1 INTRODUÇÃO

O avanço das tecnologias de reconhecimento facial (RF) e sua aplicação na persecução penal têm suscitado importantes debates sobre privacidade, direitos humanos e eficiência na segurança pública. Especificamente, este trabalho aborda a problemática jurídica do uso de RF na persecução penal e os potenciais riscos de violações de direitos fundamentais decorrentes de erros de identificação e vieses algorítmicos. A questão de pesquisa que norteia este estudo é: como a aplicação de tecnologias de reconhecimento facial na segurança pública pode impactar a proteção de direitos fundamentais, considerando os vieses e erros de acurácia dos algoritmos?

2 OBJETIVOS

O objetivo geral é analisar criticamente o impacto do reconhecimento facial na segurança pública e na persecução penal, verificando suas implicações legais e éticas. Os objetivos específicos incluem: (i) examinar os conceitos de vigilância massiva e segurança pública no contexto do reconhecimento facial; (ii) investigar os problemas de acurácia e os vieses demográficos dos algoritmos de RF; (iii) discutir as implicações legais e éticas do uso de RF na persecução penal; e (iv) propor diretrizes para a regulamentação do uso de tecnologias de reconhecimento facial no âmbito jurídico.

3 METODOLOGIA

A pesquisa será de natureza aplicada, com o objetivo de produzir conhecimento prático sobre as implicações do uso de tecnologias de reconhecimento facial (RF) na segurança pública e seus impactos legais e éticos. Utilizando o método hipotético-dedutivo, a pesquisa formulará hipóteses com base na revisão da literatura e evidências preliminares, que serão testadas para avaliar o comprometimento da privacidade, os vieses contra minorias e o potencial de abuso de poder. Ademais, a pesquisa será exploratória, investigando e tornando explícitos os problemas relacionados à vigilância massiva e falhas nos algoritmos de RF, e explicativa, buscando identificar as causas dos fenômenos observados.

Os procedimentos técnicos envolverão uma combinação de revisão bibliográfica e documental, analisando literatura científica, relatórios e documentos oficiais sobre a implementação de RF. Estudos de caso serão conduzidos para análise aprofundada de situações

específicas onde RF foi utilizada. A abordagem será mista, qualitativa e quantitativa, utilizando análise de discursos e documentos, observação participante e coleta de dados estatísticos sobre a precisão e vieses dos algoritmos de RF. Essa metodologia permitirá uma análise abrangente dos impactos das tecnologias de reconhecimento facial, fornecendo uma base sólida para recomendações políticas e éticas.

4 DESENVOLVIMENTO

A utilização de tecnologias de reconhecimento facial (RF) para a coleta e processamento de dados pessoais tem proporcionado um nível sem precedentes de vigilância, particularmente por parte das instituições governamentais. O RF, justificado pela necessidade de manutenção da segurança pública, é utilizado para monitorar espaços públicos, permitindo o gerenciamento de grandes volumes de dados biométricos. Segundo Schneider e Miranda (2020), essa capacidade de armazenamento e análise de dados viabiliza o monitoramento de populações inteiras, criando uma estrutura de vigilância massiva que pode comprometer liberdades individuais.

A implementação de sistemas de RF em locais públicos, como aeroportos, estações de metrô e eventos de grande escala, é frequentemente apresentada como uma medida essencial para a prevenção de crimes e ameaças à segurança pública. No entanto, essa abordagem levanta preocupações significativas quanto à privacidade e aos direitos civis. Conforme argumentado por Lyon (2018), a expansão do uso de RF configura um novo paradigma de vigilância, onde a coleta contínua e indiscriminada de dados biométricos pode resultar em uma sociedade onde todos os movimentos dos cidadãos são rastreados e registrados.

A centralização e análise de dados biométricos criam uma base de informações que pode ser utilizada de maneiras que extrapolam os objetivos de segurança inicialmente propostos. De acordo com Garvie, Bedoya e Frankle (2016), a coleta de dados faciais, sem o devido consentimento dos indivíduos, representa uma invasão significativa à privacidade. Além disso, a utilização desses dados para finalidades não especificadas ou posteriormente definidas amplia os riscos de abuso e vigilância indevida.

