivíduos para usar a face como impressão digital, como um índice ou vestígio visual registrado. Os cientistas da computação têm se preocupado em digitalizar rostos não necessariamente utilizando suposições como tipologias faciais. O desenvolvimento de algoritmos para traduzir imagens de rostos em modelos faciais digitais não pressupõe classificações sociais e biológicas dos rostos. Eles não estão interessados em diferenças faciais em pessoas racializadas, com determinadas identidades étnicas ou em diferenças faciais em razão do gênero (GATES, 2011, p. 19).

Estudos desenvolvidos pelo National Institute of Technology (NIST), Instituto sediado nos Estados Unidos, constataram maior probabilidade de falsos positivos em indivíduos negros e asiáticos e menor probabilidade de falsos positivos em indivíduos brancos. Na China, o resultado foi o inverso, havendo um número baixo de falsos positivos em indivíduos asiáticos (GROTHER; Ngan; HANAOKA, 2019, p. 2). Outro estudo conduzido por Buolamwini e Gebru (2018, p. 12), concluiu que os algoritmos de reconhecimento facial encontram maiores dificuldades reconhecendo mulheres e, quando se trata de mulheres negras, o reconhecimento é pior. Portanto, podemos inferir que não só a baixa preocupação com o reconhecimento facial algorítmico de mulheres, pessoas racializadas e de diferentes etnias pode estar gerando injustiças, como também que as particularidades daqueles que alimentam os bancos de dados e listas de observação ou daqueles que trabalham no desenvolvimento dos algoritmos de reconhecimento facial, têm uma grande interferência nos processos de identificação dos indivíduos. Ou ainda, as estratégias securitárias estão orientadas para isso, levando em conta as listas de observação de terroristas.

Se a classificação biológica — utilizada por Galton e Lombroso nos primórdios da criminologia — não ocorre, por outro lado, as identificações sociais acontecem no desenvolvimento da base de dados (GATES, 2011, p. 20) e acabam gerando os mesmos efeitos

de discriminação racial e étnica. De acordo com Gates (2011, p. 21), embora os algoritmos de reconhecimento facial não tenham sido desenvolvidos para classificar rostos de acordo com tipologias particulares de identidade, os sistemas de identificação de base de dados dependem - e facilitam - as estratégias securitárias biopolíticas que são orientadas para diferenciar a população de acordo com critérios raciais determinando quem é protegido e quem é uma ameaça.

Além disso, outro grande problema da aplicação do reconhecimento facial tem sido o banco de dados, ou seja, de onde os algoritmos "puxam" as fotos para realizar o reconhecimento. As tecnologias de segurança de reconhecimento facial têm sido desenvolvidas desde as décadas de 80 e 90. Contudo, após o ataque às torres gêmeas — "*post-September 11 era*" ou *"post 9/11"* — o setor da informação tecnológica e os serviços e sistemas de segurança criaram vínculos mais estreitos de forma rápida (GATES, 2011, p. 99) tendo como promessa a precisão. Em tese, a tecnologia de reconhecimento facial poderia se mostrar uma ferramenta objetiva no reconhecimento de rostos de terroristas. Importa destacar que essa lógica ressuscitou as antiquadas noções de tipos de faces desviantes e prometeu proteger os cidadãos do que Gates chama de "faces do terror" e "classe mítica de rostos demoníacos". Tudo isso aparentando neutralidade técnica. Nesse contexto é que surgem as listas de observação, que prometem classificar terroristas, mas que na verdade, os fabricam (GATES, 2011, p. 101). A base de dados define os parâmetros do que os computadores podem ser programados para ver. Ou seja, as câmeras não são a principal ferramenta capaz de reconhecer rostos criminosos, mas sim os arquivos, que necessitam ser alimentados com fotografias. As fotos são retiradas de seu contexto que é substituído por outro. Os arquivos estabelecem uma ordem em seus conteúdos, funcionando de acordo com um modelo empírico de verdade (GATES, 2011, p. 111-112). As bases de dados eletrônicas são diferentes dos arquivos convencionais porque permitem que o usuário acesse, organize e reconheça centenas, milhares ou até mesmo milhões de registros e isso presume múltiplas formas de indexação de dados (GATES apud MANOVICH, 2011, p. 111).

