
Case study 2: Facial Recognition & Policy

📌 Task Summary

A facial recognition system identifies minorities at higher error rates.
Your task:

Discuss ethical risks

Recommend policies for responsible deployment

🔷 1. Ethical Risks of Biased Facial Recognition

Facial recognition systems, especially those trained on non-diverse datasets, often misidentify racial minorities at much higher error rates. This creates serious ethical risks:

⚠️ a) Discrimination and Misidentification

Black, Indigenous, and Asian individuals are misidentified far more frequently than white individuals.

This can lead to wrongful arrests, denied access to services, or surveillance of innocent people.

⚠️ b) Violation of Privacy Rights

Individuals are often scanned and tracked without their knowledge or consent.

This undermines data protection laws, especially in countries with strong privacy regulations like the EU (GDPR).

⚠️ c) Social Marginalization

Biased systems disproportionately impact already-marginalized communities, increasing distrust in technology and public institutions.

It reinforces systemic inequalities instead of correcting them.

⚠️ d) Lack of Accountability

When facial recognition systems make mistakes, it's often unclear who is responsible—the software vendor? The agency using it? This lack of transparency leads to zero consequences.

🔷 2. Policy Recommendations for Responsible Deployment

To reduce these ethical risks, the following policies must be enforced before facial recognition is used:

✅ a) Mandatory Bias Audits

All facial recognition models must be tested for accuracy across race, gender, and age groups.

Independent fairness audits should be done before deployment and routinely after.

✅ b) Transparency & Consent

Notify individuals when facial recognition is being used.

Give them the right to opt-out unless it's legally mandated (e.g., border security).

✅ c) Human Oversight

Facial recognition decisions should never be fully automated in high-stakes situations (e.g., law enforcement).

A human must always verify matches before action is taken.

✅ d) Strict Use-Case Limitations

Ban or strictly regulate use in public surveillance unless approved by a regulatory body.

Facial recognition should only be used when:

There’s legal authority

Alternatives are inadequate

Safeguards are in place

✅ e) Explainability & Accountability Framework

Agencies using the technology must:

Publish the model’s performance by demographic group

Define who is legally and ethically accountable for errors