Os problemas associados à vigilância massiva por RF são exacerbados pela presença de vieses nos algoritmos utilizados. Um estudo realizado pelo National Institute of Standards and Technology (NIST, 2019) aponta que os algoritmos de RF apresentam variações na acurácia dependendo do grupo demográfico do sujeito. Segundo o NIST (2019), as taxas de

falsos positivos são entre 2 e 5 vezes maiores em mulheres do que em homens, variando conforme o algoritmo e a origem geográfica dos dados. Este aumento nos falsos positivos é mais pronunciado entre indivíduos de etnias sub-representadas, o que agrava ainda mais a discriminação e o potencial para injustiças.

Buolamwini e Gebru (2018) destacam que algoritmos comerciais de RF falham em classificar corretamente mulheres negras em até 34,7%, contrastando drasticamente com uma taxa de erro de no máximo 0,8% para homens brancos. Essas disparidades são emblemáticas da tendência dos algoritmos de RF em privilegiar características faciais mais similares aos dados de treinamento, que frequentemente são dominados por amostras de indivíduos brancos e masculinos.

Essa sub-representação de grupos étnicos minoritários e mulheres nos conjuntos de dados utilizados para treinar algoritmos de RF é um fator crítico na geração desses vieses. Em suma, conforme ressaltado por diversos estudos, incluindo aqueles realizados pelo National Institute of Standards and Technology (NIST), a falta de diversidade nos dados de treinamento contribui diretamente para taxas desproporcionais de erros de identificação em indivíduos de diferentes origens étnicas e de gênero (NIST, 2019).

No Reino Unido, por exemplo, um estudo conduzido pela Big Brother Watch (2018) revelou que 95% das correspondências feitas por RF resultaram em identificações incorretas. No Brasil, a situação não é diferente. Casos como o da mulher inocente confundida com uma criminosa no Rio de Janeiro destacam os riscos associados ao uso impreciso de RF pelas autoridades. Conforme relatado pelo jornal Correio (2019), a mulher foi detida injustamente devido a um erro no sistema de reconhecimento facial, evidenciando a fragilidade e os perigos de confiar cegamente em tecnologias que ainda não atingiram um nível de precisão aceitável.

Além disso, o contexto social e histórico no qual esses algoritmos são desenvolvidos e implementados também influencia significativamente sua eficácia e imparcialidade. Garvie, Bedoya e Frankle (2016) observam que sistemas automatizados de RF tendem a refletir e amplificar preconceitos existentes na sociedade, reproduzindo assimetrias de poder e marginalização. Assim, a questão dos vieses nos algoritmos de RF não se limita apenas à precisão técnica, mas levanta preocupações éticas e legais sobre o uso justo e equitativo dessa tecnologia.

Essa desigualdade no desempenho dos algoritmos de RF pode agravar discriminações já existentes na sociedade, especialmente quando tais tecnologias são empregadas em operações de segurança pública. Schneider e Miranda (2020) alertam que a vigilância massiva pode levar à subtração de liberdades individuais, especialmente para grupos marginalizados que já

enfrentam discriminação sistêmica. Nesse contexto, a vigilância por RF não apenas amplia o alcance do monitoramento estatal, mas também perpetua desigualdades sociais e raciais.

Portanto, a mitigação desses vieses requer não apenas a expansão e diversificação dos conjuntos de dados utilizados para treinamento, mas também a implementação de políticas regulatórias e práticas éticas que garantam a transparência, responsabilidade e justiça no desenvolvimento e uso de tecnologias de RF.

Adicionalmente, a falta de transparência e supervisão na implementação de tecnologias de RF em espaços públicos levanta questões sobre a responsabilidade e a governança dessas práticas. Organizações como o ICO (Information Commissioner's Office) e BBW têm alertado para os riscos associados ao uso indiscriminado dessa tecnologia, que pode facilitar a vigilância em larga escala e comprometer os direitos individuais à informação e à privacidade (ICO, 2019; BBW, 2018).

Em contextos como o da China, o emprego do RF no Social Credit System oferece um exemplo contundente de como essa tecnologia pode ser empregada para impor um controle social rigoroso sobre a população (ICO, 2019; BBW, 2018). Este sistema não só monitora o comportamento dos cidadãos, mas também atribui pontuações baseadas em critérios variados, influenciando significativamente a vida cotidiana e as oportunidades das pessoas.