Faces individuais são capturadas por câmeras de segurança, suas imagens são automaticamente extraídas, normalizadas conforme um formato padrão e digitalizadas para produzir modelos faciais matemáticos. Porém, para identificar indivíduos específicos, é necessário acumular imagens faciais nas bases de dados para servir de memória para os sistemas automatizados de identificação. Os rostos identificados precisam ser colocados em uma base de dados de lista de observação. A base de dados das listas de observação consiste em um

equipamento de visão complexo e enorme, construído em um enorme banco de dados. Para isso, é necessário muito esforço alimentando esse banco de dados (GATES, 2011, p. 110).

São exemplos de listas de observação as listas de terroristas (GATES, 2011, p. 110) e a base de dados dos sistemas prisionais (URQUHART; MIRANDA, 2021, p. 11). A base de dados dos sistemas prisionais contém fotos de pessoas com mandados de prisão, presos que fugiram, pessoas vulneráveis e que precisam de proteção, incluindo as desaparecidas (URQUHART; MIRANDA, 2021, p. 11). No Brasil, o aplicativo MOP — Sistema de Mobilidade em Operações Policiais — é um grande banco de dados presente na rotina dos policiais. O MOP é utilizado em seus aparelhos celulares e possui informações sobre os civis como: impressões digitais, registros criminais, dados de veículos, dados demográficos, de gênero e localização (FALCÃO, 2021, n.p). Apesar de não haver evidências de que esse banco de dados tenha sido utilizado nos casos de reconhecimento facial no Brasil, ele se mostra um grande meio de obtenção de dados e, portanto, é importante mencioná-lo.

Além dos bancos de dados das instituições estatais, outra possibilidade é o banco de dados de empresas particulares. As redes sociais, por exemplo, têm se mostrado um grande problema. Isso porque as empresas responsáveis pelas redes sociais mais utilizadas pelos brasileiros têm fornecido informações pessoais sem a autorização de seus usuários, demonstrando não haver nenhuma política de proteção de dados. Recentemente, se descobriu que Hoan Ton-That, empresário australiano, criou uma ferramenta de reconhecimento facial que contém cerca de três bilhões de fotos de indivíduos disponíveis em sites como Facebook, Twitter e Youtube. A ferramenta se chama Clearview AI e promete ser um banco de dados de reconhecimento facial. Essa ferramenta foi criada em 2016 e o objetivo no seu desenvolvimento era a sua venda (TRINDADE, 2020, n.p).

No âmbito brasileiro, o reconhecimento tem sido implementado em alguns Estados a partir de tecnologias importadas. O que tem se mostrado problemático se levarmos em consideração que as tecnologias importadas não estão adaptadas para o contexto racial brasileiro, país conhecido pela pluralidade racial, pelo racismo, pela letalidade policial com pessoas racializadas e pelo alto número de encarceramentos de pessoas negras. Outro grande problema levantado por pesquisadores do reconhecimento facial e do policiamento preditivo é a falta de informação sobre o tratamento de dados, o consentimento dos cidadãos na sua coleta para os fins a que se propõe o reconhecimento facial, a ausência de licitações e a falta de participação do público na tomada de decisões.

Como visto anteriormente, o reconhecimento facial automatizado exige o acesso a informações pessoais de todos os cidadãos brasileiros, sem distinção, e o acesso a esses dados pode vir de redes sociais, de órgãos governamentais, entre outros. Além disso, com a ausência de adequação ao Brasil, os sistemas de reconhecimento facial automatizados podem representar um número alto de falsos positivos. No contexto brasileiro, onde a truculência da polícia com pessoas racializadas é fator traumatizante para jovens negros, o alto número de falsos positivos com parcela dessa população se mostra apenas mais uma manutenção de velhas práticas. Nesse caso, a frase de Bauman em seu livro "Moderinidade Líquida" se aplica muito bem a essas novas práticas de vigilância, é possível vermos "a continuidade por trás das descontinuidades" (BAUMAN, 2014, n.p.).

Nesse sentido, estamos apenas modernizando as formas em que a biopolítica se opera e fornecendo ferramentas maiores, mais potentes e problemáticas às práticas de vigilância sob suposta neutralidade. Segundo Ceyhan (2012, p. 45), hoje em dia testemunhamos uma nova forma de poder, o biopoder pode ser alcançado através da digitalização e montagem de tarefas autônomas e interesse em locais inesperados por organismos de aparências amigáveis como as empresas de software e os depósitos de dados. O biopoder é híbrido e isso abre novos conjuntos de tecnologias e técnicas que já não se processa apenas pelo controle de populações através da sexualidade e saúde, mas pelo rastreamento de indivíduos através de partes dos seus corpos, comportamentos, projetos e pensamentos.

