UNIT 7

Legal and Ethical Aspects of Computing System

Student Learning Outcomes

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

- Understand the fundamental legal and ethical considerations in computing systems.
- Identify various privacy and security threats in digital environments.
- Explain strategies for preventing and mitigating security threats.
- Discuss the digital divide and its implications for different social groups.
- Recognize and address bias in computing systems.
- Utilize information safely and responsibly.
- Assess the impact of computing on individuals and society.
- Apply principles of digital citizenship and ethical conduct.

Introduction

In today's digital world, computing systems play a crucial role in every aspect of our lives, from personal devices to complex networks. As these systems become more integrated into our daily routines, understanding the legal and ethical considerations associated with their use is essential. This chapter delves into various aspects of digital technology, including terms of use, privacy and security threats, and the digital divide. The legal and ethical challenges in computing cover a range of issues such as data protection, intellectual property rights, and compliance with relevant laws. Ethical considerations address privacy, fairness, and the broader societal impacts of technology.

7.1 Understanding Terms of Use

"Terms of Use", also called Terms and Conditions or Terms of Service, are legal agreements that outline how a service or product can be used. These terms are set by the provider (like a website, app, or software company) and must be agreed upon by the user. The main purpose is to establish a fair and transparent relationship between the provider and the user, ensuring that both parties understand their rights and obligations.

Example: When you use a Pakistani online shopping platform like Daraz, the Terms of

Use may include clauses about payment methods, return policies, and delivery procedures, ensuring that customers are aware of what to expect and what is expected of them.

7.1.1 Importance

Understanding Terms of Use is important for several reasons:

1. **Protection of Rights:** Terms of Use protect users by defining their rights, such as the right to privacy, the right to receive certain levels of service, and the right to seek redress if something goes wrong.
   Example: When we use a food delivery service in Pakistan like Foodpanda, the Terms of Use specify what happens if your order is incorrect or the delivery is delayed.
2. **Clarity and Transparency:** These terms provide clarity and transparency about what users can expect from a service. They explain what the service provider will deliver, under what conditions, and what actions are not permitted. This prevents misunderstandings and helps users make informed decisions.
   Example: If we use a mobile phone for sending or receiving payments, the Terms of Use will outline transaction limits, fees, and process for reporting unauthorized transactions.
3. **Legal Safeguards:** For businesses, Terms of Use act as a safeguard against misuse of their services. They set boundaries to protect the company from potential legal issues caused by users not adhering to the rules.
   Example: A Pakistani online education platform may include terms that prohibit the sharing of course content without permission, protecting their intellectual property.

7.1.2 Common Clauses and Conditions

Terms of Use usually contain several common clauses, which are designed to protect both the provider and the user. These clauses include:

1. **User Obligations:** These clauses outline what is expected from the user.
   Example: In Pakistan, popular ride-sharing apps such as Careem include terms that require users to provide a valid phone number and prohibit the misuse of the service for non-transportation purposes.
2. **Limitations of Liability:** These clauses limit the service provider's liability if something goes wrong.
   Example: In Pakistan, if you use an online banking service and the app is temporarily down, the bank's Terms of Use will typically limit their liability for such disruptions.
3. **Privacy and Data Use:** Privacy clauses explain how a company will collect, use, and protect user data. This is particularly important given the increasing

concerns around data privacy.
Example: If you use a messaging app like WhatsApp, the Terms of Use outline how your messages are stored and protected.

4. **Intellectual Property Rights:** These clauses protect content owned by the service provider, such as logos, software, and other proprietary materials.
Example: A Pakistani news website may include terms that prohibit users from copying and distributing their articles without permission, ensuring that their content is not misused.
5. **Termination of Service:** This clause explains the conditions under which the provider can terminate a user's access to the service.
Example: Social media platforms like Facebook have terms that allow them to suspend or terminate accounts that violate community standards, such as accounts that spread hate speech or misinformation.

7.1.3 Legal Ramifications

Violating the Terms of Use can lead to serious legal consequences. Users can be fined, sued, or banned from using the service.
Example: Using software without a proper license may result in legal action for software piracy. Companies that use unlicensed software face legal risks and cybersecurity threats.

7.1.4 Ethical Considerations

Ethical considerations in Terms of Use include fairness, transparency, and respect for user rights. It is essential for companies to ensure that their terms are clear, straightforward, and not overly complex or deceptive.
Example: In Pakistan, when users sign up for an online course, the terms should clearly specify whether a certificate will be awarded, how personal data will be handled, and whether there are any additional fees.

