CASE 1: Discriminatory Algorithmic Bias in Autonomous Vehicles

Problem Statement

FutureDrive AI Pvt. Ltd. is accused of incorporating a biased decision-making algorithm in its autonomous cars, which allegedly prioritized certain vehicle types in traffic scenarios, leading to an accident that disadvantaged a smaller vehicle on a busy Bengaluru road.

A public interest litigation has been filed under the *Information Technology Act, 2000*, the *Consumer Protection Act, 2019*, and constitutional provisions on equality under *Article 14* of the *Indian Constitution*.

Legal Issues

1. Whether algorithmic bias constitutes discrimination under Indian law.
2. Whether the manufacturer can be held liable for the outcomes of biased AI algorithms.
3. Whether regulatory oversight of AI algorithms should be strengthened.

Annexures Used

Annexure E1: Technical audit report revealing algorithmic patterns.

Annexure E2: Traffic camera footage of the incident.

Annexure E3: Company's internal documents on algorithm development.

Annexure E4: Expert testimony on AI bias from a leading tech institute.

Annexure E5: Legal complaint filed in public interest.

Victim Testimony

Mr. Deepak Iyer, the driver of the smaller vehicle, claims that the autonomous car swerved unexpectedly, causing a collision that left him with spinal injuries. He argues that the AI system's preferential treatment endangered his safety.

CASE 2: Fraudulent Identity Creation Using Blockchain-Based Voting Platform

Problem Statement:

VoteSecure Pvt. Ltd. launched a blockchain-based e-voting system for corporate elections. An investigation revealed that multiple fraudulent identities were created on the platform, leading to vote manipulation and election tampering.

The affected party has filed a complaint under the *Companies Act, 2013*, *Information Technology Act, 2000*, and *Indian Penal Code, 1860* (for forgery and fraud).

Legal Issues

1. Whether blockchain-based voting systems are secure under Indian corporate governance laws.
2. Whether fraudulent identity creation amounts to cybercrime under Indian law.
3. What are the legal implications of election tampering within a corporate structure?

Annexures Used

Annexure E1: List of fraudulent voter IDs.

Annexure E2: Security audit report on the voting platform.

Annexure E3: Corporate bylaws related to election procedures.

Annexure E4: Evidence of vote manipulation from internal emails.

Annexure E5: Complaint filed by losing candidates.

Victim Testimony

Mr. Deepak Agarwal, a candidate in the corporate election, claims that the fraudulent votes resulted in an unjust election outcome, severely impacting his professional reputation.

CASE 3: AI-Generated Financial Fraud

Problem Statement:

Ms. *Kavya Iyer*, a small business owner, fell victim to an AI-generated phishing scam. The fraudster used an AI-driven chatbot that mimicked the voice of her bank manager, convincing her to transfer ₹5,00,000 under the pretense of a security update.

After the fraud was reported, investigations revealed that AI tools were being used to impersonate banking officials, leading to a rise in cyber financial crimes.

Legal Issues Involved:

1. Sections 419 and 420 of the *Indian Penal Code, 1860* (Cheating and Impersonation)
2. Sections 66C and 66D of the *Information Technology Act, 2000* (Identity Theft and Impersonation)
3. Banking regulations under the *Reserve Bank of India Act, 1934*

Reliefs Sought:

Compensation for financial loss.

Stricter AI cybersecurity measures for banks.

Criminal action against the perpetrators.

ANNEXURES FOR PROBLEM STATEMENT 5

Annexure E1: Chat log of the AI-driven phishing conversation.
Annexure E2: Transaction receipt for ₹5,00,000 transfer.
Annexure E3: Cybersecurity report on voice-mimicking AI fraud.
Annexure E4: Complaint filed with the cybercrime department.
Annexure E5: Bank's response denying security lapse responsibility.

Annexure E1: Chat Log of the AI Phishing Scam

Transcript of the fraudulent conversation between Ms. Kavya Iyer and the AI-generated impersonator. Voice analysis confirming AI-generated speech mimicking her bank manager's voice.

