Emerging Issues in Computer science

Week 12: Ethical and Legal Considerations in Emerging Technologies

Lecturer: Ikwap Flavia Agatha

Lecture learning out come

By the end of this lesson you will be able to

- Understand the Concept and concern in Ethics
- Understand the types of Ethics
- Understand the different Ethical Concerns in computer science Innovations
- Understand the different Commandments in computer Ethics
- Understand Cyber law, how it works and its importance

The Role of Ethics in Technology

- As technology evolves, it increasingly influences personal lives and society at large.
- Ethical considerations must guide the development of new tools, such as artificial intelligence, to ensure they benefit society and do not cause harm—such as job displacement or manipulation of human interactions.

What is Ethics?

- "Ethics" in computer science innovations and trends refers to the moral principles and societal impacts that guide the development, deployment, and use of technology. As new technologies emerge—like artificial intelligence, big data, facial recognition, and autonomous systems—ethical considerations help ensure they are used responsibly and do not harm individuals or society.

Common Ethical Issues

- **Intellectual Property**: Respecting copyrights and digital ownership.
- **Online Behavior (Netiquette)**: Maintaining respectful and responsible digital conduct.
- **Piracy**: Using or distributing software without proper licensing violates ethical standards.
- **Hacking**: Unauthorized access to systems is unethical and often illegal.
- **Copyright Infringement**: Duplicating or sharing digital content without permission is against ethical and legal norms.

Forms of Computer Ethics

Three Main Forms of Computer Ethics:

- **Ethics between a person and themselves**

  Refers to how an individual responsibly uses computers on a personal level, such as avoiding harmful or addictive behaviors and using devices with integrity.

- **Ethics between individuals (person-to-person)**

  Involves the ethical ways people interact through computers, such as respecting privacy, avoiding cyberbullying, or not sharing harmful or false information.

- **Ethics between the user and the device**

  Concerns the responsible use of technology, including proper handling of hardware/software, and avoiding misuse like installing pirated software or harming systems intentionally.

Common Ethical Issues in Computer Use:

Privacy Concerns:

- **Hacking**: Illegally accessing someone else's system or data without permission.
- **Malware**: Harmful software like viruses and spyware that damage or steal from computers.
- **Data Protection**: Balancing user privacy with the need for data use in business.
- **Anonymity**: The ability to hide one's identity online, which can be used ethically or unethically.

Intellectual Property Rights

- **Copyright**: Legal protection for creators, preventing unauthorized use or distribution of their work.
- **Plagiarism**: Using someone else's work without giving credit, essentially stealing intellectual content.
- **Cracking**: Bypassing software security features to access or use it without authorization.
- A **software license** grants user's permission to use digital content under specific terms outlined in a **license agreement**. It does **not transfer ownership**—the original **copyright holder retains full rights**, and users are only allowed to use the software as permitted by the license.

Importance of Ethical Behavior to a User

- Ethical behavior in computer use is essential to ensure safety, fairness, and responsibility in digital environments. It helps protect sensitive personal and commercial data, prevents cybercrimes like plagiarism and identity theft, promotes equal access to technology, and encourages fair business practices.
- Computer ethics also foster trust by ensuring information is used responsibly, contributing to a secure and respectful digital society.

Ethical Issues in Computer Science:

- Information Technology (IT) raises several ethical concerns that affect individuals, organizations, and society. This include:
- **Personal Privacy** – With widespread network connectivity, there's a high risk of unauthorized data access, making it crucial to protect user information and maintain data integrity.
- **Access Rights** – Ensuring that only authorized users access sensitive systems is a top priority, especially with the rise of e-commerce and online services.
- **Harmful Actions** – Intentional damage such as hacking, data corruption, or virus spreading can result in serious loss of information, time, and resources.

Ethical Issues in Computer Science

- **Patents** – Protecting unique software ideas through patents is challenging due to the need for full disclosure, making it harder to maintain exclusivity.
- **Copyright** – Copyright laws are vital in protecting digital content and software from misuse, especially in cases of data breaches.
- **Trade Secrets** – These protect confidential business information, offering a competitive edge, but once leaked, they lose legal protection.
- **Liability** – Developers and vendors must be clear and honest about their product claims, as misleading statements can result in legal consequences.
- **Piracy** – Illegal duplication of software remains a widespread issue, and efforts are ongoing to strengthen laws and enforcement to combat it.

