Universidade Cruzeiro do Sul
Curso de Ciência da Computação

Vinicius de Brito e Silva

Análise de Viés Tecnológico no Reconhecimento Facial

São Paulo

2025

Resumo

Este relatório analisa o viés tecnológico presente em sistemas de reconhecimento facial aplicados à segurança pública no Brasil. A partir de um estudo de caso noticiado pelo portal G1 em 2023, que revelou prisão indevida causada por erro de identificação, a pesquisa utilizou um framework estruturado com nove tópicos de análise de viés e cinco abordagens éticas. Constatou-se a ocorrência de vieses de representação, agregação e avaliação, relacionados ao uso de bases de dados pouco representativas e métricas de eficácia distorcidas. O estudo aponta para riscos éticos, jurídicos e sociais da tecnologia, destacando a necessidade de conformidade com legislações como a LGPD e de práticas de desenvolvimento ético em inteligência artificial.

Palavras-chave: Reconhecimento facial. Viés algorítmico. Segurança pública. Ética digital. Inteligência Artificial.

1. Introdução

Apresenta-se a análise de sistemas de reconhecimento facial aplicados na segurança pública, com foco na detecção de vieses tecnológicos e seus impactos sociais.

2. Metodologia

Utilizou-se um modelo estruturado com nove tópicos de análise de viés e cinco abordagens éticas (utilitarista, baseada em direitos, justiça, bem comum e virtude).

3. Estudo de Caso

Baseado em notícia do portal G1 (Alencar, 2023), que relata prisão injusta de um inocente em Salvador, vinculada ao uso de reconhecimento facial. O caso exemplifica falhas técnicas e vieses sociais amplificados pela tecnologia.

4. Análise de Viés

Os tópicos a seguir, formam um modelo estruturado de análise de viés e justiça. Assim foram levantadas diversas informações para a análise.

1. Grupos favorecidos

O uso de reconhecimento facial na segurança pública visa favorecer a população com melhoria da segurança e da agilidade no trabalho da polícia.

2. Representatividade dos dados

O uso de catálogos informais para a base de dados dos sistemas de vigilâncias, revelou risco de baixa representatividade dos dados.

3. Impacto real

Houve aumento das detenções e prisões com o apoio da tecnologia, mas incluiu pessoas inocentes durante as falhas, as quais foram mais discrepantes em grupos sub representados.

4. Diversidade nos dados de treinamento

Dados de treinamento pouco diversos.

5. Teste com grupos diferentes antes do lançamento

A inclusão de grupos diferentes em testes, auxiliaria na identificação de falsos positivos. No entanto, não houve informações nesse sentido.

6. Documentação de decisões e critérios

Poucos detalhes do sistema foram disponibilizados. Apesar disso, critérios foram observados, como "estilo de cabelo" e "estilo inferior".

7. Monitoramento dos resultados por grupos demográficos

O monitoramento teve como resultado apenas o número de prisões.

8. Feedback de usuários diversos

Ocorreram manifestações contrárias quanto às inconsistências no funcionamento, a falta de transparência pelas autoridades, ao tratamento de dados e vieses tecnológicos.

9. Ajustes no sistema quando necessário

O sistema continua recebendo investimentos e se desenvolve constantemente.

5. Abordagem Ética

A análise ética foi feita abordou os impactos das decisões éticas tomadas sob cinco abordagens.

I - Abordagem utilitarista:

O reconhecimento facial é uma inovação na segurança a pública. Além de grande quantidade de dados representativos, a implementação de princípios no desenvolvimento de Inteligência Artificial como a ética aplicada são maneiras de maior eficácia para combater os vieses algorítmicos.

II -Abordagem baseada em direitos:

Há a necessidade de adequação às novas leis e regulamentos para a garantia dos direitos digitais na sociedade, como privacidade digital, acesso à informação e proteção contra discriminação digital já previstos em leis, a exemplo da Lei 12.965/2014 do Marco Civil da Internet brasileiro.

III -Abordagem justa

Os vieses e resultados apresentados são indicações de que o sistema é desproporcional em decisões e julgamentos.

IV - Abordagem do bem comum

O reconhecimento facial permite diversos benefícios. Mas para garantir seu pleno desenvolvimento é necessário combater seus impactos negativos na sociedade.

V - Abordagem da Virtude

É fundamental uma postura empática e responsável pelos profissionais, organizações públicas e privadas, assim como a conformidade com o código de ética e diretrizes para atuação na área tecnológica pela Sociedade Brasileira de Computação (SBC, 2024).

6. Classificação de Viés

Foram identificados:

- **Viés de representação:** bases de dados pouco diversas.
- **Viés de agregação:** associação indevida de padrões.
- **Viés de avaliação:** métricas enviesadas (ex.: número de prisões).

7. Discussão Ética

A análise revelou incompatibilidades com princípios da Lei Geral de Proteção de Dados - LGPD - e do Marco Civil da Internet. Aponta-se a necessidade de transparência, auditoria independente e monitoramento contínuo.

8. Conclusão

A tecnologia apresenta potencial para segurança, mas riscos sociais e éticos exigem desenvolvimento responsável, adoção de equipes diversas, testes amplos e aplicação de princípios de *Ethical AI by Design*.

Referências

ALENCAR, Itana. Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por "racismo algorítmico". G1, 01 set. 2023. Disponível em: https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml. Acesso em: 08 set. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Código de Ética da SBC. 2024.