No tópico a seguir, trataremos sobre a implementação do reconhecimento facial na Bahia, analisando as razões para sua implementação, suas etapas e as problemáticas de sua implementação, observando a mencionada continuidade por trás das descontinuidades.

3. IMPLEMENTAÇÃO DO RECONHECIMENTO FACIAL NA BAHIA

Em 2018, o governador da Bahia à época, Rui Costa, anunciou a intenção de implementar o sistema de Reconhecimento Facial no Estado. Em fevereiro do mesmo ano, o governador instala o projeto intitulado "videomonitoramento inteligente". Isso só foi possível diante do cenário favorável, propiciado pela Copa das Confederações e pela Copa do Mundo em 2013 e 2014, respectivamente. Esses eventos propiciaram um terreno fértil para a implementação do projeto, uma vez que houve a criação da Secretaria Extraordinária de Segurança para Grandes Eventos — SESGE — que além de atuar no planejamento, implementação, definição, acompanhamento, coordenação e avaliação das ações de segurança, também foi responsável pela integração e articulação entre os órgãos de segurança pública

federais, estaduais, municipais e distritais, estimulando a modernização das ferramentas de segurança (NUNES, 2023, pp. 7-8).

Em 2013, a SESGE criou o Sistema Integrado de Comando e Controle de Segurança Pública para Grandes Eventos — SICC. Os SICC englobam os Centro Integrados de Comando — CICC — e as Plataformas de Observação Elevada — POE. O CICC e o POE são equipados com ferramentas tecnológicas vendidas à sociedade baiana como de alto desempenho, com ferramentas de inteligência e sistemas de última geração. Os CICC são equipados com telas e computadores de monitoramento de imagens. Neles também se encontram operadores da polícia. O POE é equipado com 14 câmeras que captam imagens em um ângulo de 360°, refletores dispostos nas laterais, *speed domes*, *wi-fi*, entre outros dispositivos. O POE conta com um sistema de vídeo analítico que fornece imagens em tempo real aos CICC (NUNES, 2023, p. 9).

O CICC foi inaugurado em 2015 e conta também com delegacias móveis e com uma caminhonete equipada com *softwares* de reconhecimento de placas. Além dessas implementações, houve também a instalação de 400 câmeras de vigilância na cidade de Salvador e a implementação de Centros de Monitoramento de Câmeras — CMC — nas Companhias Independentes da Polícia Militar. Com essas instalações no âmbito da Segurança Pública baiana, o terreno para receber os *softwares* de reconhecimento facial e ampliar o videomonitoramento já estava preparado (NUNES, 2023, p. 10).

Em 2016, Rui Costa institui o Centro de Operações e Inteligência — COI — com o objetivo de "fortalecer a atuação integrada e transversal das forças de segurança pública e coordenar as ações táticas e operacionais". No mesmo ano, o COI passa a atuar com os Centros Integrados de Comunicação — CICOM — fazendo uso dos sistemas de comunicação e videomonitoramento (NUNES, 2023, pp. 10-11).

Em 2018, houve por parte da Secretaria de Segurança Pública da Bahia — SSPBA — a implementação de um projeto piloto de videomonitoramento com reconhecimento facial na cidade de Salvador. Os pontos escolhidos para a implementação das câmeras de reconhecimento facial foram o aeroporto da cidade, os terminais rodoviários, o metrô e o estádio Arena Fonte Nova. Ao todo, foram instaladas 310 câmeras, incorporadas nos sistemas de monitoramento do Parque Tecnológico de Salvador (NUNES, 2023, p. 11).

O software de reconhecimento facial escolhido foi fornecido pela empresa Huawei e recebe o nome de Videocloud, possuindo capacidade de realizar reconhecimentos faciais, proceder a leitura de placas de veículos e contagem de pessoas. Além disso, através dessa

solução tecnológica, seria possível realizar a integração de 1.990 câmaras da SSPBA garantindo que o gerenciamento pudesse ser realizado (PIRES et al, 2021, p. 22). Na época da aquisição da tecnologia, ela contava com 60 terabytes para processamento e armazenamento de dados e possuía a capacidade de analisar cerca de duas mil imagens simultaneamente. Além disso, o governo da Bahia alegava que essa ferramenta possuía dados de veículos roubados e de 65 mil pessoas com mandados de prisão (BAHIA, 2018, n.p). Contudo, a meta era aumentar o banco de dados que alimentava o *software* para incluir cidadãos comuns nos cadastros do sistema (NUNES, 2023, p. 12).