7.1.5 Personal Rights

Personal rights within the Terms of Use include the right to privacy, the right to be informed, and the right to withdraw consent. It is essential for users to be aware of these rights and understand how to exercise them.
Example: Under Pakistan's Personal Data Protection Bill, users have the right to access their personal data and request corrections or deletions. When engaging with services like local e-commerce websites, users have the right to know how their personal information, such as addresses and phone numbers, will be utilized.

Some online platforms frequently update their Terms of Use. It's a good practice to review them periodically to stay informed about any changes.

7.2 Privacy and Security Threats

In today's digital world, privacy and security threats are major concerns for individuals and organizations alike. These threats have the potential to compromise personal information, financial data, and overall online security. Understanding these risks is essential for protecting sensitive information. The main types of privacy and security threats are outlined below:

7.2.1 Types of Security Threats

There are five primary categories of security threats associated with online services.

7.2.1.1 Spam

Spam refers to unwanted messages that you receive on your email or phone.

Example: You may receive numerous text messages from unknown numbers offering products or services you did not request.

7.2.1.2 Spyware

Spyware is a type of harmful software that secretly monitor your activities on your computer or mobile phone.

Example: If you download a free app from an unreliable source, it may install spyware on your device. This spyware can secretly monitor your online activities, such as the websites you visit or the information you enter, without your knowledge.

7.2.1.3 Cookies

Cookies are small files that websites place on your device when you visit them. They help the website remember things like your login details and personal preferences.

Example: When you visit an online shopping site, cookies save your login information so you do not need to enter it every time you visit. However, cookies can also track your online activities, such as the products you view, to show you advertisements related to your interests.

7.2.1.4 Phishing

Phishing is a type of scam where someone pretends to be a trustworthy organization to trick you into giving away your personal information.

Example: You may receive an email that looks like it comes from your bank, asking you to click a link and enter your account details. If you follow these instructions, your money could be at risk because the email is fake.

Pharming

Pharming is a sophisticated technique where users are redirected to a fake website without their knowledge.

Example: Imagine you want to access your online banking account, but due to a pharming attack, you are sent to a counterfeit site that looks just like your bank's real site. If you enter your login information on this fake site, the scammer collects your details.

Over 90% of phishing attacks are carried out through email. These scams often look like legitimate communications from trusted organizations, making it crucial to verify the source before clicking on any links or providing personal information.

7.2.2 Security Threat Prevention Techniques

To protect yourself from online threats, it is important to use various security tools and practices. These techniques help safeguard your personal information and ensure a safer online experience.

7.2.2.1 Spam Filters

Spam filters help keep unwanted emails out of your inbox.

Example: If you receive a lot of promotional emails that you don't want, a spam filter can automatically move these emails to a separate folder or delete them. This way, you only see the emails you actually want.

7.2.2.2 Antivirus Software

Antivirus software protects your computer from harmful programs like spyware.

Example: If you download a file from the internet, antivirus software checks it for any hidden threats. If the file is safe, you can open it without worry. If it is harmful, the software will alert you and prevent the file from causing damage.

7.2.2.3 Cookie Management

Cookies are small files stored on your computer by websites. Managing cookies means deciding which cookies you want to keep and which ones you want to delete.

Example: You can keep cookies from your favorite shopping website so you don't have to log in every time, but it is good idea to delete cookies from unfamiler sites to protect your privacy.

7.2.2.4 Recognizing Phishing

Phishing is a type of online scam where attackers try to trick you into sharing sensitive

information, such as passwords, credit card numbers, or bank details.

Example: You may receive an email that appears to be from your bank, asking you to click a link and enter your account details. Recognizing phishing involves identifying these emails as fake and avoiding clicking any links or providing any information.

7.2.2.5 Guarding Against Pharming

Pharming is when attackers redirect you from a legitimate website to a fake one to steal your information.

Example:

If you type in the URL for your bank's website, pharming can send you to a fake website that looks just like your bank's site. To guard against pharming, always check that the website's address is correct and secure (look for "https://" and a padlock symbol in the browsers address bar).

Tidbits

Effective online security involves using multiple strategies like spam filters, antivirus software, and careful cookie management to cover various threat types. Combining different security techniques provides better protection against online threats.

7.3 The Digital Divide and Its Impacts

The digital divide refers to the gap between individuals, communities, and regions that have access to modern Information and Communication Technology (ICT) and those that do not. The digital divide is a critical issue because it can lead to unequal opportunities in education, employment, healthcare, and social participation.

7.3.1 Causes of the Digital Divide

Several factors contribute to the digital divide:

1. **Economic Barriers:** One of the primary causes of the digital divide is the economic barrier. Many individuals and families cannot afford the costs associated with computers, smartphones, or broadband internet. This economic disparity is particularly evident in developing countries, rural areas, and among low-income populations.
2. **Geographical Barriers:** Access to ICT varies significantly between urban and rural areas. In many parts of the world, especially in remote or rural areas, the infrastructure necessary for internet connectivity is either underdeveloped or non-existent.

