InterSciencePlace
International Scientific Journal – ISSN: 1679-9844
Volume 19, Article nº 48 January/December 2024
D.O.I: http://dx.doi.org/10.6020/1679-9844/v19a48
Accepted: 12/07/2024 Published: 21/12/2024

A ÉTICA NO EMPREGO DA TECNOLOGIA DE RECONHECIMENTO FACIAL (TRF) NA SEGURANÇA PÚBLICA

ETHICS IN THE USE OF FACIAL RECOGNITION TECHNOLOGY (FRT) IN PUBLIC SAFETY

Pablo Angely Marques Coimbra
Mestrando do Programa de Pós-graduação em Segurança Pública da Universidade Vila Velha (UVV - bolsista pela Fundação de Apoio e Amparo à Pesquisa-FAPES). Especialista *lato sensu* em Gestão Policial Militar e Segurança Pública pela Academia de Polícia Militar do Espírito Santo (APMES) e em Gestão Integrada em Segurança Pública pela UVV. Bacharel em Ciências Policiais e Segurança Pública pela APMES. Major QOC PM. Piloto policial de helicópteros e Chefe da Seção de Controle e Doutrina da Divisão de Operações do NOTAER/ES.
E-mail: pabloangely@gmail.com
ORCID: https://orcid.org/0009-0006-0757-587X

Renata de Ávila Caiaffa Bastos
Mestranda do Programa de Pós-graduação em Segurança Pública da Universidade Vila Velha (UVV - bolsista pela Fundação de Apoio e Amparo à Pesquisa-FAPES). Especialista em Psicologia Jurídica pela Universidade de Araraquara. Bacharel em Psicologia pela Universidade Vila Velha. Psicóloga. Psicóloga Clínica e Preceptora de Estágio na Universidade Vila Velha (UVV).
E-mail: renatacaiaffab@gmail.com
ORCID: https://orcid.org/0009-0005-0821-0832

Fabio Machado de Oliveira
Doutor e Pós-Doutor em Cognição e Linguagem – PPGCL/UENF, Bacharel em Ciência da Computação - UCAM, Licenciatura Plena em Matemática
ORCID: https://orcid.org/0000-0003-1336-2994

Henrique Geaquinto Herkenhoff
Doutor em Direito Civil (USP, 2011). Pós-Doutor em Administração Pública (UFES, 2021). Tem experiência na área de Direito e de Administração Pública, havendo atuado como professor de graduação e pós graduação lato sensu em Direito (UFES, 1993/2003), procurador de diversos órgãos públicos, membro do Ministério Público Federal em 1ª e 2ª Instância (1996/2007), Desembargador Federal do TRF3 (2007/2010) e Secretário de Estado da Segurança Pública do Espírito Santo (2011/2013). Atualmente é advogado.
ORCID: https://orcid.org/0000-0003-1267-1314

Resumo

Este artigo aborda as implicações éticas do uso da tecnologia de reconhecimento facial (TRF) na segurança pública, destacando a necessidade urgente de regulamentação adequada e a mitigação de preconceitos enviesados nesses sistemas. Com o crescente uso de sistemas biométricos, sobretudo o reconhecimento facial, surgem questões sobre privacidade, viés racial e possíveis violações de direitos fundamentais. A pesquisa utilizou uma metodologia qualitativa, com base em bibliometria e revisão de literatura focada em estudos acadêmicos sobre ética, tecnologia e segurança pública. Foram analisados casos de uso prático no Brasil e no mundo, destacando tanto os benefícios operacionais quanto os desafios éticos e legais dessa tecnologia. O estudo conclui que a regulamentação adequada é essencial para equilibrar a eficácia da segurança pública, garantindo a efetividade operacional, com a proteção dos direitos individuais, garantindo transparência, responsabilidade e mitigando vieses discriminatórios no uso da tecnologia de reconhecimento facial.

Palavras-chave: reconhecimento facial; ética; tecnologia; segurança pública.

Abstract

This article addresses the ethical implications of using facial recognition technology (FRT) in public safety, highlighting the urgent need for adequate regulation and the mitigation of bias in these systems. With the increasing use of biometric systems, especially facial recognition, questions arise about privacy, racial bias and possible violations of fundamental rights. The research used a qualitative methodology, based on bibliometrics and literature review focused on academic studies on ethics, technology and public security. Practical use cases in Brazil and around the world were analyzed, highlighting both the operational benefits and the ethical and legal challenges of this technology. The study concludes that adequate regulation is essential to balance the effectiveness of public security, ensuring operational effectiveness, with the protection of individual rights, ensuring transparency, accountability and mitigating discriminatory biases in the use of facial recognition technology.

Keywords: facial recognition; ethics; technology; public safety.

INTRODUÇÃO

A crescente integração de tecnologias avançadas no campo da segurança pública tem gerado um intenso debate sobre as implicações éticas de seu uso, de modo que a conexão cada vez mais profunda e mais capilarizada da

tecnologia às práticas policiais, sobretudo, traz consigo benefícios potenciais e uma ampliada gama de potencialidades, mas também apresenta desafios éticos que precisam ser cuidadosamente considerados (DUARTE *et al.*, 2021, p. 1; LIMA *et al.*, 2024, p. 3; SHUKRI, FADZIL, 2024, p. 85-86, tradução nossa).

Em diversas áreas das atividades humanas as câmeras de segurança, com escopo na vigilância, estão sendo usadas para monitoramento. Tal prática também se apresenta no campo da segurança pública, onde essa tecnologia, além de poder ser essencial para uma análise ou investigação pós-crime, tem o potencial em ajudar a deter ou interromper um delito antes que ele ocorra (SHUKLA; PANDEY, 2020, p. 14, tradução nossa).

Uma dessas tecnologias que se apresenta e vem sendo amplamente empregada no mundo e no Brasil, ainda que aqui em ambiente pátrio careçamos de uma regulamentação específica, são os sistemas biométricos de reconhecimento facial, que se constituem em uma tecnologia emergente central (OLIVEIRA *et al*. 2022, p. 115). As pesquisas relacionadas ao tema específico vêm apresentando crescimento acelerado e as imagens digitais para reconhecimento facial já são uma realidade de emprego em diversas aplicações, de maneira que

> Este interesse se materializa no desenvolvimento de artefatos tecnológicos e algoritmos de modo a permitir a criação de sistemas de reconhecimento facial precisos e robustos. As vantagens desta tecnologia sobre outras modalidades biométricas a tornam um alvo preferencial para emprego na vigilância e segurança pública (OLIVEIRA *et al*. 2022, p. 115).

Seu uso também perpassa pelo auxílio, nas atividades policiais, na identificação e localização de suspeitos e de pessoas em situações vulneráveis, como é o caso do emprego na localização de crianças e idosos desaparecidos (GIKAY, 2023, p. 419, tradução nossa). Os sistemas biométricos de reconhecimento facial também já apresentam registros positivos de uso na identificação com posterior prisão de indivíduos com mandados de prisão em aberto e até na prevenção de potenciais ameaças de situações de terrorismo (GIKAY, 2023, p. 419-420, tradução nossa).

Contudo, os velozes avanços no emprego dessa tecnologia conjugados aos modelos de aprendizagem de máquina (*"machine learning"*), em que a atividade da inteligência artificial (IA) supera facilmente a capacidade humana de trabalho, de concentração e de foco (SHUKLA; PANDEY, 2020, p. 14, tradução

nossa), estimulam a importância de estudar a ética no emprego da tecnologia de reconhecimento facial (TRF) na segurança pública. Isso porque há uma necessidade de equilibrar a eficácia operacional com o respeito aos direitos humanos, como em qualquer outra atividade de polícia. Negligenciar esse tema pode resultar em consequências sérias para a sociedade, como a violação da privacidade e a discriminação sistêmica, além de implicar em desafios para os próprios operadores de segurança, que podem ser expostos a dilemas éticos e a riscos legais (LIMA *et al.*, 2024, p. 5-8).

Nesse sentido, complementa Gikay (2023, p. 420, tradução nossa) que a tecnologia de reconhecimento facial

> [...] traz vários riscos que podem minar os direitos de indivíduos e o bem-estar dos cidadãos. Duas preocupações comumente citadas são: o potencial de imprecisão decorrente de conjuntos de dados de treinamento de modelos tendenciosos; e intrusão de privacidade e vigilância.

Para nossa compreensão inicial, como explicita Lynch (2024, p. 2, tradução nossa), imagem facial é um tipo de identificação biométrica semelhante a impressões digitais, escaneamentos de íris ou mesmo impressões vocais: sua finalidade reside, em tese, na capacidade de identificar um indivíduo de maneira única, distinguindo-o de outros. Esse processo de identificação, assim como os demais citados como exemplo, contém informações do indivíduo que lhe são exclusivas e, por vezes, sensíveis, com a extrema diferença que podem ser coletadas pelas autoridades de segurança a grandes distâncias e mesmo sem o consentimento ou o conhecimento da pessoa afetada (LYNCH, 2024, p. 2, tradução nossa).

