Análise Ética – Reconhecimento Facial em Espaços Públicos 25 August 2025

Resumo executivo

Este relatório analisa criticamente o uso de sistemas de reconhecimento facial em espaços públicos — com ênfase em casos de coleta massiva de imagens (ex.: Clearview AI) — aplicando um framework ético baseado em princípios internacionais (transparência, justiça, responsabilidade). O objetivo é apresentar uma posição profissional fundamentada e recomendações práticas para desenvolvedores, gestores e legisladores.

1. Escolha do caso

Caso selecionado: uso comercial e por órgãos públicos de bases de dados faciais construídas por 'scraping' de imagens públicas, com foco no caso Clearview AI e em práticas de vigilância sem consentimento explícito. Observou-se intensa polêmica pública, ações judiciais e discussões sobre vieses e privacidade.

2. Método/Framework aplicado

Framework usado: extraímos requisitos de frameworks reconhecidos (EU HLEG – 'Trustworthy AI', UNESCO Recommendation on AI Ethics, OECD AI Principles) e aplicamos um checklist prático: (1) Identificação de vieses (dados e algoritmo), (2) Transparência e explicabilidade, (3) Impacto social e direitos (privacidade/LGPD), (4) Responsabilidade e governança (auditoria, documentação e mitigação).

3. Análise detalhada

3.1 Viés e Justiça

Evidências acadêmicas e avaliações governamentais mostram diferenças sistemáticas de desempenho: sistemas demonstraram maiores taxas de erro para pessoas de pele mais escura e, em particular, mulheres de pele mais escura — resultado de datasets desbalanceados e de processos de etiquetagem. Além disso, o uso em policiamento e vigilância tende a afetar desproporcionalmente comunidades racializadas e grupos vulneráveis.

3.2 Transparência e Explicabilidade

Muitos fornecedores não divulgam os dados usados para treinar os modelos, nem métricas disaggregadas por raça/gênero — tornando decisões difíceis de explicar. Soluções de 'caixa preta' reduzem a responsabilização e dificultam contestação por pessoas que foram indevidamente identificadas.

3.3 Impacto social e direitos

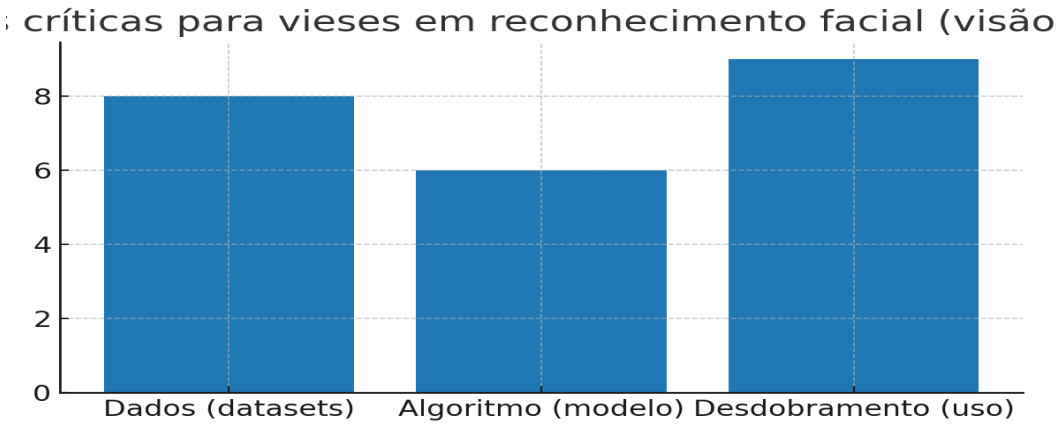
Impactos observados incluem violações de privacidade (coleta sem consentimento), risco de detenção ou abordagem indevida devido a falsos positivos, e efeitos de 'chilling' em liberdades civis (pessoas evitam manifestações ou espaços públicos). No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabelece princípios de tratamento de dados pessoais que são aplicáveis quando imagens faciais são coletadas e processadas.

3.4 Responsabilidade e Governança

Equipes poderiam ter adotado medidas de 'Ethical AI by Design' como: avaliações de impacto antes do uso, documentação detalhada (model cards/datasheets), testes públicos de desempenho por subgrupo, políticas de consentimento e retenção, além de auditorias independentes e mecanismos claros de

reparação quando ocorrem erros.

Visualização: áreas críticas



4. Posicionamento profissional

Posição: Proponho uma abordagem mista — **proibição parcial** do uso de reconhecimento facial para identificação remota em espaços públicos sem mandato judicial e sem consentimento, com **exceções restritas** (ex.: investigação de crimes graves mediante ordem judicial e supervisão clara). Para usos comerciais e administrativos, recomendo regulação rigorosa e requisitos obrigatórios de transparência, auditoria e mitigação de viés.

5. Recomendações práticas (2–3 ações concretas)

1) **Avaliação de Impacto Algorítmico (AIA) obrigatória** antes do uso em produção: incluir métricas de desempenho por subgrupo, plano de mitigação e relatório público resumido.

2) **Transparência e documentação**: publicação de model cards, descrição de datasets (datasheets), políticas de retenção e fluxos de consentimento alinhados à LGPD.

3) **Auditoria independente e governança**: auditorias periódicas por terceiros, revisão humana para decisões sensíveis, e canais claros de reparação para vítimas de falsos positivos.

6. Plano de implementação (cronograma sugerido — 6 meses)

Mês 1–2: Auditoria inicial e AIA; testes disaggregados com benchmarks públicos (ex.: NIST FRVT). **Mês 3–4:** Mitigação técnica (re-balanceamento, fairness constraints, thresholds) e criação de documentação pública. **Mês 5–6:** Auditoria externa, políticas de governança e treinamento de operadores/human-in-the-loop.

Referências e fontes selecionadas (resumo)

Buolamwini, J.; Gebru, T. Gender Shades (2018) — estudo sobre disparidades em reconhecimento facial.

NIST FRVT — Face Recognition Vendor Test (Demographic Effects; relatórios 2019 e 2022) — avaliações de performance por subgrupos.

ACLU / ações contra Clearview AI — litígios e preocupações sobre scraping e privacidade.

Lei nº 13.709/2018 — LGPD (Brasil) — disposições sobre tratamento de dados pessoais.