Laconicamente, a adoção de tecnologias de reconhecimento facial para a vigilância massiva traz implicações profundas para a segurança pública e os direitos individuais. A capacidade de monitorar continuamente os cidadãos, combinada com os vieses intrínsecos dos algoritmos de RF, exige um debate robusto e a implementação de regulamentações que protejam os direitos civis.

Destarte, a discussão sobre as implicações éticas e legais do RF é essencial para mitigar os potenciais impactos negativos sobre a privacidade, a liberdade e a dignidade das pessoas, especialmente em um contexto de avanço tecnológico acelerado e uso crescente de dados pessoais para fins diversos, incluindo a segurança pública e o controle social (ICO, 2019; BBW, 2018).

5 CONCLUSÃO

A aplicação de tecnologias de reconhecimento facial (RF) na segurança pública representa uma inovação significativa no monitoramento e prevenção de crimes, mas também levanta preocupações substanciais sobre a proteção de direitos fundamentais. A utilização de

RF permite um nível de vigilância massiva que, se não for adequadamente regulado, pode comprometer liberdades individuais, como o direito à privacidade e à liberdade de ir e vir.

Os estudos demonstram que os algoritmos de RF são propensos a vieses, especialmente em relação a grupos demográficos sub-representados, como mulheres e pessoas negras, que enfrentam taxas de erro significativamente mais altas. Essa falta de precisão pode levar a identificações incorretas, resultando em consequências graves, como detenções injustas e discriminação sistemática. A dependência de RF em contextos de segurança pública sem a devida supervisão e regulação aumenta o risco de abusos de poder e vigilância indevida, transformando uma ferramenta potencialmente útil em um instrumento de controle social.

A resposta para a interrogante da pesquisa, sobre como a aplicação de tecnologias de RF na segurança pública pode impactar a proteção de direitos fundamentais, considerando os vieses e erros de acurácia dos algoritmos, é clara: a tecnologia, sem regulamentação adequada, pode violar direitos fundamentais. A vigilância constante e a falta de transparência associadas ao uso de RF exacerbam os riscos de discriminação e erros de identificação. Para mitigar esses impactos, é imperativo que haja uma legislação robusta que assegure o uso responsável e ético dessas tecnologias, com salvaguardas que garantam a proporcionalidade, a necessidade e a transparência. Somente assim será possível equilibrar a segurança pública com a proteção dos direitos individuais, promovendo um uso justo e equitativo do reconhecimento facial.

REFERÊNCIAS

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: 26 jun. 2024.

BIGO, D. Security, Exception, Ban and Surveillance. *In*: LYON, D. **Theorizing Surveillance.** The Panopticon and beyond. Reino Unido: Wilan, 2006, p. 46-68.

BUOLAMWINI, J.; GEBRU; T. **Gender Shades**: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research, v. 81, p. 1-15, 2018.

CORREIO. **Inocente é confundida com criminosa por câmera de reconhecimento facial no Rio**. Correio, Da redação, 11 jul. 2019. Disponível em: https://www.correio24horas.com.br/brasil/inocente-e-confundida-com-criminosa-por-camera-de-reconhecimento-facial-no-rio-0719. Acesso em: 26 jun. 2024.

GARVIE, C.; BEDOYA, A.; FRANKLE, J. The Perpetual Line-up. **Unregulated police face recognition in America**. Center on Privacy & Technology at Georgetown Law, 18 out. 2016.

Disponível em: https:// www.perpetuallineup.org/findings/racial-bias#footnote223_i485k1t. Acesso em: 26 jun. 2024.

ICO – Information Comissioner's Office. **ICO investigation into how the police use facial recognition technology in public places**. 31 out. 2019. Disponível em: https://ico.org.uk/media/about-the-ico/ documents/2616185/live-frt-law-enforcement-report-20191031.pdf. Acesso em: 26 jun. 2024.

NIST - National Institute of Standards and Technology. **Face Recognition Vendor Test (FRVT) Part 3**: Demographic Effects. 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. Acesso em: 26 jun. 2024.

SCHNEIDER, C. B.; MIRANDA, P. F. M. **Vigilância Digital como instrumento de promoção da segurança pública**. Publicatio UEPG – Ciências Sociais Aplicadas, Ponta Grossa/RS, v. 28, p. 1-14, 2020.