Dilemas Éticos em Inteligência Artificial

Caso Escolhido: Reconhecimento Facial

Introdução

O reconhecimento facial é uma tecnologia de Inteligência Artificial (IA) aplicada em diferentes contextos, como segurança pública, autenticação digital e redes sociais. Apesar de sua utilidade, o tema suscita importantes dilemas éticos relacionados a viés algorítmico, privacidade, vigilância em massa e riscos de discriminação. Este trabalho tem como objetivo analisar tais dilemas a partir de um estudo de caso real e discutir os desafios de governança e regulamentação dessa tecnologia.

1. Viés e Justiça

Viés nos dados: Os bancos de imagens utilizados para treinar os modelos, em sua maioria, são compostos por rostos de homens brancos, o que compromete o desempenho quando aplicado a minorias étnicas.

Viés do algoritmo: Quando persistem mesmo após ajustes técnicos, resultando em maior incidência de falsos positivos para determinados grupos. Assim, enquanto empresas e governos se beneficiam de maior eficiência em vigilância, os riscos recaem desproporcionalmente sobre cidadãos vulneráveis, que podem ser injustamente vigiados ou acusados.

Grupos afetados: mulheres, pessoas negras e outras.

2. Transparência e Explicabilidade

Os algoritmos de reconhecimento facial são frequentemente considerados uma “caixa preta”, pois as empresas alegam segredo industrial para não revelar detalhes técnicos. Isso dificulta que cidadãos compreendam ou contestem decisões automatizadas. Além disso, há baixo nível de transparência pública quanto às condições de uso e aos locais de implantação da tecnologia.

3. Impacto Social e Direitos

- **Mercado de trabalho:** Substituição de funções humanas de vigilância.
- **Autonomia individual:** Monitoramento sem consentimento.
- **Direitos Fundamentais:** A utilização de dados biométricos envolve sérios riscos à privacidade e à presunção de inocência. Ao serem classificados pela LGPD

como dados pessoais sensíveis, sua coleta e tratamento devem observar critérios rigorosos de necessidade, proporcionalidade e finalidade. Caso contrário, podem abrir precedentes para práticas de vigilância em massa, incompatíveis com os princípios democráticos e com a proteção das liberdades individuais.

4. Atores Envolvidos

- **Empresas de tecnologia:** desenvolvem os algoritmos e comercializam soluções.
- **Governos:** utilizam a tecnologia em políticas de segurança e monitoramento.
- **Usuários e trabalhadores:** impactados por erros de reconhecimento e possíveis violações de direitos.
- **Sociedade civil e órgãos reguladores:** fiscalizam e cobram transparência e respeito às normas legais.

5. Valores em Conflito

O uso do reconhecimento facial evidencia a tensão entre:
Segurança pública e eficiência tecnológica X **Privacidade e direitos fundamentais**.

Também se contrapõem:
Inovação e progresso econômico X **Justiça social e não-discriminação**.

6. Responsabilidade e Governança

Para reduzir riscos, equipes de desenvolvimento devem adotar práticas como:

- utilização de datasets diversos e representativos;
- realização de auditorias independentes;
- definição de limites claros de uso, sempre com consentimento informado.

Princípios de *Ethical AI by Design* recomendam justiça, não-discriminação, transparência e respeito aos direitos humanos. No âmbito regulatório, a LGPD (Brasil) protege dados biométricos, enquanto o AI Act (União Europeia) classifica o reconhecimento facial em tempo real como tecnologia de alto risco, exigindo restrições severas.

7. Estudo de Caso

Em 2021, o motorista Pa Edrissa Manjang, do Uber Eats (Reino Unido), teve sua conta suspensa devido a falhas do sistema de reconhecimento facial da Microsoft, que não reconhecia corretamente seu rosto negro. O caso mobilizou sindicatos e órgãos de direitos humanos, resultando em acordo judicial e reativação da conta. O episódio expôs como falhas algorítmicas podem comprometer o direito ao trabalho e reforçou a necessidade de auditorias independentes e regulação governamental clara.

Discussão

A análise mostra que, embora a tecnologia de reconhecimento facial não deva ser totalmente proibida, seu uso deve ser limitado a contextos legítimos e com consentimento (como autenticação bancária ou desbloqueio de dispositivos). O caso Uber Eats ilustra a gravidade de erros discriminatórios, reforçando que a responsabilidade ética e legal deve recair sobre empresas que desenvolvem e aplicam tais sistemas.

Conclusão

O reconhecimento facial representa um avanço tecnológico relevante, mas permeado por dilemas éticos significativos. Sua aplicação demanda equilíbrio entre inovação e proteção de direitos fundamentais. Regulamentações robustas, transparência, auditorias independentes e respeito à diversidade são condições essenciais para que a tecnologia seja utilizada de forma justa e democrática.

Referências

- BBC News. Uber Eats driver wins payout over 'racist' facial recognition app. 2024. Disponível em: https://www.bbc.com/news/technology-68655429.
- The Times. Uber Eats courier wins payout over 'racist' facial recognition app. 2024. Disponível em: https://www.thetimes.co.uk/article/uber-eats-courier-wins-payout-over-racist-facial-recognition-app-dzhkbn2lx.
- Biometric Update. Uber Eats settles driver’s biometric ID verification discrimination case. 2024. Disponível em: https://www.biometricupdate.com/202403/uber-eats-settles-drivers-biometric-id-verification-discrimination-case.
- LGPD – Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709, de 14 de agosto de 2018.
- União Europeia. Artificial Intelligence Act. 2021.