Do ponto de vista ético, é preciso conjugar ainda as visões acima com o que alertam Duarte *et al.* (2021, p. 3) sobre o uso de tais sistemas nas rotinas policiais nas quais, em casos mais extremos, existe a possibilidade de que pessoas sejam privadas de sua liberdade em virtude do emprego do reconhecimento facial, além de “[...] todos os efeitos que decorrem desta medida extrema de retirada do indivíduo do convívio social” (DUARTE *et al.*, 2021, p. 3).

Diante da breve problemática descrita e da relevância que se depreende do tema, este artigo objetiva analisar, brevemente, as implicações éticas no emprego da tecnologia de reconhecimento facial na segurança pública: é imprescindível que o uso de tais sistemas automatizados por operadores de segurança pública seja fundamentado em métodos técnicos e científicos a fim

de se alcançar o devido e legítimo equilíbrio entre o direito de privacidade do cidadão, a transparência e prestação de contas às comunidades e a proteção e segurança jurídica desses mesmos operadores em suas atuações diárias.

Para o debate proposto, foi adotada neste artigo uma metodologia qualitativa, com uma abordagem exploratória e descritiva. A revisão teórica foi o principal método de coleta de dados, analisando criticamente obras acadêmicas que versam sobre ética, tecnologia e segurança pública. Tal análise foi empregada para relacionar os conceitos de ética com o uso específico de tecnologias na segurança pública. A revisão também incluiu estudos sobre possíveis implicações sociais do uso de tecnologias de segurança, com foco e recorte no reconhecimento facial. Para tanto, buscou-se, sem esgotar a temática, uma resposta para o problema provocado. As fontes selecionadas foram prioritariamente produções científicas nas bases de dados do *Google Scholar*, do *SciELO*, do *Scopus* e dos Periódicos da CAPES, somando, em um primeiro momento, 80 publicações acadêmicas sobre a temática aqui abordada. Para as buscas em tais bases foram utilizadas as palavras-chave “ética”, “tecnologia”, “segurança pública”, “reconhecimento facial”, inclusive em inglês e com a combinação variada de operadores booleanos. Todas as produções encontradas foram avaliadas considerando sua relevância para a abreviada discussão deste artigo, sendo que as selecionadas foram gerenciadas, à luz da bibliometria, por meio *software Zotero,* com armazenamento, organização e compartilhamento, e do *software VOSviewer,* para operacionalizar a construção de mapas que permitem visualizar as redes bibliométricas e sua relevância junto ao tema, tudo com a meta de sintetizar comparativamente as informações coletadas. A metodologia também se baseou em estudos de caso que ilustram as aplicações práticas e os desafios éticos do uso de tecnologias bem como em breves dados estatísticos a respeito da adoção da tecnologia de reconhecimento facial pelas instituições de segurança pública do Brasil.

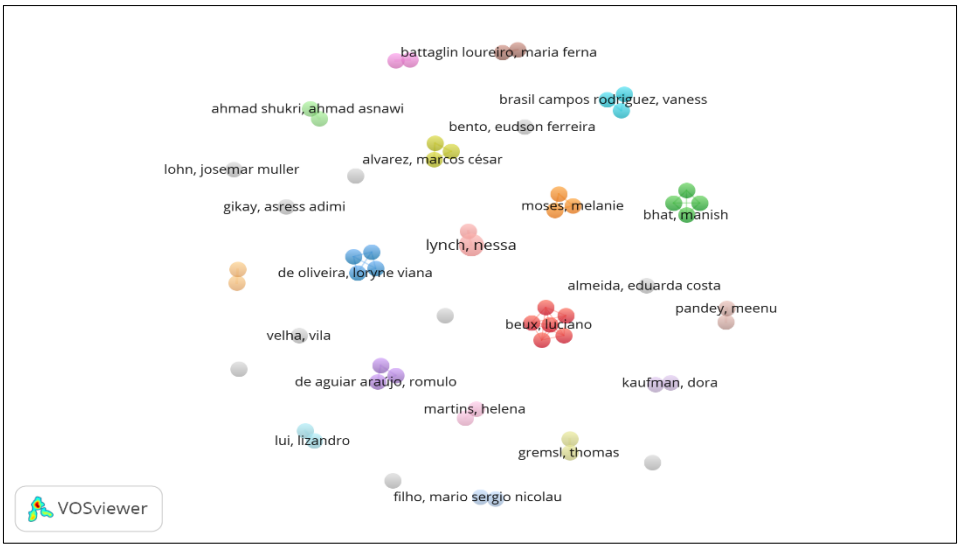

Figura 01 - Esquema (*clustering*) da bibliografia selecionada.
Fonte: Elaborada pelos autores no *VOSviewer* (2024).

O mapa de referência acima foi retirado e elaborado através do software *VOSviewer* sendo colocadas as bibliografias selecionadas para produção deste artigo conforme seus agrupamentos e características teóricas proximais dos autores selecionados.

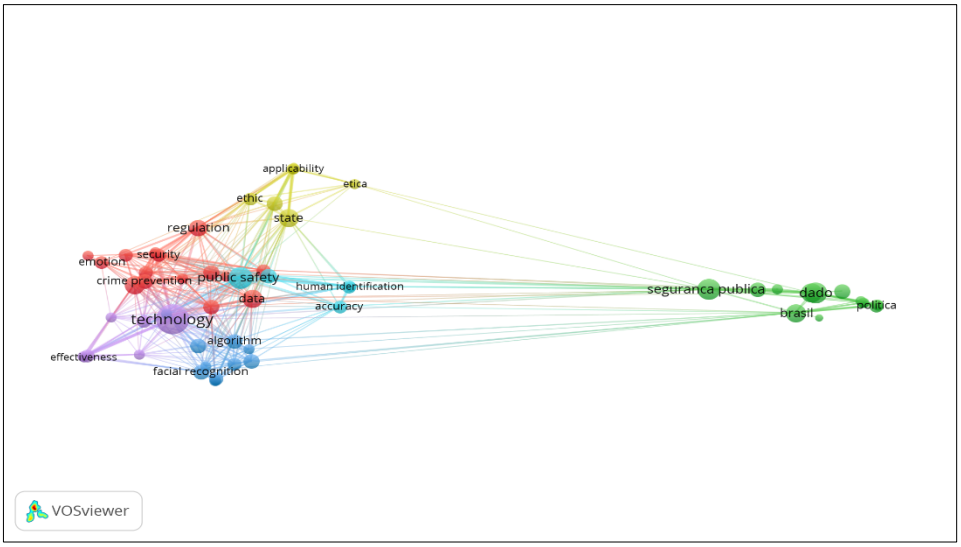

Figura 02 – Visão esquemática da bibliometria realizada.
Fonte: Elaborada pelos autores no *VOSviewer* (2024).

O mapa de referência ante exposto é referente a uma visão esquemática, realizada com o software *VOSviewer* com base na bibliometria efetivada, da ligação entre as principais palavras-chave da revisão teórica, sobretudo a relação entre a segurança pública com a tecnologia passando pela ética, a identificação humana e outras questões relevantes.

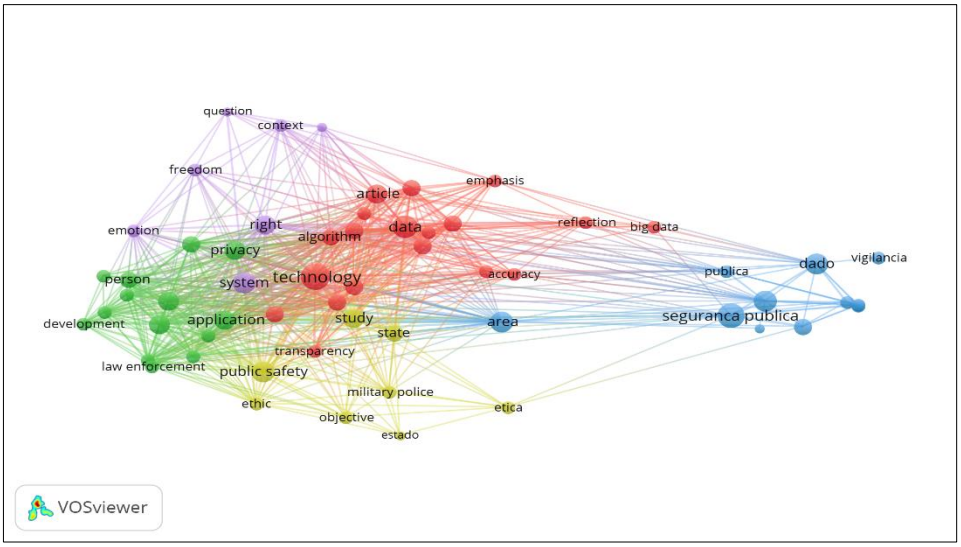

Figura 03 – Visão esquemática, com base na bibliometria realizada.
Fonte: Elaborada pelos autores no *VOSviewer* (2024).

No mesmo sentido, a Figura 03 representa uma visão esquemática dos termos de maior relevância na revisão teórica realizada, sua ligação em *clusters* e também a interligação entre eles.