Não se sabe quais as bases de dados utilizadas na realização do reconhecimento. Contudo, a SSP/BA aponta que há possibilidade de utilização de fotos extraídas de redes sociais como o Facebook que possui fonte aberta (NUNES, 2023, p. 13). O reconhecimento facial foi utilizado em algumas oportunidades pela SSP/BA: na Micareta de Feira de Santana, em abril de 2019, e no Carnaval de Salvador, em março do mesmo ano. No primeiro, foram capturados mais de 1,3 milhões de rostos e foram gerados 903 alertas. Desses 903 alertas, 15 pessoas foram presas e 18 mandados de prisão foram cumpridos, ou seja, 870 pessoas foram abordadas equivocadamente. No segundo, 15.880 rostos foram capturados, 361 alertas foram gerados e apenas uma prisão foi efetuada, ou seja, 360 pessoas foram abordadas sem justificativa (PIRES et al, 2021, p. 29).

Ainda em 2018, o governador da Bahia informou sua intenção de levar a tecnologia de reconhecimento facial para toda a Bahia. No mesmo ano, foi lançado o Termo de Referência que buscava a contratação de três serviços: Monitoramento e Sustentação de Infraestrutura de Operações, Pontos de Imagem e Comunicação Nível Crítico com banda larga. Dois dos Pontos de Imagem solicitados tinham reconhecimento facial: um para ambientes externos e internos com número reduzido de pessoas e outro para ambientes externos e internos com alto número de circulação de pessoas. Rui Costa almejava distribuir esses serviços entre a capital e 58 municípios do interior (NUNES, 2023, p. 18).

Em 2019, houve uma ampliação no número de locais que recebem esses serviços, aumentando para 78 municípios. O contrato firmado em 2021 foi com a Oi Móvel S/A e o consórcio Avantia Tecnologia e Engenharia S/A. O *software* da Huawei ainda é utilizado no Estado (NUNES, 2023, pp. 18-19). A empresa Oi foi a mesma envolvida no projeto de videomonitoramento com reconhecimento facial no Rio de Janeiro, que também trouxe resultados insatisfatórios (NUNES, 2022, p. 9). Importa destacar que em 2014 a Oi foi multada por monitorar a navegação de consumidores na internet. Ela e a empresa britânica Phorm

estavam criando um *software* chamado "Navegador" que buscava mapear o tráfego de dados dos consumidores na internet para compor um perfil de navegação. Os perfis eram comercializados com anunciantes, agências de publicidade e portais da *web* com o objetivo de personalizar conteúdos e fazer ofertas publicitárias — ou seja, a empresa coletava e vendia dados de seus clientes sem suas autorizações (BRASIL, 2014, n.p).

O atual projeto de reconhecimento facial prevê a contratação de um serviço mensal — fornecido pela Oi Móvel S/A e pelo consórcio Avantia Tecnologia e Engenharia S/A — onde a contratada disponibiliza equipamentos, infraestrutura e *softwares*, ficando responsável pela instalação, desinstalação, atualização do sistema, manutenção nos equipamentos, etc. Atualmente, no ano de 2023, o estado da Bahia conta com 76 municípios com reconhecimento facial. Além da ausência de clareza sobre a base de dados dos sistemas de reconhecimento utilizados pelo Estado da Bahia, também não há nenhuma informação sobre os motivos que levaram à extensão do projeto de videomonitoramento para os municípios do interior. Um dos critérios para a escolha dos municípios, de acordo com o governador, seria o número da população e alta taxa de homicídios. No entanto, alguns municípios escolhidos possuem 5 mil habitantes (NUNES, 2023, p. 19).

Rui Costa convocou a iniciativa privada para se juntar ao projeto de videomonitoramento. Os pontos comerciais que possuem câmeras cederiam as imagens à polícia. Dessa forma, a abrangência do monitoramento aumentaria, terceirizando custos. Em março de 2022 foi lançado o projeto Câmera Interativa, câmeras residenciais, de empresas e comércios se somariam ao sistema de monitoramento da SSP/BA (NUNES, 2023, 19-20).

No Termo de Referência do projeto, uma das funções da análise de vídeo é reconhecer o estilo do cabelo e o estilo inferior. Para Nunes (2023, p. 22), o *software* adquirido pelo Estado da Bahia é capaz de reconhecer rostos, identificar elementos do corpo humano, acessórios e roupas. Após críticas de racismo, o governador da Bahia alterou o Termo de Referência para constar apenas a identificação do sexo, a idade, a bolsa e a mochila das pessoas no vídeo.

