Al-Mustaqbal University / College of Technical Engineering
Department (Department of Cybersecurity Techniques Engineering)
Class (First)
Ethics for the Information Age/ Code -UOMU0208025
Lecturer (Dr. Ahmed Hasan Al-Janabi & Msc. Heba Hussien)

2nd term – Lecture 2 Introduction to Ethics

Lecture 2

Introduction to Ethics

Email (heba.hussein.abdalabbas@uomus.edu.iq)

2nd term – Lecture 2 Introduction to Ethics

Lecture Objectives

By the end of this lecture, students will be able to:

1. Define ethics and moral principles.
2. Understand the importance of ethics in technology.
3. Identify major ethical theories.
4. Analyze technological behavior from an ethical perspective.

1. Definition of Ethics

Ethics is the study of moral principles that determine what is right and wrong behavior. It is a branch of philosophy that explores questions of morality, examining how individuals and societies make decisions about what constitutes acceptable conduct. Ethics provides frameworks for evaluating actions, intentions, and consequences, helping people navigate complex moral situations with clarity and purpose.

Ethics helps individuals make responsible decisions in society. By establishing principles and values, ethics guides behavior in personal, professional, and public contexts. It enables people to consider the impact of their actions on others, fostering a sense of responsibility and accountability that is essential for maintaining trust and cooperation within communities.

2. Computer Ethics

Computer ethics studies the ethical issues related to the use of computers and digital technologies. As technology becomes increasingly integrated into every aspect of modern life, the field of computer ethics has expanded to address a wide range of concerns, from personal privacy to global cybersecurity. This discipline examines how traditional ethical principles apply in digital environments and develops new frameworks for addressing emerging challenges.

Examples include:

- Privacy protection: Safeguarding **personal information from unauthorized access and** ensuring individuals maintain control over their own data.

- Software piracy: Understanding the ethical and legal implications of ***copying, distributing, or using software without proper licensing***.
- Cybercrime: Examining the ethical dimensions of malicious activities such **as hacking, identity theft, and online fraud**.
- Responsible online behavior: Promoting respectful, honest, and constructive interactions in digital spaces.

3. Why Do We Study Ethics in Technology?

Technology can be used in both positive and negative ways. The dual nature of technological tools means that the same innovations that enable progress and connection can also be weaponized for harm. Understanding this duality is essential for developing ethical frameworks that maximize benefits while minimizing risks to individuals and society.

3.1 Positive Uses

- Education: Online learning platforms, digital libraries, and educational software have democratized access to knowledge, enabling students worldwide to learn at their own pace.
- Scientific research: Advanced computing power accelerates discoveries in medicine, climate science, and engineering through data analysis and simulation.
- Communication: Email, video conferencing, and social media connect people across continents, fostering collaboration and maintaining relationships.
- Information sharing: The internet enables rapid dissemination of news, research, and ideas, supporting informed decision-making and public discourse.

3.2 Negative Uses

- Hacking: Unauthorized access to computer systems can compromise sensitive data, disrupt services, and cause significant financial and reputational damage.
- Identity theft: Criminals use stolen personal information to commit fraud, open accounts, and impersonate victims, causing lasting harm to individuals.

- Data breaches: Large-scale security incidents expose millions of records, eroding trust in organizations and exposing individuals to various risks.
- Online harassment: Digital platforms can be misused for bullying, stalking, and coordinated attacks that cause psychological harm to victims.

Therefore, ethical rules are necessary to guide the development and use of technology in ways that serve humanity's best interests.

4. Major Ethical Theories

4.1 Utilitarianism

Principle:

An action is ethical if it produces the greatest benefit for the greatest number of people. This consequentialist approach, developed by philosophers such as Jeremy Bentham and John Stuart Mill, evaluates actions based on their outcomes rather than their intrinsic nature. The goal is to maximize overall happiness and minimize suffering across all affected parties.

Example:

Developing security updates that protect millions of users from cyber threats. When software companies invest in security patches, they may incur costs and inconvenience some users, but the overall benefit to the global user community justifies these measures under utilitarian reasoning.

4.2 Duty Based Ethics (Deontology)

Principle:

People must follow rules and duties regardless of the consequences. Associated primarily with Immanuel Kant, deontological ethics holds that certain actions are inherently right or wrong, independent of their outcomes. This approach emphasizes moral rules, rights, and duties that should be respected in all circumstances.

Example:

A cybersecurity professional should not hack systems without authorization. Even if hacking could reveal vulnerabilities and ultimately improve security, the duty to

respect laws and individual rights prohibits unauthorized access, regardless of potential benefits.

4.3 Rights-Based Ethics

Principle:

Every person has fundamental rights that must be respected in all contexts, including digital environments. This framework emphasizes that certain entitlements belong to individuals by virtue of their humanity, and these rights create corresponding duties for others to respect them.

These fundamental rights include:

1. Privacy: The right to control access to one's personal information and to be free from unwarranted surveillance.
2. Freedom of expression: The right to share ideas and opinions without undue restriction or censorship.
3. Protection of personal data: The right to have one's information handled responsibly and securely by organizations that collect it.

These rights must be respected in digital environments, where technology creates new challenges for their protection and enforcement.

5.Ethical Issues in Technology

Examples of ethical problems in computing include:

1. **Hacking someone's account without permission:** Unauthorized access violates privacy, breaches trust, and often violates laws designed to protect digital assets.
2. **Sharing private information online**: Disclosing confidential or personal data without consent can harm individuals and damage professional relationships.
3. **Using pirated software**: Copying software without proper licensing deprives developers of compensation and undermines the sustainability of software development.

4. **Collecting user data without consent**: Gathering personal information without transparent disclosure violates autonomy and can expose users to privacy risks.

Classroom Activity 1

A student discovers a security vulnerability in the university system. This situation presents an ethical dilemma that requires careful consideration of responsibilities, potential consequences, and professional standards.

What should the student do?

A. Exploit the vulnerability
B. Sell the vulnerability
C. Report it to the university administration

Discuss which option is ethically correct and why. Consider how different ethical theories (utilitarianism, deontology, rights-based ethics) would approach this dilemma.

Classroom Activity 2

GroupDiscussion

Case Study:

A social media company collects user data without informing users. This practice has become increasingly common, raising important questions about corporate responsibility, user autonomy, and the boundaries of acceptable data collection.

Students should discuss:

1. Is this ethical? Consider the various stakeholders affected by this practice, including users, shareholders, employees, and society at large.
2. What risks may result? Explore potential harms including privacy violations, identity theft, manipulation, and erosion of trust.
3. What should companies do to protect users? Discuss transparency measures, consent mechanisms, and corporate governance practices.

Short Questions

2nd term – Lecture 2 Introduction to Ethics

1. What is computing?
2. Name one early computing device.
3. What is computer ethics?
4. Give two examples of ethical issues in technology.

Email (heba.hussein.abdalabbas@uomus.edu.iq)