1 A TECNOLOGIA DE RECONHECIMENTO FACIAL

A sociedade contemporânea experimenta uma era de datificação [1] (*datafication*): toda ação e interação social são transformadas em dados que são quantificados e também qualificados, conforme o objetivo pretendido e de modo *on-line*, o que permite que as pessoas sejam monitoradas em tempo real e que seus comportamentos sofram inclusive uma espécie de análise preditiva, fazendo com que lhes sejam "oferecidos" serviços, promoções, produtos e conforto (conforme a visão e as preferências de cada um). Isso se aplica desde o uso extremamente individual e privado de um *smartphone* repleto de aplicativos até situações mais "coletivas" quando, por exemplo, permite-se que seja feita uma foto para cadastro para acesso a determinado prédio, academia ou consultório, tarefa hoje rotineira e muitas vezes acompanhada do fornecimento voluntário de dados pessoais, como nome completo, número de telefone, endereço de correio eletrônico, entre outros.

Não se trata aqui de desconhecer os benefícios da tecnologia, mas fica explícito que o uso indiscriminado da datificação é um risco à privacidade dos dados pessoais: um cruzamento de dados de diversos bancos de armazenamento, por exemplo, e na velocidade em que trabalham os superprocessadores, pode levar a conclusões muito precisas e específicas sobre detalhes da vida íntima de qualquer pessoa. Projetando essa preocupação para o campo da segurança pública e da vigilância, não se torna tarefa difícil imaginar consequências da datificação para a privacidade e demais direitos individuais em situações em que não haja a devida regulação e transparência de emprego (LIMA *et al.*, 2024, p. 6; SANTAELLA; KAUFMAN, 2021, p. 220).

As tecnologias de biometria pertencem a esse mundo datificado, utilizando de suas fontes e sinergicamente fornecendo ininterruptamente dados para os mesmos bancos de onde se alimentam. Para a compreensão de nosso

[1] Datificação é um termo atualmente empregado para definir a quantificação e a qualificação da vida, das informações pessoais e de comportamentos em dados. Isso se torna uma valiosa moeda para empresas e governos, constituindo-se em verdadeiros ativos digitais. Diversas plataformas tecnológicas coletam e interpretam esses dados, direcionando para os usuários anúncios relacionados às suas pesquisas e interações nas redes sociais, tudo para sua "melhor experiência". A vida atual datificada se converte, a todo instante, em dados computadorizados: o monitoramento por algoritmos de inteligência artificial é uma constante, percebam e consintam as pessoas ou não (MARTINS; VALENTE, 2019; SANTAELLA; KAUFMAN, 2021; GREMSL; HÖDL, 2022, tradução nossa).

breve estudo, podemos dizer que a etimologia do vocábulo *biometria*, de maneira simples, seria algo como medida (*metria*) do vivo ou da vida (*bio*). Na relação prática de emprego da tecnologia em questão, seria um "[...] método para a determinação da identidade de uma pessoa com fundamento nas suas características biológicas (anatômicas, bioquímicas e fisiológicas) e ou comportamentais" (BRASIL, 2022, p. 5). A legislação da União Europeia (UE) a respeito do tema, bastante avançada na discussão e pujante na sua constituição, traz uma definição de dados biométricos:

> [...] dados pessoais resultantes de processamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitem ou confirmam a identificação única dessa pessoa natural, como imagens faciais ou dados dactiloscópicos (GIKAY, 2023, p. 418, tradução nossa; LYNCH, 2024, p. 2, tradução nossa).

O reconhecimento facial, portanto, encaixa-se no grupo das biometrias. O entendimento técnico predominante atualmente define que o exame da face de uma pessoa, via emprego de uma tecnologia biométrica, desenvolve-se de duas formas que são a comparação facial e o reconhecimento facial propriamente dito (BRASIL, 2022, p. 5):

> A primeira forma de identificação[2] denomina-se exame de comparação facial e envolve o confronto entre duas imagens, com o fim de determinar se foram ou não produzidas pelo mesmo indivíduo. A primeira, denominada imagem padrão, consiste em amostra cuja autoria é conhecida, ao passo que a segunda, imagem questionada, detém autoria desconhecida. Ato seguinte, o examinador analisa os dois objetos com fundamento nas características anatômicas da face, a fim de determinar se pertencem ou não ao mesmo indivíduo. Em caso de resultado positivo, fica estabelecida a identificação da pessoa. A segunda forma de identificação facial denomina-se Reconhecimento ou Busca Facial (*Facial Recognition*). Esse exame biométrico difere do anterior, em razão da necessidade de uso de software para reconhecimento de faces, o que lhe confere maior grau de complexidade quando comparado à comparação facial pura e simples.

O emprego automatizado via *softwares* específicos permite que a TRF seja usada, como descrito, em uma variedade de aplicações gerais e nos contextos específicos de policiamento, envolvendo a análise de um modelo gerado por computador com base em imagens faciais de determinada pessoa e

[2] Para efeitos do nosso breve estudo, usaremos os conceitos de identidade como um conjunto de características físicas, funcionais e ou psíquicas, inatas ou adquiridas, porém permanentes, que tornam uma pessoa diferente das demais e idêntica a si mesma (BRASIL, 2022) e de identificação como processo de determinação da identidade de uma pessoa, comparando-se dados obtidos no presente com outros previamente armazenados em bancos de dados (BRASIL, 2022).

a comparação com bancos de imagens já armazenadas (isso se dá por meio da transformação das características faciais em representações numéricas compreensíveis para a inteligência artificial para permitir a comparação), considerando atributos faciais específicos (forma de mandíbula, distância entre olhos e entre esses e nariz, além de outros pontos de referência únicos e individualizantes no rosto de uma pessoa) (LYNCH, 2024, p. 2, tradução nossa; RANKIN; MOSES; POWERS, 2024, p. 678, tradução nossa; SARTORI, 2024, p. 80).

Essa característica computacional permite, como vantagem, a possibilidade de uso em "[...] grandes espaços públicos para monitorar potenciais alvos, sem a necessidade de abordagem policial direita, pessoal e invasiva" (BRASIL, 2022, p. 10). Além da cobertura espacial ampla e à distância, o emprego sistematizado e autônomo se impõe com vantagens claras sobre o serviço humano nessa mesma tarefa no que tange à fadiga, à velocidade de processamento, à capacidade de foco e de permanência ininterrupta na atividade. Além disso, em casos específicos, a TRF pode ajudar atividades de inteligência policial, inclusive com o intuito de minimizar ações e abordagens que feitas da maneira tradicional podem resultar, em última instância, em confrontos armados com danos para os próprios policiais e para terceiros inocentes: o monitoramento e o acompanhamento de um alvo podem ser realizados e uma abordagem ou interceptação planejadas para que ocorram em área que minimize os danos colaterais e de forma que reduzam as chances de reação e ou de fuga, por exemplo.

Toda essa lógica, entretanto, depende da inserção prévia de imagens das faces de pessoas em sistemas biométricos para que a análise possa ser realizada pelo computador e a inteligência artificial específica possa ir aprendendo, a cada erro e acerto via os algoritmos empregados. Esse, sinteticamente, é o processo que se denomina na ciência da computação de *machine learning* (aprendizado de máquina), no qual a máquina é calibrada através de critérios de aceitação e rejeição da comparação (erros e acertos) para evitar o que se chama de falsos positivos ou falsos negativos. Esse é um ponto crucial, pois a efetividade do sistema vai depender da forma que essa calibragem de margem de erro é realizada (DUARTE *et al.*, 2021, p. 5).

As situações mais críticas para a atividade policial e para a garantia dos direitos individuais ocorrem quando há imprecisão da tecnologia no reconhecimento e os resultados apresentados são errôneos. Primeiramente, podem ocorrer os falsos negativos, ou seja, a chamada assinatura facial do sujeito está contida no banco de dados, mas o sistema falha ao indicar a correspondência com o rosto em questão, retornando zero resultados (quando, na verdade, há um resultado válido, podendo se tratar de pessoa que cometeu crime). No segundo momento, ocorrem os falsos positivos quando o sistema indica uma compatibilidade entre o rosto capturado ou monitorado de uma pessoa em tempo real e um rosto datificado no banco de dados, sendo que não se trata da mesma pessoa (constituindo-se em um resultado inválido e que pode ensejar consequências fáticas diversas para esse cidadão, causando danos a uma pessoa não culpável) (ALMEIDA, 2022, p. 268).

São processos amplos e variados, em sistemas automatizados, que tentam identificar ou validar a identidade de uma pessoa (BUOLAMWINI *et al.*, 2020, p. 2, tradução nossa; OLIVEIRA *et al*. 2022, p. 116) conforme a categoria em que esses sistemas se enquadram. De modo geral, a TRF pode ser agrupada em três categorias mais amplas, conforme a especificidade da questão que buscam responder: "[...] (a) *há um rosto na imagem?*; (b) *que tipo de rosto há na imagem?*; e (c) *a quem pertence o rosto na imagem?*" (BUOLAMWINI *et al.*, 2020. p. 2, tradução nossa).