O *software* Videocloud da empresa Huawei foi um requisito no Termo de Referência do projeto (NUNES, 2023, p. 18). Contudo, até agora não se sabe de fato como ele funciona e quais bancos de dados são utilizados. O que temos são apenas noções escassas coletadas nos veículos de notícia. Informações como o tipo de algoritmo que suas câmeras de reconhecimento possuem — AFR ou AFE — são de extrema importância e no caso objeto de análise, não foram divulgadas pelo governador da Bahia e nem pela SSP/BA. A única informação que se tem até o momento é que a Huawei é uma empresa chinesa que possui sede no Brasil e que o Termo de

Referência solicita que o *software* reconheça a identificação do sexo, a idade, a bolsa e a mochila das pessoas no vídeo. A menção da necessidade de reconhecimento de sexo não nos autoriza a pensarmos que a solução tecnológica fornecida pela Huawei possuirá algoritmos que reconheçam o gênero da pessoa, tendo em vista as defasagens dos algoritmos nesse tipo de reconhecimento.

Deve-se pontuar que ao solicitar o reconhecimento de sexo no Termo de Referência, questiona-se se o reconhecimento da solução fornecida identificaria mulheres transgênero ou ainda, se identificaria mulheres racializadas, bem como homens racializados e pessoas de etnias diversas. Tendo em vista que a empresa Huawei é chinesa, podemos inferir que seu *software* pode não estar adaptado para a realidade racial brasileira, o que geraria diversos problemas de direitos humanos em abordagens equivocadas. Como mencionado anteriormente, houve diversos falsos positivos nos eventos em que se utilizou o reconhecimento facial. Abordagens equivocadas e truculência garantem traumas e manutenções de práticas racistas.

A ausência de informação não nos permite ter controle sobre o modo como estamos sendo vigiados. Outro fato que chama atenção é que ao invés da tecnologia ser adquirida por meio de licitação, o que ocorreu foi um aditivo em contrato (NUNES, 2023, p. 12), demonstrando a urgência de sua implementação, uma vez que há cidades baianas que não possuem saneamento básico e suas comarcas de primeira instância foram desativadas, inviabilizando a busca por direitos. Além disso, as cidades baianas beneficiadas com a tecnologia também possuem apenas 50% de taxa de urbanização (NUNES, 2023, p. 26). Nesse sentido, é possível verificarmos aquilo que Ceyhan (2012, p. 45) pontua: atualmente, o biopoder é híbrido. Controla populações através da saúde e pelo rastreamento de pessoas através de partes dos seus corpos, comportamentos e pensamentos.

4. ANÁLISE CRÍTICA

A política de insegurança é implementada pelas mídias sociais, jornais, etc. e pelos agentes políticos há muito tempo. Esse estado de insegurança tem sido intensificado pelas políticas estatais. A mídia e os agentes políticos manipulam informações — de forma intencional ou não — desviando o foco do problema original. Nesse caso, ignora-se o contexto social brasileiro de fome, desigualdade econômica, no acesso à saúde e moradia e se priorizam políticas de vigilância como ferramentas do poder punitivo. Essas políticas incluem tecnologias que prometem diminuir o número de crimes. Contudo, a questão que chama atenção é que os

indivíduos e locais que entram nas listas de predição da vigilância ostensiva são sempre os mesmos.

A criminologia verde, ramo da criminologia que busca estudar os danos ambientais provocados por indivíduos, Estados e empresas em razão da prática de uma atividade danosa ou da negligência que ocasiona desastres naturais e consequências danosas (BUDÓ apud NATALI, 2019, p. 489), denuncia a seletividade penal. Os causadores desses tipos de danos sociais possuem a garantia da não responsabilização pelo sistema de justiça criminal e não são classificados como criminosos (MELCHIORS; GLOECKNER; BUDÓ, 2021, n.p), porque as condutas praticadas por eles não são criminalizadas, uma vez que o Direito Penal não leva em consideração esse tipo de dano (COLOGNESE, 2018, 958). Isso porque aqueles que o praticam são detentores do poder político e econômico (BUDÓ, 2016, p. 15).

Quando se trata de crimes ambientais, o Estado facilita e estimula atividades ilegais através de atos comissivos e omissivos, diretos ou indiretos (COLOGNESE, 2018, p. 967). Chama a atenção, por exemplo, que enquanto é possível verificarmos por parte dos políticos o avanço e o incentivo de táticas de policiamento preditivo nos crimes de rua, quando se trata dos crimes ambientais, o esforço é no sentido contrário. O avanço da PEC 65/2012 em 2016, um ano após o Caso Mariana, é um exemplo disso, já que de acordo com alguns pesquisadores, na prática, acabaria com o licenciamento ambiental (COLOGNESE, 2018, p. 980; BRASIL, 2018, n.p.).