Annexure E2: Transaction Receipt

Bank transaction details showing a transfer of ₹5,00,000 made under fraudulent circumstances. Includes date, time, and beneficiary account information.

Annexure E3: Cybersecurity Report on Voice-Mimicking AI Fraud

Technical report detailing the growing use of AI in financial fraud. Provides case studies of similar incidents globally.

Annexure E4: Cybercrime Complaint Copy

Complaint filed with the *Cyber Crime Cell* under relevant provisions of the *Information Technology Act, 2000*. Official acknowledgment of the complaint.

Annexure E5: Bank's Response

Formal communication from the bank denying liability.

States that the bank followed all regulatory protocols for security.

VICTIM TESTIMONY: *Ms. Kavya Iyer*

*"I am Kavya Iyer, a small business owner who trusted her bank implicitly. One day, I received a call from someone who sounded exactly like my bank manager. He warned me about a security breach and asked me to transfer funds to a secure account.

It turned out to be an AI-generated voice scam. I lost ₹5,00,000, my savings meant for my business expansion.

This technology can be dangerously misused, and I believe financial institutions should be better equipped to prevent such frauds. I am here to seek justice for my loss and to ensure others don't fall victim to such deception."*

CASE 4: Cyberbullying and Mental Health

IN THE HON'BLE HIGH COURT OF MADRAS

Ms. Priya Menon ..... Petitioner
Versus
FaceConnect India Pvt. Ltd. & Others ..... Respondents

Problem Statement

Ms. Priya Menon, a university student, was the victim of a targeted cyberbullying campaign on *FaceConnect*, a popular social media platform. Anonymous users circulated derogatory memes and personal information, leading to severe mental health issues and hospitalization.

Despite multiple reports, the platform failed to remove the content or reveal the identities of the perpetrators. The petitioner argues that the platform violated its duty of care under the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.

Legal Issues Raised

1. Whether social media platforms have a legal obligation to prevent cyberbullying?
2. Whether failure to act amounts to negligence under Indian tort law?
3. What compensation, if any, should be awarded for mental distress caused by cyberbullying?

Legal Framework Involved

Information Technology Act, 2000

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Indian Penal Code, 1860 (Sections 354D - Stalking, 503 - Criminal intimidation)

Mental Healthcare Act, 2017

Prayer for Relief

The petitioner seeks damages for mental trauma and a directive for stricter monitoring by the platform.

ANNEXURE E1: Screenshots of Abusive Messages Received by Ms. Priya Menon

Contains derogatory memes, threats, and personal information being circulated anonymously.

ANNEXURE E2: Medical Report from *Apollo Hospitals*

Diagnoses severe anxiety and depression resulting from the online harassment.

ANNEXURE E3: *FaceConnect*'s Content Removal Response

States: *"Our platform is reviewing your complaint. Content removal decisions typically take up to 14 days."*

ANNEXURE E4: FIR Filed by Ms. Priya Menon

Charges under Sections 354D (Stalking) and 503 (Criminal intimidation) of IPC.

ANNEXURE E5: National Crime Records Bureau (NCRB) Report on Cyberbullying (2024)

States that cyberbullying cases have increased by 45% in the past two years, with young adults being the most affected demographic.

VICTIM TESTIMONY :

Witness: *Ms. Priya Menon* (University Student and Victim of Cyberbullying)

*"My name is Priya Menon. I am a university student pursuing my Master's degree in Literature. It all began when I expressed my opinion on a social issue through a post on *FaceConnect*. Soon after, anonymous accounts began targeting me with cruel messages, edited images, and hateful memes.

They even leaked my personal information—phone number and home address—which made me feel unsafe even within my own home. The bullying was relentless. I reported the harassment to the platform, but they took weeks to respond and did not remove the harmful content immediately.

This experience deeply affected my mental health. I was diagnosed with anxiety and depression, and I had to take a break from my studies to recover.