A complexidade e os desafios são tamanhos, uma vez que responder a tais questionamentos aparentemente "simples" exige da tecnologia de reconhecimento facial lidar com questões intrínsecas e extrínsecas ao sistema e que podem comprometer a sua confiabilidade, como envelhecimento da pessoa real (que não necessariamente será acompanhado do seu envelhecimento virtual), a luminosidade no momento e local do monitoramento, as expressões faciais, a velocidade de processamento e armazenamento, o tamanho e a qualidade da imagem, o ângulo de visão fornecido pela câmera de vigilância e a variabilidade entre tipos de etnias (BUOLAMWINI *et al.*, 2020. p. 2, tradução nossa; DUARTE *et al.,* 2021, p. 5).

Porém, o mais contundente desses fatores, inclusive pelo ponto de vista ético, são os vieses nos dados[3] de treinamento da tecnologia em questão (BUOLAMWINI *et al.*, 2020, tradução nossa; RANKIN; MOSES; POWERS, 2024, tradução nossa): conforme destacado por pesquisadores, o viés na alimentação e no treinamento desses sistemas impacta, de forma significativa, indivíduos de pele mais escura, com alguns sistemas, conforme registros, falhando em aproximadamente vinte e dois por cento desses rostos. Em contrapartida, para o grupo composto por rostos masculinos e de pele clara a taxa de erro foi menor do que um por cento (CODED, 2020, tradução nossa; RANKIN; MOSES; POWERS, 2024, tradução nossa). Uma relação indicada nessas pesquisas, inclusive, é que a maior parte dos dados que treinam os modelos analisados foram coletados da força de trabalho de tecnologia masculina branca (RANKIN; MOSES; POWERS, 2024, p. 678-679, tradução nossa).

Esse alerta, ainda que no campo do ensaio para a realidade capixaba, indica que todo o processo de treinamento de IA, as coletas de dados para a aprendizagem de máquina e a alimentação de bancos de dados devem considerar a perspectiva empregada ou, melhor ainda, não se revestir de quaisquer vieses a fim de que consequências intencionais ou não da atuação do reconhecimento facial por meio da IA não ditem os resultados socias do emprego dessa ferramenta. Isso nos leva a pensar então em importantes considerações éticas que precisam ser feitas quando do emprego dessas tecnologias para a segurança pública tendo em mente que para a aplicação da lei “[...] é crucial ter clareza sobre a regulamentação do uso da tecnologia [...]” (GIKAY, 2023, p. 416, tradução nossa).

2 BREVES CONSIDERAÇÕES ÉTICAS

Como visto, o emprego de TRF na segurança pública é uma atividade que apresenta vantagens, mas pode se revestir de riscos para os direitos fundamentais do indivíduo, sobretudo nos aspectos da liberdade, da privacidade

[3] “Isso é comumente atribuído à seleção tendenciosa de dados, também conhecida como viés estatístico, que ocorre quando dados de certos grupos são sub-representados no conjunto de dados de treinamento” (GIKAY, 2023, p. 421, tradução nossa). Para informações mais detalhadas, sugerimos assistir ao documentário *Coded Bias* (CODED, 2020).

e da inviolabilidade da vida íntima, que se constituem em valores caros à sociedade moderna (ALMEIDA, 2022, p. 273).

A sociedade, por sua vez, de maneira acertada apresenta uma conduta mais ativa diante de atos ilegais ou ilegítimos praticados por agentes do estado, inclusive os responsáveis pela aplicação da lei, cobrando transparência, realizando denúncias e exigindo providências no sentido de reparação cujo objetivo é manter minimamente uma reciprocidade na relação (FILHO; NICOLAU, 2022, p. 70215), o que se pode chamar de uma mudança da postura ética da sociedade diante do que normaliza como legítimo e assume como ilegítimo e, em muitas vezes por decorrência, como ilegal.

Se por um lado a sociedade estabelece parâmetros e cobranças, as instituições responsáveis por operacionalizar a segurança pública não se distanciam desse pensamento. Tomando como exemplo, no recorte territorial capixaba, a Polícia Militar do Espírito Santo (PMES), a conceituação de ética aparece dentro de um escopo duplo, servindo tanto para definir, especificar e classificar as eventuais infrações disciplinares cometidas pelos agentes quanto para estabelecer condutas norteadoras na atividade policial, entre as quais

> [...]
> § 1º São manifestações da ética:
> I - cultuar a verdade, a lealdade e a responsabilidade como fundamentos de dignidade pessoal;
> II - exercer, com autoridade, eficiência e probidade, as funções que lhe couberem em decorrência do cargo ou função;
> [...]
> XV impessoalidade, imparcialidade e objetividade;
> XVI - preservação da intimidade e do sigilo profissional; e
> XVII - exercício da tolerância e do respeito às diferenças [...] (ESPÍRITO SANTO, 2021, p. 1-2).

É evidente que ambas as formas buscam um modo de sancionar atitudes que excedem a práxis social salutar e eficiente.

Seja em âmbito social amplo ou em grupos específicos, como no exemplo da PMES, é preciso compreender que preceitos que ditam a ética nas relações são fundamentais visando um corpo social bem sucedido, até porque esses grupos específicos em dados momentos e em maior ou menor grau irão interagir com outros grupos dentro do contexto social. É o caso do emprego de TRF nas atividades de segurança pública. Nessas relações é preciso caminhar no sentido do que afirmam Gremsl e Hödl (2022, p. 168, tradução nossa):

> A ética deve, portanto, concentrar-se no bem-estar das pessoas – todas elas – que são afetadas por essas tecnologias, e isso,

> por sua vez, chama a atenção para duas questões-chave: o debate sobre o bem comum e a dignidade humana.

Nesse esteio, é importante que na construção e no emprego da tecnologia de reconhecimento facial os vieses comentados anteriormente, à luz das considerações éticas, sejam analisados quanto aos riscos discriminatórios que possam apresentar, quais sejam: num primeiro momento, na estruturação da base de dados histórica, já que os algoritmos irão começar a aprender com as informações anteriores e previamente carregadas; na sequência, na formação da equipe desenvolvedora, que deve ser norteada a trabalhar com boas práticas de governança e de respeito aos direitos individuais e à dignidade humana; e, por fim, na gestão e na avaliação do aprendizado do sistema ao longo do tempo (MARTINS, 2023).

Conforme Almeida (2022, p. 276) um relatório produzido pelo *Big Brother Watch (BBW)*, que se trata de um grupo que atua em campanhas de liberdades civis no Reino Unido e prioritariamente preocupados com questões de privacidade e de liberdades neste momento de enorme mudança tecnológica (BBW, 2018, p. 3, tradução nossa) indica que naquele território 95% das correspondências indicadas via TRF resultaram em falsos positivos. Quais os impactos disso, dessas correspondências inexatas? As considerações éticas acima exemplificadas estão sendo levadas a efeito? São questionamentos válidos e que temos de ter em mente pensando na aplicação dessas tecnologias no Brasil.

Retomando em nossa discussão a informação de Buolamwini *et al.* (2020, tradução nossa) e de Rankin, Moses e Powers (2024, tradução nossa) de que alguns sistemas podem falhar em até vinte e dois por cento dos casos quando se tratam de pessoas de pele preta e parda e considerando os dados do último censo demográfico (IBGE, 2022) do Instituto Brasileiro de Geografia e Estatística (IBGE), no qual consta para a população capixaba um total de 3.833.712 pessoas, sendo que a população negra do Espírito Santo representa o percentual aproximado de 61% desses residentes (cerca de 49,78% de pardos e 11,21% de pretos, um valor de 2.338.564 milhões de pessoas), o erro indicado acima, se reproduzido aqui, poderia afetar, por exemplo, até 514 mil pessoas aproximadamente por conta da construção e do emprego da tecnologia de reconhecimento facial com base em vieses discriminatórios.

Outra questão que não se pode perder de vista nessa discussão é como são usados os dados construídos para emprego da tecnologia de reconhecimento facial. A datificação constrói verdadeiras minas de ouro virtuais e seu mau uso ou mesmo vazamento, pensando em bancos de dados a serviço do Estado e dos governos, podem servir de combustível para práticas de delitos diversos, como fraudes, estelionatos, entre outros – um "mais do mesmo", porém moderno, da criminalidade.

Nesse ponto, a Lei Geral de Proteção de Dados Pessoais (LGPD), aprovada em 2018 (BRASIL, 2018) se constitui em legislação fundamental e genérica para a lida diária nessa seara e também para a nossa análise, uma vez que representa impactos éticos diretos sobre a privacidade e o tratamento de dados pessoais no Brasil. O dispositivo legal aborda o tratamento de dados pessoais

> "[...] **inclusive nos meios digitais**, por pessoa natural ou por **pessoa jurídica de direito público** ou privado, com o objetivo de **proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural** (BRASIL, 2018, p. 1, grifo nosso).