Ethnical concern in emerging technologies

Virtual reality

- Virtual reality (VR) presents a range of ethical concerns, including possible effects on users' physical and mental health, as well as their behavior and social interactions. Addressing these emerging issues will require not only formal laws and regulations—such as governmental or institutional oversight—but also practical ethical approaches that emphasize respect, empathy, moral awareness, and education.
- Embedding ethical considerations into the development process is known as “anticipatory technology ethics,”

Ethical Considerations in Virtual Reality (VR) and Augmented Reality (AR)

1. ***Physiological and Cognitive Impacts***

- **Health Concerns**: VR and AR can affect users' physical and mental health—causing issues such as motion sickness, disorientation, or cognitive overload.
- **Addiction & Overuse**: Immersive environments may lead to compulsive use or escapism, especially among younger or vulnerable users.

2. ***Behavioral and Social Dynamics***

- **Behavior Modification**: Prolonged exposure to immersive environments can influence real-world attitudes and behaviors (e.g. desensitization to violence or social isolation).
- **Identity and Presence**: Users may struggle to differentiate between real and virtual experiences, potentially impacting their sense of self and relationships.

Ethical Considerations in Virtual Reality (VR) and Augmented Reality (AR)

3. ***Privacy and Data Security***

- **Surveillance Risk**: AR/VR systems can collect detailed biometric, behavioral, and environmental data.
- **Informed Consent**: Users may not fully understand what data is being collected or how it's used, creating concerns around transparency and exploitation.

4. ***Psychological Manipulation***

- **Persuasive Design**: VR and AR can subtly influence users through highly tailored, immersive content, raising concerns about manipulation or propaganda.
- **False Realities**: There is ethical risk in creating environments or scenarios that intentionally deceive or emotionally manipulate users.

Ethical Considerations in Virtual Reality (VR) and Augmented Reality (AR)

5. Inclusion and Accessibility

- **Bias and Exclusion**: VR/AR content and hardware often lack inclusive design, potentially alienating people with disabilities or underrepresented groups.
- **Digital Divide**: Widespread VR/AR adoption may worsen inequities in access to technology.

6. Ethical Design and Responsibility

- **Anticipatory Ethics**: Designers and developers must consider potential long-term consequences during early development stages.
- **Respect and Care in Practice**: Ethics should go beyond regulation—embedding values like empathy, consent, and social good directly into system design.

Ethical concerns in Block Chain

- Privacy and Data Security: Block-chain's inherent transparency and immutability mean that once data is added, it cannot be altered and is visible to all participants. This becomes problematic when sensitive or personal data is involved, as it may conflict with privacy regulations like the GDPR.
- Absence of Regulatory Frameworks: Due to its decentralized structure, block-chain lacks centralized control or enforcement mechanisms. This can enable unlawful behavior such as money laundering, tax avoidance, or trafficking in illegal goods.
- Example: Crypto-currencies being utilized for transactions on illegal online platforms.

Ethical concerns in Block Chain

- Impact on the Environment: Energy-intensive consensus mechanisms like Proof-of-Work require vast computational power. The significant energy consumption contributes to environmental degradation and climate concerns.
- Technological Exclusion and Inequality: Access to block chain technology is not universally available, especially in low-income or remote regions, this technological gap may worsen existing economic and social disparities. Example: People without internet access being unable to benefit from block-chain based financial tools.

Ethical concerns in Block Chain

- Lack of Clear Accountability: In decentralized systems, it is often unclear who should be held responsible when problems arise. Therefore Victims of technical failures or fraudulent activities may have limited avenues for recourse. Example: Users losing funds due to bugs or vulnerabilities in smart contracts.
- Potential for Mass Surveillance: Block chain technology could be used by states or corporations to track user activities. This raises concerns about privacy rights and the misuse of personal data.
- Over-Commercialization through Tokenization: Block chain enables the conversion of nearly any asset or concept into digital tokens. This may lead to the inappropriate monetization of deeply personal or cultural elements. Example: Selling personal genetic information or life experiences as non-fungible tokens (NFTs).