As técnicas de vigilância têm sido atualizadas e modernizadas no âmbito dos aparelhos repressivos do Estado não só para encontrar e punir pessoas específicas, como também para vigiar lugares específicos. Em nome da predição de crimes e da otimização na busca de criminosos, tem se aceitado não só a violação dos direitos de uma sociedade inteira — no que diz respeito ao tratamento de dados —, como também a violação a direitos de pessoas específicas — pessoas racializadas, de diferentes etnias e mulheres —, tendo em vista que são humilhadas e hostilizadas diante dos falsos positivos.

De acordo com Schwab (2016, p. 19), estamos na Quarta Revolução Industrial, que teve início na virada do século XXI e é caracterizada:

> por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina). As tecnologias digitais, fundamentadas no computador, software e redes, não são novas, mas estão causando rupturas à terceira revolução industrial; estão se tornando mais sofisticadas e integradas e, consequentemente, transformando a sociedade e a economia global

Na mesma medida em que a Quarta Revolução Industrial nos traz benefícios, como tudo na vida, também nos traz desvantagens. Não se pode evitá-la, assim como o controle exercido pela Sociedade do Controle. Contudo, o sistema de pesos e balanças de uma sociedade deve ser capaz de direcionar a Quarta Revolução Industrial na regulação de seus efeitos e amenizar o controle exercido sob nossos corpos. Para que isso ocorra, precisamos tomar medidas a fim de evitar a continuidade de práticas rechaçadas há muito tempo.

O controle exercido sob nossos corpos, nossas vidas e nossa intimidade não pode mais operar de acordo com as velhas diretrizes autoritárias, racistas e misóginas. Como já sinalizado anteriormente, o que se tem é a manutenção de velhas práticas sob a roupagem da neutralidade. Assim como o juiz não é neutro — é o que nos sinaliza a psicologia cognitiva —, as máquinas de reconhecimento facial e seus bancos de dados também não o são. Isso porque dependem de humanos para sua criação. Mesmo que não haja projetos políticos na criação de algoritmos, bases de dados e banco de dados, ambos são criados e produzidos por humanos, sujeitos a toda uma sociedade estruturalmente e institucionalmente racista e misógina e, portanto, possuem seus vieses e conceitos subjetivos, intrínsecos a todos nós. Somos produtos dos aparelhos disciplinares do Estado. Passamos por um processo de fabricação e por isso, a criminologia, a sociologia e a história têm papéis fundamentais em todos os âmbitos da sociedade, já que a matemática não é capaz de lidar com as complexidades humanas. Como Gates (2011, p. 10) sinaliza, ver também é uma prática cultural e se as tecnologias de reconhecimento facial são capazes de ver, elas também incorporam formas específicas de fazer isso.

A ausência de uma política de securitização que tenha um sistema de pesos e balanças, levando em consideração questões de direitos humanos, nos leva a constatar o autoritarismo na implementação desse sistema de vigilância. Parece haver uma certa inquisitoriedade por trás dessas práticas de aplicação: se define o criminoso e o lugar que será vigiado, se aplicam ferramentas tecnológicas vendidas como imbuídas de neutralidade para depois prender as pessoas de forma “justa”. Tudo isso ignorando os vieses racistas e misóginos dos algoritmos. A falta de informações sobre os algoritmos, a base de dados e as funcionalidades do sistema adquirido pela SSP/BA e o grande número de falsos positivos nas experiências baianas de reconhecimento facial, não nos permite acreditar na neutralidade científica dessa ferramenta.

CONCLUSÃO

O reconhecimento facial automatizado tem sido utilizado por alguns estados brasileiros sob a alegação de suposta neutralidade para prever a ocorrência de crimes e localizar

criminosos. Contudo, observamos vieses racistas e misóginos nos algoritmos de reconhecimento facial, bem como nos seus bancos de dados, bases de dados e listas de observação. Isso porque para que as máquinas funcionem, elas precisam da intervenção humana na criação de elementos essenciais no seu funcionamento. Os estados têm adquirido essas ferramentas importadas de países que não possuem o contexto racial brasileiro, como no caso da China. O problema da aquisição dessas ferramentas e da falta de neutralidade e informação sobre os softwares utilizados no Brasil é que não sabemos a qualidade das tecnologias utilizadas e nem se elas foram adaptadas ao país.