O reconhecimento facial é considerado um dado sensível pela LGPD[4]. Isso significa que seu tratamento, em regra geral, deve ser feito com cautela e seguindo regras específicas. As instituições que coletam, tratam, armazenam ou retiram dados biométricos, como o reconhecimento facial, devem informar aos titulares o motivo da captura, o período de armazenamento e obter aprovação para o uso. O titular tem o direito de aprovar ou solicitar a retirada de suas informações. A legislação em tela apresenta ainda alguns princípios aplicáveis ao reconhecimento facial, tais como: a boa-fé, a finalidade, a adequação, a necessidade, o live acesso por parte do titular, a qualidade dos dados, a transparência, a segurança, a prevenção de danos, a não discriminação e a responsabilização e prestação de contas (BRASIL, 2018, p. 3-4).

Logo, a regra geral serve para reforçar a importância dos cuidados éticos necessários ao se tratar o reconhecimento facial. Contudo, existem as exceções

[4] Para efeitos da LGPD, conforme seu inciso II, artigo 5º, é considerado um dado sensível: "[...] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou **biométrico, quando vinculado a uma pessoa natural**" (BRASIL, 2018, p. 2, grifo nosso).

previstas para a segurança pública, de acordo com a própria LGPD, ou seja, situações em que o consentimento não é necessário. Por exemplo, a supracitada Lei permite o tratamento de dados pessoais e o reconhecimento facial sem consentimento quando necessário para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou ainda atividades de investigação e repressão de infrações penais (artigo 4º, inciso III) com a ressalva de que tal teor previsto "[...] será regido por legislação específica, que deverá **prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público**, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (BRASIL, 2018, p. 2, grifo nosso).

A mencionada legislação específica ainda não existe no país, deixando uma vacância no assunto quando se trata do tratamento de dados pessoais no âmbito da segurança pública e, por consequência, do emprego de TRF. O que há é um Projeto de Lei em discussão na Câmara dos Deputados[5] (BRASIL, 2022) que busca regulamentar o uso de reconhecimento facial pelas forças de segurança pública no Brasil em investigações criminais ou procedimentos administrativos. O projeto propõe que ações de restrição da liberdade de ir e vir baseadas apenas em reconhecimento facial sejam confirmadas por especialistas e que placas visíveis informativas sejam fixadas nos locais onde ocorre a captura de imagens para esse fim (BRASIL, 2022, p. 1-2) a fim de promover a transparência da ação para o público.

A ideia defendida pelo relator do Projeto é estabelecer regras claras para o uso dessa tecnologia, garantindo que ela seja aplicada de forma responsável e respeitando os direitos individuais. De acordo com o Projeto, o reconhecimento facial poderá ser utilizado no âmbito de investigações policiais "[...] sempre que houver necessidade de se averiguar a identidade de autores, coautores, testemunhas e ou vítimas relacionadas a algum fato criminoso" (BRASIL, 2022, p. 1) ou ainda em procedimentos administrativos e ou cíveis para "[...] a busca

[5] De acordo com informação disponível no sítio eletrônico da Câmara dos Deputados, a última movimentação do Projeto se deu em 14 de março de 2023 com a proposição sendo sujeita à apreciação conclusiva pelas Comissões envolvidas; o Projeto permanece aguardando o parecer do Relator na Comissão de Constituição e Justiça e de Cidadania (CCJC). Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2345261. Acesso em: 10 set. 24.

de pessoas eventualmente desaparecidas, tais como crianças, idosos, pessoas em situação de vulnerabilidade, entre outros" (BRASIL, 2022, p. 1).

Outros pontos do Projeto que merecem ser destacados e por nós entendidos como sensíveis são os que afirmam que nenhuma ação policial destinada a restringir a liberdade de ir e vir de qualquer pessoa poderá ocorrer, com emprego de reconhecimento facial, sem a validação de um revisor ou de um perito papiloscopista com especialização em identificação facial. O uso de TRF pelas polícias poderá ser feito tanto a partir de equipamentos públicos para esse fim específico quanto a partir do emprego de imagens fornecidas por terceiros, mediante a devida regulamentação (BRASIL, 2022).

O relator do Projeto defende as medidas aqui exemplificadas e outras com base na premissa de que a tecnologia deve ser aplicada com precaução para que eventuais falhas não se convertam em restrição injustificada de direitos dos cidadãos, sobretudo da liberdade das pessoas. A intenção é que o dispositivo, se promulgado, seja um norteador do equilíbrio entre as atividades de segurança pública e a proteção dos direitos individuais no emprego da TRF no país, destacando que embora "[...] saibamos que o seu uso foi afastado em alguns países, entendemos que essas restrições decorrem do seu uso equivocado e do desconhecimento de alguns para com a tecnologia de reconhecimento facial" (BRASIL, 2022, p. 4).

Do que vimos até aqui, percebe-se que há uma amplitude enorme de possibilidades de emprego dessa tecnologia passando por questões éticas de seu emprego, que podem ser ou estar enviesadas, e culminando em uma necessidade de regulação que não é só brasileira, mas que está em voga mundo afora. No Brasil, apesar de se haver caminhado no sentido da proteção de dados pessoais, ainda há um vácuo no ordenamento jurídico quando se trata de regulamentar as ações de reconhecimento facial no campo da segurança pública – o que significa, como alertamos, proteção e garantias para a sociedade como um todo e para os operadores de segurança em sentido estrito. A regulamentação específica se torna fundamental por ser vetor capaz de "[...] incorporar os conhecimentos dos campos social, político, jurídico e econômico no campo da ciência, tecnologia e inovação" (SANTOS; PRADO; RODRIGUEZ, 2023, p. 82).

Sobre a proteção de dados pessoais em sentido geral e a ausência de regulamentação específica para tratamento desses dados no campo da segurança pública no que diz respeito ao reconhecimento facial, chama atenção o dado trazido pela revista eletrônica Consultor Jurídico (TAJRA, 2024b, n. p.) ao analisar dados das secretarias estaduais de segurança pública. O levantamento indica que até maio de 2024 um pouco mais de mil e setecentas pessoas já haviam sido presas com base no emprego de tecnologia de reconhecimento facial, mesmo sem a devida regulamentação – e que somente cinco estados da federação forneceram suas estatísticas a respeito (TAJRA, 2024b, n. p.), o que indica que esse número pode ser bem maior. De acordo com o levantamento realizado, a Bahia responde por um percentual de 90% das prisões aferidas, em torno de 1.547 pessoas, desde que implantou o sistema em 2018 e começou a usar a TRF no Carnaval de 2019[6]. Em São Paulo, aquela Secretaria de Segurança reportou a prisão de 52 pessoas com mandados de prisão em aberto. O Rio de Janeiro informou que emprega a tecnologia desde o final de dezembro de 2023 e que em virtude disso mais de 130 pessoas já foram detidas. Roraima, por sua vez, indicou o uso do sistema em meados de 2023, durante as festas juninas, o que resultou na prisão de 15 pessoas. E, por fim, Sergipe[7] indicou a prisão de oito pessoas desde que começou a usar a tecnologia (TAJRA, 2024b, n. p.).

O levantamento ainda chama a atenção (TAJRA, 2024b, n. p.) para o fato de que há unidades federativas que afirmam usar a TRF em nível estadual de segurança pública, mas não forneceram dados detalhados, sobretudo sobre

[6] Para nossa discussão importa citar aqui, conforme demonstram Santos, Prado e Rodriguez (2023, p. 79-80) que os sistemas de reconhecimento facial "[...] na área de segurança pública foram oficialmente inaugurados no Brasil em 2019, por meio da Portaria nº 793/2019, do Governo Federal. O art. 4º, III, b, do referido documento, autorizou o uso do Fundo Nacional de Segurança Pública no fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition - OCR*, uso de inteligência artificial ou outros, como medida de enfrentamento à criminalidade. É importante tecer comentários em relação à palavra "oficialmente", pois como se pôde observar, esses sistemas foram implantados na segurança pública do estado da Bahia no ano anterior à Portaria, ignorando as questões éticas, morais e jurídicas que envolvem o tema".

[7] O estado de Sergipe responde por duas prisões equivocadas com o emprego da TRF. De acordo com o levantamento da revista Consultor Jurídico, tais registros foram excluídos dos dados oficiais. Mais à frente abordaremos detidamente o caso das prisões.

número de prisões. Por exemplo, as secretarias de Acre e Maranhão se limitaram a confirmar que usam a tecnologia para fins policiais sem fornecer demais informações. No Pará, a secretaria admitiu que emprega, mas que não há como mensurar o número de prisões. Em Minas Gerais, a secretaria de segurança indicou ter feito testes no Carnaval de 2024 e ter avaliado bem o sistema, sem ter efetuado prisões. No Espírito Santo[8], o governo anunciou que a partir de 10 de setembro de 2024 o sistema de reconhecimento facial voltado às ações de segurança pública começou a operar integrado a câmeras já existentes nos sistemas de transporte público e nas estradas que cortam o estado. Outros estados, como Tocantins, Mato Grosso, Alagoas, Ceará e Goiás informaram que os projetos de emprego de TRF na segurança pública se encontram em fase de estudo, de testes ou em vias de implantação, enquanto Santa Catarina, Paraná, Mato Grosso do Sul, Piauí, Rio Grande do Norte e o Distrito Federal reportaram que não empregam a tecnologia em questão para fins de segurança pública estadual. O levantamento informa ainda que Paraíba, Pernambuco, Rio Grande do Sul, Amazonas e Amapá não responderam à coleta dos dados da revista eletrônica (TAJRA, 2024a, n. p.; TAJRA, 2024b, n. p.). Apesar de não constar no levantamento feito pela revista eletrônica, os autores deste artigo detectaram que a secretaria de segurança pública estadual de Rondônia já emprega a TRF em atividades policiais[9].

