Análise Ética de Sistemas de Reconhecimento Facial sob a Perspectiva de Responsabilidade e Governança

1. Introdução

Sorria! Seu rosto pode estar sendo não só filmado, mas também classificado, comparado e identificado — muitas vezes sem o seu conhecimento. Esse é o cenário apontado em pesquisa da Defensoria Pública da União (DPU) em parceria com o Centro de Estudos de Segurança e Cidadania (CESeC), instituição acadêmica vinculada à Universidade Candido Mendes, no Rio de Janeiro.

Segundo o relatório *Mapeando a Vigilância Biométrica*, divulgado em 7 de fevereiro de 2024, após a Copa do Mundo de 2014 o Brasil se tornou um vasto campo de vigilância digital, onde as Tecnologias de Reconhecimento Facial (TRFs) encontraram terreno fértil para se expandir. Isso ocorreu em parte pela promessa de facilitar a identificação de criminosos e a localização de pessoas desaparecidas.

No entanto, seu uso em espaços públicos tem gerado debates intensos, especialmente sobre privacidade, discriminação e controle social. A ausência de diretrizes claras e de mecanismos de governança levanta sérias questões éticas sobre quem é responsável pelos erros e abusos decorrentes dessas tecnologias.

Este trabalho utiliza o framework de análise ética em Inteligência Artificial, com foco no eixo de **Responsabilidade e Governança**, para refletir sobre como esses sistemas devem ser avaliados e regulados.

---

2. Aplicação do Framework

Viés e Justiça

Estudos já mostraram que sistemas de reconhecimento facial apresentam maior taxa de erro para pessoas negras, mulheres e latinas. Esses sistemas não são neutros, especialmente quando utilizados pela polícia. Como afirmou um especialista, “se você tiver um sistema treinado majoritariamente com rostos de universitários americanos, você terá um sistema muito eficiente para identificar homens brancos, mas falho para reconhecer minorias étnicas”. Isso gera uma vulnerabilidade desproporcional e produz injustiças sociais e legais.

Transparência e Explicabilidade

Muitos desses sistemas funcionam como verdadeiras *caixas-pretas*. Os modelos de aprendizado profundo utilizados no reconhecimento facial são altamente complexos e exigem conhecimentos técnicos avançados para serem compreendidos. Essa complexidade dificulta o acesso dos órgãos reguladores às suas diretrizes internas e torna auditorias independentes mais desafiadoras. Como consequência, há pouca transparência sobre como as decisões são tomadas, o que compromete a responsabilização em casos de falhas.

Impacto Social e Direitos

O uso sem regulamentação pode violar a privacidade, em conflito com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), em vigor no Brasil desde 2020. Além disso,

reduz liberdades individuais e pode ser aplicado de forma abusiva por governos ou empresas, afetando diretamente direitos fundamentais da sociedade.

Responsabilidade e Governança

Aqui está o eixo central: quem deve ser responsabilizado quando a tecnologia falha ou é mal utilizada?

- **Empresas desenvolvedoras** devem ser obrigadas a seguir princípios de *Ethical AI by Design*.
- **Governos** precisam criar regulações que limitem o uso indevido e garantam auditorias periódicas.
- **Instituições que aplicam a tecnologia** devem responder legalmente em casos de abuso, assegurando a proteção dos cidadãos.
- É fundamental também estimular as empresas desenvolvedoras de software de reconhecimento facial a treinar sistemas com bases de dados etnicamente diversas, reduzindo vieses.

---

3. Posição Final

Entendemos que o uso de reconhecimento facial **não deve ser banido totalmente**, mas precisa ser **rigorosamente regulamentado**. A ausência de governança clara aumenta riscos de violações de direitos e de injustiças sociais.

---

4. Recomendações Práticas

1. **Regulamentação obrigatória:** criação de leis específicas que definam limites de uso e prevejam responsabilização legal.
2. **Comitês de Ética e Auditoria:** sistemas só devem ser implementados após validação por órgãos independentes.
3. **Transparência pública:** divulgação periódica de relatórios sobre viés, taxas de erro e impacto social.

---

5. Conclusão

A governança responsável da Inteligência Artificial é essencial para garantir que avanços tecnológicos estejam alinhados com valores éticos e direitos fundamentais. Portanto, o reconhecimento facial, se aplicado sem responsabilidade e governança, representa mais riscos do que benefícios. Apenas com regulamentação robusta será possível equilibrar segurança pública e a proteção dos direitos dos cidadãos.