Overview of IOT Ethics

- Ethics, as a philosophical discipline, governs human behavior by distinguishing right from wrong. In the context of the Internet of Things (IOT), ethics involves creating standards and regulations to guide how humans interact with IOT technologies.

Need for Ethical Frameworks in IOT

- Due to IOT's vast scale, diversity, and complexity, existing policies are often insufficient. As IOT grows, ethical concerns rise from issues like user privacy, transparency, and algorithmic decision-making.
- A meaningful ethical framework must apply across human, autonomous systems, and both digital and physical environments. Companies that uphold ethical standards can improve product design and maintain user trust, while failure to do so may result in data access losses.

Ethical Design for IOT

- With billions of devices generating vast data, there’s a pressing need for ethically designed systems. Ethical IOT products should give users control over their personal data and offer customizable privacy settings.
- These options would be built into algorithms by developers and might come at an extra cost, offering users the choice to pay for added ethical features such as better data protection.

Key features of ethically designed IOT devices include

- User control over data collection and distribution
- Ability to enforce privacy rules regardless of location
- Flexibility to adapt to different environments (e.g., home, work)
- Support for ethically significant relationships and decisions

Ethical Challenges in IOT

- Despite widespread adoption, IOT faces several ethical hurdles:
- **Data Ownership**: It's often unclear who owns the data collected, especially without user consent.
- **Public vs. Private Boundaries**: IOT sensors may blur lines between private and public information.
- **Real-World Impact**: Security breaches in IOT systems can have direct physical consequences, such as manipulating home systems or vehicles, potentially endangering lives.

Ethical issues in cloud computing

Data Ownership

- **Ambiguity of Ownership**:

  Cloud usage raises the question of whether data remains private property or becomes owned by the service provider.

- **Cloud Service Usage**:

  Individuals and businesses use cloud services for flexibility and scalability without owning infrastructure.

  Services are provided by various companies with differing policies.

Ethical issues in cloud computing

Regulatory Challenges

- Cloud computing operates across international borders.
- National laws often fail to align or apply effectively at a global scale.
- Current regulations are largely domestic and not well-suited for global cloud operations.

Ethical Considerations

- Ethics, especially human dignity, privacy, and data protection, are central to the debate.
- The European Data Protection Supervisor (EDPS) emphasizes human dignity as a foundation for digital rights.

Four pillars for ethical cloud computing:

- Future-oriented regulation
- Accountability through codes of conduct and audits
- Privacy-aware engineering
- Empowerment of end users

Complex Nature of Ownership

- Ownership depends on how and where data is created.
- Some data is user-generated; some is produced or processed by cloud services.
- Terms of service may result in users losing ownership or rights over their data.
- Manipulation and optimization (e.g., through algorithms) further blur ownership lines.

Data security and Privacy

1. ***Definition and Scope***

- **Data security** in cloud computing refers to protecting data from unauthorized access.
- It’s primarily a **technical responsibility** of cloud service providers.

2. ***Complexity and Risks***

- Cloud environments involve **multiple interconnected services** and providers.
- The **“weakest link”** in the network can compromise the entire system.

Data security and Privacy

3. Ethical Responsibility

- Data security extends beyond legal requirements—ethical responsibility lies in protecting stakeholders' data.
- Upholding data security is seen as contributing to the greater societal good.

4. Dependence on Cloud Models

- In SaaS, users rely fully on the provider for security.
- In PaaS, developers also bear some security responsibilities.

Data security and Privacy

5. Data Lifecycle Security

- Security must be maintained at all stages: Create, Store, Use, Share, Archive, Destroy
- Special attention is needed for data traces that remain after deletion.

6. Core Data Properties

- Users expect protection of:
  - **Integrity** – no unauthorized modifications.
  - **Confidentiality** – no unauthorized disclosure.
  - **Availability** – reliable access and recovery

Data security and Privacy

7. Trust and Verification

- Providers must monitor access, involve third-party oversight, and verify integrity to build user trust.

