Relatório – Dilema Ético em IA: Reconhecimento Facial

1. Escolha do Caso

O dilema ético escolhido é o uso de sistemas de reconhecimento facial em espaços públicos e privados. Essa tecnologia vem sendo utilizada para segurança, identificação de suspeitos e até controle de acesso em empresas, mas levanta questões éticas e legais importantes.

2. Análise com o Framework Ético

Viés e Justiça

Estudos mostram que sistemas de reconhecimento facial apresentam viés de dados, já que foram treinados com maior número de imagens de pessoas brancas. O resultado é uma taxa de erro maior para mulheres e pessoas negras, que podem ser desproporcionalmente afetadas. Isso gera uma distribuição injusta dos riscos, pois certos grupos sofrem mais com falsas identificações.

Transparência e Explicabilidade

Na maioria dos casos, os sistemas funcionam como uma 'caixa-preta', sem explicação clara de como a decisão foi feita. A falta de transparência impede que os afetados compreendam ou contestem decisões erradas.

Impacto Social e Direitos

Pode comprometer o direito à privacidade, violando a LGPD no Brasil, já que envolve coleta e uso de dados biométricos. Afeta a autonomia individual, pois cidadãos podem ser constantemente monitorados sem consentimento. Pode gerar impactos sociais negativos, como vigilância em massa e criminalização de determinados grupos.

Responsabilidade e Governança

As empresas poderiam ter investido em bases de dados mais diversas e realizado auditorias de viés antes do uso. Princípios de Ethical AI by Design deveriam ter sido aplicados: justiça, transparência e respeito à privacidade. Leis como a LGPD (Brasil) e discussões sobre regulação da IA na União Europeia já tratam da necessidade de limites no uso dessa tecnologia.

3. Posicionamento

Com base na análise, entende-se que o reconhecimento facial não deve ser banido totalmente, mas precisa ser redesenhado e regulado para reduzir riscos éticos e sociais.

Recomendações práticas:

1. Exigir auditorias independentes para verificar viés nos sistemas antes da aplicação em larga escala.
2. Garantir transparência sobre como a IA funciona, permitindo contestação de decisões erradas.
3. Restringir o uso a contextos específicos (ex.: segurança em aeroportos), proibindo vigilância em

massa sem autorização legal.