Não podemos evitar nossa sujeição a Sociedade do Controle e nem parar os avanços da Quarta Revolução Industrial. Contudo, podemos amenizar seus efeitos sobre a vida das pessoas na medida em que incluímos os brasileiros nesse processo de tomada de decisão e regulamentamos sua utilização e aquisição. Por exemplo, precisamos de boas justificativas para a sua implementação em determinadas cidades e espaços, além de informações fundamentais sobre as tecnologias que estão sendo utilizadas. As ferramentas de reconhecimento facial automatizado podem trazer benefícios à sociedade na medida em que, por exemplo, podem ser utilizadas para reconhecer crianças desaparecidas ou sequestradas.

Como Bauman sinaliza (2013, n. p), as tecnologias são espadas de dois gumes. Podem oferecer benefícios e malefícios. O sistema de pesos e balanças de uma sociedade é que será capaz de direcionar seus rumos. No caso do reconhecimento facial automatizado, no contexto brasileiro, é urgente a mudança de direção, uma vez que essas ferramentas prometem apenas dar continuidades a práticas a muito tempo criticadas pela criminologia.

REFERÊNCIAS

ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. Sistemas de Policiamento Preditivo e Afetação de Direitos Humanos à Luz da Criminologia Crítica. Revista Direito Público, Brasília, v. 18, n. 100, p. 666 - 671, 27 jan. 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5978. Acesso em: 12 nov. 2023.

BAHIA. Lançado sistema de videomonitoramento inteligente de segurança. Casa Civil da Bahia, Salvador. Disponível em: http://www.casacivil.ba.gov.br/2018/12/1271/Lancado-sistema-de-videomonitoramento-inteligente-de-seguranca.html. Acesso em: 12 nov. 2023, 20:34.

BARACUHY, Regina; PEREIRA, Tânia Augusto. A biopolítica dos corpos na sociedade de controle. Gracoatá, Niterói, v. 18, n. 34, p. 317-330, 06 jul. 2013. Disponível em: https://periodicos.uff.br/gragoata/article/view/32974/18961. Acesso em: 12 nov. 2023.

BAUMAN, Zigmund; LYON, David. Vigilância líquida. Rio de Janeiro: Zahar, 2014. *E-book.*

BAUMAN, Zigmund. Medo Líquido. Rio de Janeiro: Zahar, 2008.

BIGO, Didier; TSOUKALA, Anastassia. Understanding (in)security. In: BIGO, D.; TSOUKALA, A. (org.). Terror, Insecurity and Liberty Illiberal practices of liberal regimes after 9/11. Oxon: Routledge, 2008. p. 1-9.

BOULAWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, v. 8, p. 1-15, 2018. Acesso em 12 nov. 2023. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a.html?mod=article_inline&ref=akusion-ci-shi-dai-bizinesumedeia. Acesso em: 12 nov. 2023.

BRASIL. Ministério da Justiça multa Oi por monitorar navegação de consumidores na internet. Ministério da Justiça e Segurança Pública, Brasília - DF. Disponível em: https://www.justica.gov.br/news/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet. Acesso em: 12 nov. 2023, 20:20.

BRASIL. Senado Federal. Proposta de Emenda à Constituição n° 65, de 2012. Brasília, DF: Senado Federal. 21 dez. 2018. Assunto: licença ambiental. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/109736. Acesso em: 20 nov. 2023.

BUDÓ, Marília de Nardin. "A blindagem discursiva das mortes causadas pelo Amianto no Brasil: Criminologia Crítica e Dano Social. Conpedi Law Review, v. 2, n. 1, 2016, p. 1-21. Disponível em: https://indexlaw.org/index.php/conpedireview/article/view/3592/3097. Acesso em: 20 nov. 2023.

BUDÓ, Marília de Nardin. "Um massacre silencioso que continua": um olhar criminológico sobre os Danos Sociais causados pelo Amianto. Novos Estudos Jurídicos, Itajaí, v. 24, n. 2, 08 ago. 2019, p. 484-513. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/14961. Acesso em: 18 set. 2023.

CEYHAN, Ayse. Surveillance as biopower. *In*: BALL, K.; HAGGERTY, K.; LYON, D. (org.). Routledge Handbook of Surveillance Studies. Oxon: Routledge, 2012. p. 38-45.