8. Data Privacy

- Data privacy is the perception of security from the user's perspective.
- Privacy means users can control how and when their data is shared

9. Legal and Regulatory Compliance

- Data privacy laws mandate consent, notice, and accountability (e.g., GDPR, U.S. Privacy Act).
- Providers must balance privacy, usability, and compliance.

Data security and Privacy

10. Ongoing Concerns

- Cloud data is still too mobile and vulnerable.
- Providers may track and share data without user knowledge or consent.

11. Policy and Ethical Frameworks

- Government initiatives like the UK Data Ethics Framework promote transparency, accountability, and ethical use of data.
- The European Data Protection Supervisor (EDPS) stresses human-centric, purpose-bound data use

Cloud Providers

1. Stakeholder Ethics and Power Imbalance

- Cloud providers and users have different roles and ethical concerns.
- Users often surrender control of their data, relying on trust in providers.

2. Trust as Central to Cloud Engagement

- Trust is essential: without it, users are hesitant to engage with cloud services.
- Ethical behavior by providers helps build and sustain user trust.

3. Codes of Ethics as Tools for Trust

- Codes of ethics can promote trust across international boundaries where regulation varies.
- They guide both individual conduct (codes of conduct) and organizational behavior (codes of ethics).

4. Benefits of Ethical Codes

- Promotes responsible behavior, improves products/services, boosts workplace culture, and enhances overall quality.
- Ethics need to be adaptable and robust to match the evolving nature of cloud computing.

5. Ethical Frameworks

- Codes are influenced by:
  - Deontological ethics (duty-based imperatives like honesty, privacy, intellectual property).
  - Utilitarian ethics (balancing diverse stakeholder interests).

6. Challenges of Global Ethics Implementation

- Ethics codes must transcend cultural and legal differences.

- Proposals include two-part codes:
  - One part for universal principles.
  - One part for local applicability.
- Codes should be specific enough to guide behavior but flexible enough to evolve.

7. Limitations of Codes

- Ethical codes are **often seen as insufficient** to change organizational culture alone.
- They are **necessary but not always effective** without proper enforcement and buy-in.

Artificial Intelligence Ethics

- Although there’s no universal governing body enforcing guidelines, many tech companies have adopted their own AI ethical codes. AI ethics serve as principles that ensure AI development and usage are responsible, fair, and safe for users and society.

What Are AI Ethics?

- AI ethics are guiding principles used by stakeholders—engineers, companies, and policymakers—to ensure AI is developed and deployed in a responsible and humane way. Key concerns include:

What Are AI Ethics?

- Preventing algorithmic bias
- Safeguarding user data and privacy
- Reducing environmental harm
- AI ethics are implemented through company policies and national or international regulations. While ethics discussions began in academic circles and nonprofits, today major tech firms like Google, Meta, and IBM have dedicated teams addressing these concerns.

Historical Context

- Science fiction writer Isaac Asimov predicted AI risks early on through his "Three Laws of Robotics," which focused on preventing harm to humans. These ideas inspired modern ethical frameworks, such as the **Asilomar AI Principles**, developed by experts across various fields to guide the safe evolution of AI.

Key Stakeholders

- Developing ethical AI requires collaboration across sectors:
- **Academics**: Provide research and theory to support ethical AI design.

Key Stakeholders

- **Governments**: Create national strategies and regulations (e.g., NSTC's AI report in 2016).
- **Global Bodies**: Organizations like the UN promote global standards (e.g., UNESCO's AI ethics agreement in 2021).
- **Nonprofits**: Advocate for inclusive and fair AI (e.g., Black in AI).
- **Private Companies**: Build internal ethical frameworks and codes of conduct.

Why AI Ethics Matter

- AI systems often mirror human biases and can perpetuate harm, especially to underrepresented groups. If built on flawed or biased data, AI can lead to discrimination, security risks, and ethical violations. Embedding ethics early in development helps prevent these issues.