Uma relevante contribuição para nossa discussão são os dados trazidos pelo Panóptico[10], um projeto desenvolvido pelo Centro de Estudo de Segurança e Cidadania (CESeC), do Núcleo de Estudos da Violência da Universidade de São Paulo (NEV/USP), que se dedica, desde 2019, a monitorar a adoção da tecnologia de reconhecimento facial pelas instituições de segurança pública do Brasil (LIMA *et al.*, 2024; PANÓPTICO, 2024). Por exemplo, um dos efeitos detectados pelo projeto a respeito de efeitos de emprego de TRF pelas polícias é que “[...] cerca de 90% das pessoas presas com o uso dessa tecnologia eram

[8] Disponível em: https://www.agazeta.com.br/es/cotidiano/cameras-comecam-a-fazer-reconhecimento-facial-em-onibus-e-estradas-no-es-0924.

[9] Vide https://www.alertarolim.com.br/noticia/caca-foragidos-cameras-de-reconhecimento-facial-serao-utilizadas-pela-policia-durante-o-carnaval-em-ro.

[10] Vide https://www.opanoptico.com.br/#mapa.

negras” (PANÓPTICO, 2024, n. p.). Outra contribuição relevante para a avaliação do emprego da tecnologia e das considerações éticas que lhe são devidas é mostrar onde o reconhecimento facial está sendo aplicado no país, trazendo dados pormenorizados sobre os casos de adoção nos estados e municípios brasileiros, “[...] além de apresentar o papel de governos e empresas no financiamento e na oferta dessa tecnologia” (PANÓPTICO, 2024, n. p.).

O Projeto Panóptico acompanha a aplicação de TRF em locais como vias públicas, estádios e escolas, direcionando seu levantamento de dados para projetos que utilizam o reconhecimento facial para identificar indivíduos (PANÓPTICO, 2024). Sua metodologia[11] foca em entidades governamentais ou privadas que compartilham dados com os governos para fins de segurança pública, permitindo uma capilarização a nível de municípios que empregam a tecnologia. Importa ressaltar que sistemas em espaços privados não são incluídos em seus bancos de dados (PANÓPTICO, 2024).

Assim, algumas informações relevantes merecem ser destacadas (PANÓPTICO, 2024)[12]:

a) atualmente há 282 projetos que utilizam técnicas de reconhecimento facial no país;
b) tais projetos se refletem em 76.596.071 pessoas potencialmente vigiadas por reconhecimento facial;
c) o Sudeste é a região do país com o maior número de projetos ativos, 83 no total, dos quais 35 estão em São Paulo (líder do quesito na região). Isso equivale a um total de 35.038.923 pessoas potencialmente vigiadas, sendo que 17.428.255 somente no estado paulista;
d) na sequência, vem o Centro-Oeste, com 79 projetos ativos, refletindo em 5.332.665 pessoas potencialmente vigiadas. Goiás apresenta uma relevância, inclusive em nível nacional, com a incrível marca de 66 projetos ativos, sendo também na região o líder em pessoas potencialmente vigiadas: 3.077.321;

[11] Para informações detalhadas sobre a metodologia de monitoramento do Projeto Panóptico, acessar: https://docs.google.com/document/d/1CM4P68Npyr6zR2myvjo1ulqJtpdoqOuPam8TiFah7yI/edit.

[12] Dados atualizados até 06 de setembro de 2024.

e) na Região Sul o Projeto Panóptico computou 52 projetos ativos e 10.437.445 pessoas potencialmente vigiadas. Rio Grande do Sul e Paraná empatam na quantidade de projetos ativos, com 19 cada. Contudo, o estado gaúcho é o que possui mais pessoas potencialmente vigiadas, num total de 5.584.352;
f) a Região Nordeste conta com 45 projetos ativos, o que equivale a 19.078.507 pessoas potencialmente vigiadas. Pernambuco é o estado que possui mais projetos ativos, oito no total, e a Bahia é o ente que conta com mais pessoas em possibilidade de vigilância, alcançando a marca de 7.717.177 indivíduos; e
g) na Região Norte, o número de projetos ativos é de 23, o que se reflete em 6.708.531 pessoas potencialmente vigiadas, das quais 2.512.651 são do Pará (o estado com a maior marca nesse quesito na região). Amazonas lidera o número de projetos na região, com cinco.

Apesar dos esforços de levantamento realizados tanto pela mencionada revista eletrônica Consultor Jurídico quanto do metodologicamente complexo Projeto Panóptico, é de se afirmar que a ausência de dados fornecidos e ou acessíveis em um sentido de totalidade no âmbito das secretarias de segurança pública estaduais e, por que não afirmar, municipais também, contribuem para uma dificuldade de melhor compreensão do contexto nacional no que tange ao emprego de TRF na segurança pública. Isso sem mencionar que a tecnologia, como discutido, carece de regulamentação em nível nacional, ou seja, investimento público tem sido feito em sistemas que não possuem o devido amparo legal.

Alguns casos ocorridos em solo pátrio reforçam a preocupação discutida neste artigo sobre a necessidade de um perfeito casamento entre o emprego da tecnologia com os ditames éticos que permeiam a segurança pública. Em Sergipe, em abril deste ano, durante um jogo de futebol alusivo à final do campeonato estadual, um homem foi abordado na arquibancada pela polícia e conduzido até uma sala dentro do estádio onde passou por uma busca pessoal e uma espécie de interrogatório por parte dos agentes policiais. Os policiais foram motivados a realizar a abordagem após a ferramenta de reconhecimento facial empregada pela Polícia Militar no evento ter indicado que se tratava de um

foragido. Contudo, após consulta ao sistema devido, foi detectado que não se tratava da pessoa correta. Esse não foi o primeiro caso no contexto sergipano: em 2023, uma mulher foi abordada por três vezes pela polícia, durante um evento conhecido como “micareta”, após o mesmo sistema de reconhecimento facial indicá-la como procurada. Ela chegou a ser conduzida para uma viatura antes de ser liberada (DURÃES, 2024, n. p.). Diante desses equívocos no emprego da tecnologia, o governador daquele estado se manifestou suspendendo seu emprego até a padronização de protocolos. Além de esses dois cidadãos terem em comum o fato de estarem em Sergipe e terem sido alvo de falsos positivos, ambos, conforme as fontes consultadas, são negros (DURÃES, 2024, n. p.).

Também em abril deste ano (MILLAN, 2024, n. p.), um homem foi abordado pela polícia durante uma consulta em uma clínica em Bonsucesso, no Rio de Janeiro, após ter seu rosto (presente em uma fotografia de posse dos policiais) confundido com o rosto de um criminoso com mandado de prisão em aberto cadastrado no sistema de reconhecimento facial da Polícia Militar fluminense. Somente após ser conduzido a uma delegacia e ter seus dados comparados e validados é que o abordado pôde ser liberado, depois de todo o constrangimento da abordagem dentro de um consultório e a condução em viatura para uma delegacia. Novamente, um caso de falso positivo em uma pessoa negra.

Complementando nossos exemplos, Duarte *et al.* (2021, p. 7) afirmam que nos Estados Unidos, em São Francisco, um importante polo tecnológico de ponta que abriga a sede de diversas empresas de tecnologia, como *Google*, *Facebook* e *Uber*, foi proibido o uso de tecnologia de reconhecimento facial pela polícia em virtude de possíveis erros na identificação de pessoas.

Com esses exemplos e os dados apresentados acima, verifica-se que a discussão do tema, junto à sociedade, é fundamental. Por certo o caminho não passa pelos extremos de banir ou proibir o uso e nem de emprego por entes estatais sem a devida (e discutida) regulamentação.

O uso indiscriminado, sem as condicionantes legais, pode suscitar na sociedade preocupações quanto ao surgimento de um estado de vigilância, incrementando não uma sensação de segurança, mas de medo, principalmente sobre privacidade (RANKIN; MOSES; POWERS, 2024, p. 698, tradução nossa).

Por outro lado, o não emprego pode colocar autoridades, governos e sociedade em uma condição de desvantagem tecnológica junto à criminalidade e àqueles que promovem de fato a insegurança. É o que estamos discutindo aqui do ponto de vista ético, indicando que é preciso encontrar um equilíbrio entre o direito de privacidade e o direito de transparência e as ações de segurança pública com foco no benefício geral, amplo, irrestrito.