COLOGNESE, Mariângela Matarazzo Fanfa. O Caso Samarco: Vitimização Ambiental e Dano Social Corporativo no cenário de Mariana: uma investigação empírica a partir da perspectiva das vítimas (Parte I). Revista Eletrônica Direito e Política, v. 13, n. 2., 29 ago. 2018, p. 956-988. Disponível em: https://periodicos.univali.br/index.php/rdp/article/view/13366/7597. Acesso em: 20 nov. 2023.

FALCÃO, Cintia. A ascensão do tecnoautoritarismo: Parte 4. Intercept Brasil, 20 set. 2021, 00:05. Disponível em: https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/. Acesso em: 12 nov. 2023, 21:22.

FOUCAULT, Michel. Vigiar e punir. Lisboa: Almedina, 2013. *E-book.*

GATES, Kelly A. Our Biometric Future: facial recognition technology and the culture of surveillance. Nova York: New York University Press, 2011.

GLESS, Sabine. Policiamento preditivo: em defesa dos "verdadeiros positivos". Revista de Direito GV, São Paulo, v. 16, n. 1, p. 5, 8 set. 2020. Disponível em: https://periodicos.fgv.br/revdireitogv/article/view/81697. Disponível em: 12 nov. 2023.

GROTHER, Resende; NGAN, Mei; HANAOKA, Kayee.Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. National Institute of Standards and Technology Interagency of Internal Report, dec. 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.Acesso em: 12 nov. 2023.

MELCHIORS, Rafaela Bogado; GLOECKNER, Ricardo Jacobsen; BUDÓ, Marília de Nardin. SEMINÁRIO DE CIÊNCIAS CRIMINAIS E LITERATURA: PENSAR AS VOZES SILENCIADAS, 1., Porto Alegre. [Anais]. Porto Alegre, RS: Programa de Pós-Graduação em Ciências Criminais da Pontifícia Universidade Católica do Rio Grande do Sul, 2021. *E-book*.

NUNES, Pablo; LIMA, Thallita G. L.; CRUZ, Thaís G. O sertão vai virar mar: Expansão do reconhecimento facial na Bahia. Rio de Janeiro: CESeC. 2023. *E-book*. Disponível em: https://opanoptico.com.br/wp-content/uploads/2023/08/O_sertao_vai_virar_mar-expansao_do_reconhecimento_facial_na_Bahia.pdf. Acesso em: 12 nov. 2023.

NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel R. Um Rio de olhos seletivos: uso de reconhecimento facial pela polícia fluminense. Rio de Janeiro : CESeC. 2022. *E-book*. Disponível em: https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 12 nov. 2023.

PIRES et al. Alvos predeterminados: um estudo de caso sobre a implementação de tecnologia de reconhecimento na Bahia. *In*: ALMEIDA, E. M; ESTELLITA, H. (org.). Dados, privacidade e persecução penal: cinco estudos. FGV: Escola de Direito de São Paulo, 2021. p. 17-62. *E-book*. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/31784/Dados%2c%20privacidade%20e%20persecu%c3%a7%c3%a3o%20penal.pdf?sequence=1&isAllowed=y. Acesso em: 12 nov. 2023.

PURSHOUSE, Joe; CAMPBELL, Liz. Automated facial recognition and policing: A Bridge too far?. Legal Studies, Cambridge, v. 42, i. 2, p. 1-23, 27 ago. 2021. Disponível em: https://www.cambridge.org/core/journals/legal-studies/article/abs/automated-facial-recognition-and-policing-a-bridge-too-far/347341E2BFA2EF1E3CC896A9C5ECDAD5. Acesso em: 12 nov. 2023.

SCHWAB, Klaus. A Quarta Revolução Industrial. 1. ed. São Paulo: Edipro, 2016.

TRINDADE, Rodrigo. Serviço misterioso pode te identificar a partir de fotos postadas na web. Uol, São Paulo, 18 jan. 2020, 13:58. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/01/18/servico-misterioso-de-pode-te-identificar-a-partir-de-fotos-postadas-na-web.htm. Acesso em: 12 nov. 2023, 21:19.

TSOUKALA, Anastassia. Defining the terrorist threat in the post-September 11 era. In: BIGO, D.; TSOUKALA, A. (org.). Terror, Insecurity and Liberty Illiberal practices of liberal regimes after 9/11. Oxon: Routledge, 2008. p. 49-99.

URQUHART, Lachlan; MIRANDA, Diana. Policing faces: the present and future of intelligent facial surveillance. Information & Communications Technology Law, v. 32, i. 2, p. 1-26, 28 out. 2021. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13600834.2021.1994220. Acesso em: 12 nov. 2023.