Examples of AI Ethics Issues

- **Lensa AI** (2022): Criticized for using artists' work without consent.
- **ChatGPT**: Raises concerns about misuse in education and content creation.
- These examples show the potential for both innovation and ethical dilemmas in AI applications.

Common Ethical Challenges

- **Bias**: AI tools, like Amazon's resume scanner, have shown gender bias due to flawed training data.
- **Privacy**: AI often collects data without users' explicit consent, leading to privacy concerns.
- **Environmental Impact**: Large AI models consume vast energy, raising sustainability issues.

Overview of the Ten Commandments in Computer Ethics

- **Do not harm others using a computer** – Avoid any activity that could hurt people physically, emotionally, or financially, including data theft or cyberbullying.
- **Do not interfere with others' digital work** – It's unethical to disrupt or hinder others' use of computers, such as through malware or resource hogging.
- **Respect others' digital privacy** – Peeking into someone else's files or emails without permission is akin to invading personal space and is ethically wrong.

Overview of the Ten Commandments in Computer Ethics

- **Do not steal with a computer** – Using technology to take confidential information, financial data, or intellectual property is equivalent to theft.
- **Avoid spreading false information** – Contributing to misinformation or rumors via emails, social media, or websites is unethical and can cause real-world harm.
- **Do not use unlicensed software** – Copying or using proprietary software without permission violates ownership rights and is considered digital piracy.
- **Avoid unauthorized use of others' resources** – Accessing another person's computer or network without consent or compensation is unethical.

Overview of the Ten Commandments in Computer Ethics

- **Give credit for others' digital work** – Misappropriating someone's code, content, or digital creation without attribution is theft of intellectual output.
- **Think about the social impact of your digital creations** – Developers should consider how their software or systems may affect users or society at large.
- **Always use technology respectfully and considerately** – Your digital behavior should reflect respect for others' rights, well-being, and digital space.

What is Cyber Law and How it Works?

- **Cyber Law**, also known as **digital law**, refers to the legal framework that governs the use of the internet, digital communication, and modern technologies like smartphones and computers. It addresses issues such as **online privacy**, **freedom of expression**, **data protection**, and **cybercrimes**.
- The main goal of cyber law is to **protect individuals and organizations** from malicious online activities and to **regulate** the safe and ethical use of technology.
- Parliaments and governments are encouraged to **enforce and operationalize cyber laws** to enhance **security**, **trust**, and **integrity** in electronic transactions, helping to foster a safe environment for **e-business** and digital interactions.

Importance and Role of Cyber Law

- Cyber law plays a vital role in regulating the safe use of electronic devices and digital systems. According to the Computer Misuse Act, cyber law aims to:
- Ensure the security of electronic transactions and information systems.
- Prevent unauthorized access and the misuse or abuse of computers.
- Promote trustworthy and secure conduct of digital activities.

Why Cyber Law Is Important

- **Protects Businesses**: Helps secure companies from cyber threats that could harm operations and data.
- **Ensures Safe Work Environment**: Safeguards employees from risks related to cyber-attacks, maintaining productivity.
- **Protects Personal Information**: Keeps user data safe, ensuring customer trust and privacy.
- **Preserves Productivity**: Prevents slowdowns or disruptions caused by viruses or malware.
- Cyber laws are especially critical for small businesses, which often have weaker cyber security and higher vulnerability to digital threats.

Summary of computer science trends

1. Synthetic Media

Synthetic media refers to AI-generated content, including virtual announcers and AI hosts. While still in experimental stages, this technology is expected to revolutionize content creation and distribution across various platforms.

2. Post-Quantum Cryptography

As quantum computing advances, traditional encryption methods become vulnerable. Post-quantum cryptography focuses on developing new algorithms to secure data against potential quantum attacks, ensuring the integrity and confidentiality of information in the quantum era.

3. Hybrid Computing Systems

Hybrid computing integrates various computing models, such as classical, quantum, and neuromorphic systems, to perform complex tasks more efficiently. This approach optimizes performance by leveraging the strengths of each computing paradigm.

4. Edge Computing

Edge computing processes data closer to its source, reducing latency and bandwidth usage. This is particularly beneficial for applications like autonomous vehicles and industrial automation, where real-time data processing is critical.