Lynch (2024, p. 12, tradução nossa) faz uma afirmação contundente ao dizer que embora

> [...] a inovação no uso da tecnologia no policiamento e na segurança seja absolutamente necessária, é improvável que essas instâncias levem em conta adequadamente as opiniões públicas e comunitárias ou tenham os requisitos de transparência e legitimidade necessários.

Essa afirmativa ganha corpo quando ações como as das secretarias estaduais de segurança pública brasileiras se materializam, no sentido de empregar a tecnologia de reconhecimento facial sem a devida regulamentação e outras daí decorrentes, como o não fornecimento de dados (LIMA *et al.*, 2024, p. 6-7; TAJRA, 2024a, n. p.; TAJRA, 2024b, n. p.).

De fato, existem desafios: orçamentários, culturais, legais. Um caminho que estes autores entendem ser plausível para superar as dificuldades previsíveis e as já experimentadas em diversas sociedades (tendo como base alguns exemplos trazidos aqui neste texto) e que pode ajudar na consolidação da temática no Brasil é o percurso ético. Como ensinam Rankin, Moses e Powers (2024, p. 699, tradução nossa), “Os direitos mais importantes na era da IA são o direito à privacidade para indivíduos e o direito à transparência quando a IA é usada em algoritmos que tomam decisões consequentes que impactam vidas e liberdade”. Reforçam o nosso sentimento Gremsl e Hödl (2022, p. 169, tradução nossa) quando dizem que “Os desafios associados às crescentes conquistas tecnológicas da transformação digital representam, portanto, um imperativo para a ação pela ética”.

Entendemos que a TRF em momento algum deve ser usada para constranger indivíduos ou tolher a liberdade de expressão, impondo condutas. Seu foco deve ser, ao mesmo tempo em que se constitui em ferramenta útil, indispensável e de segurança para agentes de segurança pública, o de mitigar os impactos negativos de seu uso, sobretudo para os membros da sociedade que são histórica e estatisticamente mais afetados, de modo que a construção

ética do emprego da tecnologia passe por orientações estruturadas “[...] no contexto de processos sociais suportados digitalmente” (GREMSL; HÖDL, 2022, p. 170, tradução nossa).

Passa ainda pelas considerações éticas a importância da capacitação de policiais e demais agentes envolvidos em todas as fases de emprego de TRF, de maneira que eventuais danos, quando e se acontecerem, sejam devidamente tratados. Além da capacitação e do treinamento constantes, outras ações que podem ajudar nesse sentido são “[...] auditoria de transparência, explicabilidade, precisão e confiabilidade na IA. E os remédios devem ser implementados em todos os estágios do desenvolvimento da IA: coleta de dados, treinamento, operação, aplicação e avaliação” (RANKIN; MOSES; POWERS, 2024, p. 695, tradução nossa).

3 CONSIDERAÇÕES FINAIS

Tecnologia e ética podem – e devem – caminhar juntas e harmoniosamente. Não que seja tarefa simples equilibrar “[...] necessidades, direitos, proteções, benefícios e danos concorrentes. Não existe justiça matemática” (RANKIN; MOSES; POWERS, 2024, p. 697, tradução nossa), mas é possível superar o preconceito e almejar a imparcialidade no emprego de tecnologias de reconhecimento facial.

Nesse sentido, este artigo buscou demonstrar, sucintamente, que a ética no emprego de tecnologias de reconhecimento facial na segurança pública é um tema complexo que requer uma abordagem cuidadosa e informada. Os dilemas éticos desse uso mostram que a tecnologia, embora potente, precisa ser usada com precaução e sempre em conformidade com os princípios que protejam os direitos e a dignidade humanos.

Importa haver também o desenvolvimento de diretrizes claras e específicas que orientem o uso dessas tecnologias, garantindo que sua aplicação não comprometa os direitos individuais nem perpetue injustiças ao mesmo tempo em que forneça segurança jurídica para os responsáveis pela aplicação da lei, uma vez que a integração de tecnologias na segurança pública, sob um aporte ético, não é apenas desejável, mas essencial para a legitimidade e efetividade das operações de segurança.

Como destaca Nakashima (2024, p. 1328), é preciso que os responsáveis pela gestão do emprego dessas tecnologias, seus operadores (tanto em níveis táticos quanto operacionais) e a sociedade enquanto fiscalizadora encontrem um equilíbrio no seu emprego tendo como contraparte o uso da inteligência humana na rotina policial a fim de que os limites e os benefícios de cada um sejam reconhecidos e usados ao máximo. A tecnologia pode e deve ser empregada como recurso fundamental para otimizar ações, acelerar processos e permitir ganhos, mas não de maneira que venha a substituir "[...] o julgamento, a criatividade, a sensibilidade e a **ética dos profissionais da segurança pública**. A inteligência humana pode complementar e aprimorar a inteligência artificial, garantindo uma atuação policial mais efetiva e humana" (NAKASHIMA, 2024, p. 1328, grifo nosso).

Enquanto "novidade" no campo da segurança pública, o uso do reconhecimento facial deve estar regulamentado pelo governo, considerando ainda ser importante a opinião pública na construção de requisitos de transparência e de legitimidade no que tange ao emprego da TRF. Iniciativas como o Projeto de Lei nº 3069/2022 não podem caminhar em sua construção distantes da apreciação das comunidades locais. Essa conjugação pode contribuir para a desconstrução dos vieses exemplificados ao longo de nossa breve discussão ao mesmo tempo em que tem o potencial de ajudar na preservação de direitos, permitindo que a sociedade e as organizações de segurança pública usufruam dos reais benefícios da tecnologia (OLIVEIRA *et al.* 2022, p. 126).

Algumas sugestões passíveis de serem aqui apresentadas, à guisa de exemplo para o caso brasileiro, seguem no sentido de que ensinam Rankin, Moses e Powers (2024, p. 701-702, tradução nossa): inicialmente, ponto crucial é confirmar que as imagens que estão sendo capturadas pelos sistemas, de maneira automática, estão sendo processadas e utilizadas nas mais diversas condições livres de viés preconceituoso. Em seguida, testes conclusivos dos sistemas e das tecnologias em contextos operacionais diversos são fundamentais. Outra questão importante apontada é garantir que haja dispositivos que regulem de maneira rigorosa a salvaguarda das imagens e das informações relacionadas e a garantia da privacidade a fim de que a atividade com emprego de TRF não se transforme em ferramenta de vigilância invasiva.

Outra iniciativa que pode ser adotada como exemplo de boas práticas e de boa governança e que as agências encarregadas de aplicação da lei podem estar aptas a observar no Brasil quando da implantação, regulamentação, auditorias e revisão de seus sistemas de reconhecimento facial são os protocolos descritos no Catálogo de Casos de Uso de Reconhecimento Facial para Aplicação da Lei, um esforço conjunto da Força-Tarefa composta pelo Instituto de Sistemas Integrados de Informação de Justiça (IJIS) e pela Associação Internacional de Chefes de Polícia, dos Estados Unidos da América (INSTITUTE, 2019). O documento define critérios objetivos balizadores da ação dos agentes e lista cinco aspectos do sistema com possíveis perguntas sobre parâmetros de uso após cada emprego e que os policiais responsáveis pela aplicação da lei podem ser questionados e devem estar preparados para responder e prestar contas (INSTITUTE, 2019, p. 6, tradução nossa):

a) Captura de Imagem: Quem capturou a imagem? Quando foi capturada? Como foi capturada? Por que foi capturada? Foi dado consentimento para capturá-la?
b) Uso da Imagem: Quem usará a imagem? Quando ela será usada? Como ela será usada? Por que ela será usada? O consentimento será dado cada vez que ela for usada?
c) Retenção de Imagem: Quem tem o direito de reter a imagem? Quando eles têm o direito de retê-la? Como ela será retida? Por quanto tempo ela será retida?
d) Precisão da imagem: Os métodos de qualidade, captura e comparação de imagens são padronizados? As imagens de amostra e de galeria são padronizadas de forma semelhante? Os erros de precisão são aleatórios ou padronizados por sexo, raça, cor da pele, aflição, escolhas de estilo, precisão da imagem, etc.? e
e) Supervisão Humana: Os examinadores treinados são os tomadores de decisão finais? Os examinadores são treinados para certos padrões? Com que frequência?

Apesar de algumas dessas perguntas poderem ser respondidas de formas diferentes de acordo com o uso específico e ou regional do reconhecimento facial e conforme o momento, a motivação e mesmo a agência

que o está empregando (INSTITUTE, 2019, p. 7, tradução nossa), a ideia caminha no sentido defendido por Gikay (2023, p. 414, tradução nossa) ao discorrer que em vez de uma completa proibição no uso dessa tecnologia por parte de autoridades policiais o mais sensato talvez seja promover ajustes à estrutura legal existente, adotando critérios de transparência capazes de promover, quando preciso, a devida responsabilização sem prejudicar os objetivos da aplicação da lei e, também, o emprego ético da tecnologia como aliada da segurança pública.

