REPORT

---

1. Introduction to Data Ethics

In the modern digital era, data has become one of the most valuable resources. Organizations collect, process, and analyze massive amounts of data every day. This data includes personal information such as names, locations, browsing habits, preferences, and even psychological traits. While data helps businesses improve services and make better decisions, it also raises serious ethical concerns.

Data ethics refers to the moral principles and standards that guide how data is collected, stored, processed, and shared. It ensures that individuals' privacy, rights, and dignity are protected. Ethical data practices help maintain public trust and prevent misuse.

With the rapid growth of artificial intelligence (AI), big data analytics, and social media platforms, data ethics has become more important than ever. A major example that highlights the importance of data ethics is the **Facebook–Cambridge Analytica scandal (2018)**.

2. Overview of the Case: Facebook–Cambridge Analytica Scandal

The **Facebook–Cambridge Analytica scandal** became public in 2018 and revealed one of the largest data misuse incidents in history. It involved the social media platform Facebook (now Meta Platforms Inc.) and a political consulting firm called Cambridge Analytica.

The scandal showed how personal data of millions of users was collected without proper consent and used for political purposes, including influencing elections.

This case raised global concerns about:

- User privacy
- Informed consent
- Transparency
- Corporate accountability
- Data protection laws

3. Background of the Incident

In 2014, a researcher named Aleksandr Kogan developed a personality quiz app called **“This Is Your Digital Life.”** The app was available on Facebook and claimed to be for academic research.

Around 270,000 users downloaded the app and agreed to share their data. However, due to Facebook’s data-sharing policies at that time, the app was also able to collect data from users’ friends without their knowledge.

As a result, data from approximately 87 million Facebook users was collected.

This data was later shared with Cambridge Analytica, which used it for political advertising and voter profiling.

4. What Exactly Happened?

4.1 Data Collection

- Users installed the quiz app voluntarily.
- The app collected personal information such as:
    - Name
    - Gender
    - Location
    - Likes and interests
- It also collected data of users’ friends without their consent.

4.2 Creation of Psychological Profiles

Cambridge Analytica used the collected data to create detailed psychological profiles of individuals. These profiles were based on behavioral patterns and personality traits.

Using data analytics and algorithms, they categorized users into personality types such as:

- Introvert/extrovert
- Conservative/liberal
- Emotional/stable

4.3 Targeted Political Advertising

The profiles were used to send personalized political advertisements to specific groups of voters.

This strategy was reportedly used during:

- The 2016 U.S. Presidential Election
- The Brexit referendum in the UK

Targeted ads were designed to influence voter opinions and behavior.

5. Ethical Issues Involved

5.1 Lack of Informed Consent

One of the most serious ethical problems was the absence of proper informed consent.

- Users were not clearly informed about how their data would be used.
- They did not know their friends' data would also be accessed.
- The data was used for political campaigns, not just academic research.

Ethical data practices require full transparency and clear permission from users.

5.2 Privacy Violation

Privacy is a fundamental right. In this case:

- Personal data was accessed without explicit permission.
- Friends of users had no idea their data was collected.
- Sensitive information was used for manipulation.

This was a direct violation of privacy rights.

5.3 Data Misuse

Data collected for research purposes was transferred to a political consulting firm. This is considered unethical because:

- Data was used beyond its original purpose.
- It was used to influence democratic processes.

This violates the principle of purpose limitation in data ethics.

5.4 Lack of Transparency

Facebook initially failed to inform users about the data breach.

- The issue became public only after media investigation.
- The company delayed taking responsibility.

Transparency is essential for maintaining user trust.

5.5 Manipulation and Impact on Democracy

The use of psychological profiling to influence voters raises serious concerns about democracy.

- Voters were targeted with emotionally persuasive content.
- Information may have been misleading or biased.
- Citizens' free decision-making ability was potentially compromised.

This shows how data misuse can affect society at a large scale.

6. Legal and Social Consequences

6.1 Public Reaction

When the scandal became public in 2018, there was worldwide outrage.

- Millions of users deleted their Facebook accounts.
- Social media campaigns like #DeleteFacebook trended globally.

6.2 Government Investigations

Governments in the United States and the United Kingdom launched investigations.

The U.S. Federal Trade Commission (FTC) fined Facebook $5 billion in 2019 for privacy violations.

Cambridge Analytica later declared bankruptcy and shut down operations.

6.3 Impact on Reputation

- Facebook's public image was severely damaged.
- Users lost trust in the platform.
- Investors became concerned about long-term risks.

7. Role of Data Protection Laws

The scandal increased awareness about the importance of strong data protection laws.

One major regulation that gained global attention is the European Union's **General Data Protection Regulation (GDPR)**, which came into effect in 2018.

Key Features of GDPR:

- Right to access personal data
- Right to be forgotten
- Clear consent requirements
- Strict penalties for violations

After the scandal, many countries started strengthening their data protection frameworks.

8. Lessons Learned from the Case

8.1 Importance of Clear User Consent

- Consent must be informed, specific, and explicit.
- Users must know exactly how their data will be used.

8.2 Data Minimization

- Collect only necessary data.
- Avoid excessive data collection.

8.3 Accountability

- Companies must take responsibility for data handling.
- Regular security audits should be conducted.
- Ethical review boards should monitor data usage.

8.4 Transparency

- Users must be informed about data breaches immediately.
- Privacy policies should be simple and understandable.

8.5 Ethical AI Development

AI systems must be:

- Fair
- Transparent
- Free from bias
- Regularly tested for ethical compliance

9. Importance of Data Ethics in AI and Technology

Data ethics is crucial in modern technologies such as:

9.1 Banking

AI systems analyze credit scores and financial history. If data is biased, decisions may be unfair.

9.2 Healthcare

Medical AI systems use patient data for diagnosis. Privacy and confidentiality must be maintained.

9.3 Recruitment and Hiring

AI-based hiring systems must avoid discrimination based on gender, race, or background.

9.4 Social Media

Algorithms must avoid spreading misinformation and harmful content.

Ethical practices ensure fairness, trust, and long-term sustainability.

10. Recommendations for Organizations

To prevent similar incidents, organizations should:

1. Implement strict data governance policies.
2. Conduct regular cybersecurity audits.
3. Train employees in data ethics.
4. Appoint Data Protection Officers (DPOs).
5. Use encryption and secure storage methods.
6. Perform impact assessments before launching new technologies.

11. Role of Engineers and Future Professionals

As future engineers and AI professionals:

- We must design systems that respect privacy.
- Follow ethical coding practices.
- Avoid collecting unnecessary data.
- Ensure transparency in AI algorithms.
- Promote responsible innovation.

Ethics should be integrated into technical education and practice.

12. Conclusion

The Facebook–Cambridge Analytica scandal clearly demonstrates how unethical handling of data can cause serious harm to individuals, organizations, and even democratic systems.

It highlights the importance of:

- Informed consent
- Transparency
- Privacy protection
- Accountability
- Strong regulatory frameworks

Data ethics is not just a legal requirement but a moral responsibility. In the age of AI and big data, ethical data practices are essential to build trust, protect human rights, and ensure fair technological development.

As responsible engineers and technologists, we must prioritize ethical decision-making and contribute to building secure, transparent, and trustworthy digital systems.