5. 5G-Advanced Networks

5G-Advanced, also known as 5.5G, offers enhanced connectivity with higher speeds and lower latency. It supports applications such as extended reality and massive machine-type communication, paving the way for innovations in smart cities and industrial automation.

6. Cybersecurity Innovations

As digital threats evolve, cybersecurity is becoming more proactive. AI-based threat detection, zero-trust architectures, and biometric authentication are being implemented to safeguard systems and data from increasingly sophisticated cyberattacks.

7. Bio-Inspired Computing

Bio-inspired computing draws from natural processes to solve complex problems. Techniques like evolutionary algorithms and swarm intelligence are applied to optimize solutions in areas such as logistics and artificial intelligence.

8. Blockchain Beyond Cryptocurrency

Blockchain technology is finding applications beyond cryptocurrencies. It's being utilized in supply chains for enhanced traceability, in decentralized finance (DeFi) for increased access to financial services, and in entertainment for managing intellectual property through smart contracts.

9. Cyberbiosecurity

Cyberbiosecurity is an emerging field at the intersection of cybersecurity and biosecurity. It addresses the potential for malicious activities targeting biological data and processes, aiming to safeguard the bioeconomy by protecting valuable information and materials at the interface of life sciences and digital technologies.

10. Polyfunctional Robots

Polyfunctional robots are machines capable of performing multiple tasks across different domains. These versatile robots are utilized in various industries, including manufacturing and healthcare, adapting to various roles as needed.

11. Neuromorphic Computing

Neuromorphic computing mimics the structure and function of the human brain using specialized hardware. This approach enables more efficient processing for tasks like pattern recognition and sensory processing, paving the way for cognitive computing systems.

12. DNA Computing

DNA computing leverages the unique properties of DNA molecules to perform computations. This unconventional approach holds promise for solving complex problems in areas like cryptography and data storage.

13. Spatial Computing

Spatial computing enables interaction with digital content in a three-dimensional space. By integrating sensors and computer vision, devices can understand and respond to the physical environment, enhancing experiences in virtual reality, augmented reality, and mixed reality applications.

14. Quantum Computing

Quantum computing leverages the principles of quantum mechanics to process information in fundamentally new ways. Companies like Google, IBM, and Microsoft are developing quantum processors such as Google's Willow chip, which can solve complex problems in seconds that would take classical computers millennia. This technology promises advancements in cryptography, optimization, and drug discovery.

16. Artificial Intelligence (AI)

AI continues to revolutionize various sectors, from healthcare diagnostics and drug development to autonomous systems and creative industries. Advancements in machine learning and neural networks enable AI to perform complex tasks, enhancing efficiency and innovation across fields.

17. Robotics and Autonomous Systems

The integration of AI into robotics has led to the development of autonomous systems capable of performing tasks in dynamic environments. Applications range from industrial automation and logistics to healthcare and service industries, improving productivity and safety.

18. Extended Reality (XR): AR, VR, MR

Extended Reality encompasses Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR), technologies that blend the physical and digital worlds. These immersive experiences are transforming sectors such as education, training, entertainment, and design by providing interactive and engaging environments.

19. Sustainable Computing

With growing environmental concerns, sustainable computing focuses on creating energy-efficient systems and reducing the carbon footprint of technology. This includes developing green data centers, optimizing algorithms for energy consumption, and promoting eco-friendly hardware.

20. Huawei's HarmonyOS Laptops

Huawei has introduced laptops running its proprietary HarmonyOS 5, challenging traditional operating systems. The MateBook Fold features an 18-inch OLED foldable screen and aims to reduce reliance on Western technologies, reflecting a significant shift in the global tech landscape.

Reference

Farsi, M. (2019). *Digital Twin Technologies and Smart Cities* . UK: Springer.

Lynn, T. (2021). *Data Privacy and Trust in Cloud Computing.* Palgrave Macmillan.

Slater, M. (2020). The Ethics of Realism in virtual and Augmented Reality.

Fontiers In Virtual Reality, 1-13.

http://tpointtech.com/