I am here today because I believe that platforms must be held responsible for ensuring the safety of their users and that those who abuse social media should face legal consequences."*

CASE 5: Unfair Trade Practice by a Fitness Center

Problem Statement

FitLife Gym Pvt. Ltd. offered a one-year membership with promises of access to premium facilities and personalized training. However, after enrolling, the gym frequently shut down its services without prior notice, and essential facilities were either unavailable or poorly maintained. Despite repeated complaints, the gym refused to issue refunds.

The affected consumers filed a complaint under Section 2(47) of the *Consumer Protection Act, 2019* for unfair trade practices and deficiency in service.

Legal Issues

1. Whether *FitLife Gym Pvt. Ltd.* engaged in unfair trade practices under the *Consumer Protection Act, 2019*.
2. Whether the gym's failure to provide agreed services amounts to a deficiency in service.
3. Whether consumers are entitled to compensation or refunds for breach of contract.

Annexures Used

Annexure E1: Membership contract between the gym and consumers.

Annexure E2: Record of gym closures and service downtimes.

Annexure E3: Written complaints by members addressed to gym management.

Annexure E4: Promotional materials advertising premium services.

Annexure E5: Gym's response citing maintenance and operational issues.

Victim Testimony

Mr. Karan Singh, a fitness enthusiast, shares that he joined *FitLife Gym* for its advanced facilities, but frequent closures and poorly maintained equipment made it impossible to utilize the membership, causing financial loss and mental frustration.

CASE 6: Unauthorized Cognitive Device Data Sharing in Healthcare

Problem Statement

NeuroHeal Pvt. Ltd. developed an AI-powered brain stimulation device for patients with neurological disorders. A patient discovered that his health data was being shared with insurance companies without consent, leading to increased premiums and denial of claims.

The patient filed a case under the *Information Technology Act, 2000*, *Digital Personal Data Protection Act, 2023*, and the *Medical Council of India (Professional Conduct, Etiquette and Ethics) Regulations, 2002*.

Legal Issues

1. Whether sharing sensitive health data without consent violates Indian data protection laws.
2. Whether health data misuse constitutes medical negligence.
3. What are the obligations of healthcare providers regarding patient data confidentiality?

Annexures Used

Annexure E1: Patient consent form provided by *NeuroHeal Pvt. Ltd.*

Annexure E2: Data-sharing agreement between the device manufacturer and insurance firms.

Annexure E3: Evidence of increased insurance premiums following unauthorized data sharing.

Annexure E4: Medical ethics committee report on data misuse.

Annexure E5: Statement from the Health Ministry on the use of cognitive devices.

Victim Testimony

Mr. Sameer Desai, a patient, testifies that the disclosure of his confidential medical data caused significant financial and emotional hardship, as insurance providers increased his premiums without prior justification.

CASE 7: Cartelization in the Cement Industry

Problem Statement

An investigation has been launched against major cement manufacturers for allegedly forming a cartel to fix prices and limit production. This alleged collusion violates Section 3(1) of the *Competition Act, 2002* and has resulted in inflated cement prices across the country.

The *Builders' Association of India* has filed a formal complaint, claiming that these practices have significantly raised construction costs and restricted fair competition.

Legal Issues

1. Whether major cement manufacturers formed a cartel violating Section 3(1) of the *Competition Act, 2002*.
2. Whether the alleged cartelization resulted in artificial price inflation and restricted market competition.
3. Whether these practices caused an appreciable adverse effect on competition and consumer welfare.

Annexures Used

Annexure E1: Email communications showing evidence of coordinated price-fixing between major cement companies.

Annexure E2: Comparative charts showing identical price hikes across all accused manufacturers.

Annexure E3: Preliminary CCI investigation report highlighting evidence of collusion.

Annexure E4: Expert analysis on the economic impact of cartelization within the construction sector.

Annexure E5: Official statements from the cement companies denying any collusion or cartel behavior.

Victim Statement

Mr. Ramesh Desai, a real estate developer, reports that the uniform price hikes across cement brands led to significant delays in construction projects, increasing costs for builders and homebuyers alike.