REFERÊNCIAS

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

BBW – Big Brother Watch. ***Face Off****: the lawless growth of facial recognition in UK policing*. maio 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 5 set. 2024.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. **Projeto de Lei nº 3069/2022**, de 22 de dezembro de 2022. Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências. Câmara dos Deputados, Brasília, DF, 22 dez. 2022.

BUOLAMWINI, J. *et al*. *Facial recognition technologies: a primer.* ***Algorithmic Justice League***, 2020. Disponível em: https://www.ajl.org/federal-office-call. Acesso em 1 set. 2024.

CODED Bias. Direção: Shalini Kantayya. Produção: Shalini Kantayya, Regina K. Scully. Streaming online. (Documentário). 2020. Disponível em: https://www.netflix.com/title/81328723. Acesso em: 12 ago. 2024.

DUARTE, R. *et al.* Aplicação dos sistemas biométricos de reconhecimento facial na segurança pública. ***Brazilian Journal of Forensic Sciences, Medical Law and Bioethics***, Ribeirão Preto, v. 11, n. 1, p. 1-21, 2021. Disponível em: https://www.bjfs.org/bjfs/bjfs/article/view/848. Acesso em: 1 set. 2024.

DURÃES, Uesley. Reconhecimento facial: erros expõem falta de transparência e viés racista. **UOL**, 28 abr. 2024. Cotidiano. Disponível em:

https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/04/28/reconhecimento-facial-erros-falta-de-transparencia.htm. Acesso em: 1 set. 2024.

ESPÍRITO SANTO (Estado). Polícia Militar. Comando-Geral. **Boletim Geral da Polícia Militar no 001**, de 07 de janeiro de 2021. Vitória: Comando-Geral, 2021. Disponível em: https://pm.es.gov.br/. Acesso em: 15 ago. 2024.

FILHO, Mário Sérgio Nicolau; NICOLAU, Mário Emílio. A aplicabilidade da ética na atividade policial militar no estado do Paraná. ***Brazilian Journal of Development***, Curitiba, v. 8, n. 10, pág. 70214–70227, 2022. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/53649. Acesso em: 1 set. 2024.

GIKAY, Asress Adimi. *Regulating use by law enforcement authorities of live facial recognition technology in public spaces: an incremental approach.* ***The Cambridge Law Journal***, v. 82, n. 3, p. 414-449, 2023. Disponível em: https://www.cambridge.org/core/journals/cambridge-law-journal/article/regulating-use-by-law-enforcement-authorities-of-live-facial-recognition-technology-in-public-spaces-an-incremental-approach/AC209366CAD49EA97CBB5B9FF760F20F. Acesso em: 18 ago. 2024.

GREMSL, Thomas; HÖDL, Elisabeth. *Emotional AI: Legal and ethical challenges.* ***Information Polity***, v. 27, n. 2, p. 163-174, 2022. Disponível em: https://content.iospress.com/articles/information-polity/ip211529. Acesso em: 31 ago. 2024.

IBGE. **Censo Brasileiro de 2022:** Cidades, Espírito Santo, Panorama. Rio de Janeiro: IBGE, 2022. Disponível em: https://cidades.ibge.gov.br/brasil/es/panorama. Acesso em: 9 set. 2024.

INSTITUTE For Justice Information Sharing (IJIS). International Association Of Chiefs Of Police. ***Facial Recognition Use Case Catalog***. Ashburn, VA: IJIS; Alexandria, VA: IACP, 2019. Disponível em: https://www.theiacp.org/resources/document/law-enforcement-facial-recognition-use-case-catalog. Acesso em: 14 ago. 2024.

LIMA, T. *et al*. **Vigilância por lentes opacas**: mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil. Rio de Janeiro: CESeC, 2024. Disponível em: https://lapin.org.br/2024/10/04/vigilancia-por-lentes-opacas/. Acesso em: 05 out. 2024.

MARTINS, Laura. LGPD e reconhecimento facial: o lado mais polêmico da proteção de dados. **IT Forum**, 26 jan. 2023. Negócios. Disponível em: https://itforum.com.br/noticias/reconhecimento-facial-polemicas-permeiam-a-protecao-de-dados/. Acesso em: 12 ago. 2024.

LYNCH, Nessa. *Facial recognition technology in policing and security - case studies in regulation.* ***Laws***, v. 13, n. 3. p. 1-14, 2024. Disponível em: https://doi.org/10.3390/laws13030035. Acesso em: 27 ago. 2024.

MARTINS, H.; VALENTE, J. Datificação da economia e impactos nos mercados das comunicações digitais: uma análise do *Google* e do Grupo Globo. **Revista Eletrônica Internacional de Economia Política da Informação, da Comunicação e da Cultura**, v. 21, n. 3, p. 85-100, 2019. Disponível em: http://hdl.handle.net/20.500.11959/brapci/155437. Acesso em: 1 set. 2024.

MILLAN, Samantha. Morador do Alemão é abordado por policiais em Bonsucesso devido a erro de reconhecimento facial. **Voz das Comunidades,** 19 abr. 2024. Disponível em: https://vozdascomunidades.com.br/casos-de-policia/morador-do-alemao-e-abordado-por-policiais-em-bonsucesso-devido-a-erro-de-reconhecimento-facial/. Acesso em: 1 set. 2024.

NAKASHIMA, Maurício. Desvendando o potencial e os desafios da inteligência artificial na Polícia Militar do Paraná: estratégias para predição e prevenção de crimes. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v.10. n. 1, p. 1321-1336, jan. 2024.

OLIVEIRA, L. V. *et al.* Aspectos ético-jurídicos e tecnicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, Curitiba, v. 18, n. 50, p.114-135, jan./mar. 2022. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/12968. Acesso em: 16 ago. 2024.

PANÓPTICO. **Monitor de novas tecnologias na segurança pública do brasil**. 2024. Disponível em: https://www.opanoptico.com.br/. Acesso em: 1 set. 2024.

RANKIN, S. M. G.; MOSES, M.; POWERS, K. L. *Automated stategraft: electronic enforcement technology and the economic predation of black communities*. ***Wisconsin Law Review,*** Wisconsin, v. 2024, n. 2, p. 665-706, 2024. Disponível em: https://repository.law.wisc.edu/s/uwlaw/ark:/86871/w11679830. Acesso em: 20 ago. 2024.

SANTAELLA, Lucia; KAUFMAN, Dora. Os dados estão nos engolindo? **Civitas: revista de Ciências Sociais**, Porto Alegre, v. 21, n. 2, p. 214–223, 2021. Disponível em: https://revistaseletronicas.pucrs.br/civitas/article/view/39640. Acesso em: 2 set. 2024.

SANTOS, L. R.; PRADO, V. J.; RODRIGUEZ, V. B. C. Os reflexos de uma abolição mal-acabada no Brasil: da coroa ao algoritmo. **Revista de Direito, Governança e Novas Tecnologias**, v. 9, n. 1, p. 74-91, jan./jul. 2023. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/9684. Acesso em: 29 ago. 2024.

SARTORI, Landa Carretero Nunes Marques. **A tecnologia usada como vantagem contra a criminalidade**: uma análise da evolução tecnológica das

forças de segurança, com um recorte para a Guarda Municipal de Vila Velha. 2024.107 f. Dissertação (Mestrado em Segurança Pública) – Programa de Pós-graduação em Segurança Pública, Universidade Vila Velha, Vila Velha, 2024.

SHUKLA, Harsh; PANDEY, Meenu. *Human Suspicious Activity Recognition.* ***International Innovative Research Journal of Engineering and Technology***, Índia, v. 5, n. 4, p. 14-17, jun. 2022. Disponível em: https://iirjet.org/index.php/home/article/view/72. Acesso em: 3 set. 2024.

SHUKRI, Ahmad Asnawi Ahmad; FADZIL, Lokman Mohd. *Evil and fear detection using facial recognition algorithms for crime prevention - a survey.* ***SSRG International Journal of Electrical and Electronics Engineering***, Malásia, v. 11, n. 5, p. 85-101, maio 2024. Disponível em: https://www.researchgate.net/publication/381348495_Evil_and_Fear_Detection_Using_Facial_Recognition_Algorithms_for_Crime_Prevention_-_A_Survey. Acesso em: 28 ago. 2024.

TAJRA, Alex. Anais da vigilância - Veja como cada estado brasileiro utiliza o reconhecimento facial para fins policiais. **Consultor Jurídico**, 17 maio 2024a. Criminal. Disponível em: https://www.conjur.com.br/2024-mai-17/veja-como-cada-estado-usa-o-reconhecimento-facial-para-fins-policiais/. Acesso em: 19 ago. 2024.

TAJRA, Alex. Vigiar e punir - Ainda sem regulação, estados prendem centenas de pessoas utilizando reconhecimento facial. **Consultor Jurídico**, 17 maio 2024b. Criminal. Disponível em: https://www.conjur.com.br/2024-mai-17/sem-regulacao-estados-prendem-centenas-utilizando-reconhecimento-facial/. Acesso em: 19 ago. 2024.

AGRADECIMENTOS

Ambos os autores agradecem à FAPES pelo fomento e o amparo à pesquisa e à inovação no Espírito Santo.