3. **Educational Barriers:** Lack of digital literacy is another significant factor contributing to the digital divide. Even when the technology is available, individuals may not know how to use it effectively due to a lack of proper education and training.
4. **Social Barriers:** Age, gender, and disability can also affect access to technology. For example, older adults may be less inclined or able to use new technologies, and women in some regions may face cultural barriers that limit their access to ICT.

7.3.2 Impacts of the Digital Divide

The digital divide has far-reaching impacts on individuals and society as a whole. These impacts can exacerbate existing inequalities and create new ones.

7.3.2.1 Educational Inequality

Access to the internet and digital tools is increasingly essential for education. Students who lack access to these resources are at a significant disadvantage.

Example: During the COVID-19 pandemic, when schools in Pakistan and around the world shifted to online learning, students from low-income families or rural areas struggled to keep up with their studies due to a lack of internet access or devices. This has led to a widening of the educational gap between different socio-economic groups.

7.3.2.2 Economic Disparities

The digital divide also has significant economic implications. In today's economy, many jobs require at least basic digital skills. Those without access to technology or the internet may find it challenging to secure employment, leading to higher unemployment rates in already disadvantaged communities.

Example: In Pakistan, access to online job portals and digital banking services is often limited to those in urban areas, further widening the economic gap between urban and rural populations.

7.3.2.3 Social and Civic Participation

The digital divide can also affect social and civic participation. Access to social media, online news, and digital government services allow individuals to stay informed and engaged in civic activities. However, those without access are often excluded from these opportunities, leading to a lack of representation and participation in democratic processes.

Example: In Pakistan, access to e-government services is more readily available in cities, leaving rural populations with limited means to participate in governmental processes or access social services.

7.3.2.4 Health Disparities

The digital divide can lead to unequal access to health information and services. Digital platforms provide valuable resources for health education, telemedicine, and appointment scheduling.

Example: In Pakistan, rural communities with limited internet access may struggle to find reliable health information online or participate in telemedicine consultations.

7.3.2.5 Digital Literacy Gap

A significant digital divide also creates a gap in digital literacy. Individuals who do not have access to technology may not develop essential digital skills, further reinforcing the divide between those who are tech-savvy and those who are not.

Example: In Pakistan, people who lack access to computers and the internet may miss out on opportunities to learn and practice digital skills.

7.3.3 Bridging the Digital Divide

Bridging the digital divide means making sure everyone has equal access to technology and the internet. This is important for giving everyone the same chances to learn and grow. Here are some ways to do it:

1. **Government Initiatives:** The government can help by building the infrastructure needed for internet access in areas where it's not available.
2. **Educational Programs:** Schools and community centers can teach people how to use technology.
3. **Public-Private Partnerships:** When the government teams up with businesses and nonprofits, they can make technology more affordable.

The Government of Pakistan has launched several initiatives to increase internet access in rural areas, including the introduction of mobile broadband services in remote regions.

Class Activity

Think about your own community. Are there people who may not have access to the internet or digital devices? What can be done to help them? Write a short paragraph on how your school or community can help bridge the digital divide.

7.4 Computing's Impact on Individuals and Society

Computing systems have revolutionized the way we live, work, and communicate, bringing profound changes to society. The widespread adoption of technologies like the

internet, smartphones, and Artificial Intelligence (AI) has led to both positive and negative impacts.

7.4.1 Positive Impacts

One of the most significant positive impacts of computing is the increased accessibility to information. The internet has made it possible for people to access vast amounts of information on nearly any topic, breaking down barriers to education and knowledge.

Example: Online educational platforms such as Coursera and edX allow students from remote areas to take courses from prestigious universities around the world.

Moreover, computing has improved communication, making it easier and faster for people to connect globally. Social media platforms like Facebook and X (Twitter) have not only facilitated personal connections but also enabled social movements, such as the #MeToo movement, to gain global traction. In Pakistan, social media played a crucial role in raising awareness about the 2014 Peshawar school attack, mobilizing support and solidarity.

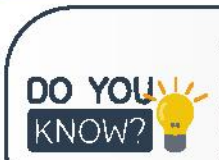
Computing has also driven economic growth by creating new industries and job opportunities. The rise of e-commerce platforms like Daraz has transformed traditional business models, allowing small businesses in Pakistan to reach customers nationwide and even internationally.

7.4.2 Negative Impacts

However, the impact of computing is not without its drawbacks. One of the major concerns is the digital divide, where a significant portion of the population lacks access to modern computing technologies. In Pakistan, the urban-rural divide is evident, with rural areas having limited access to reliable internet and computing devices, leading to unequal opportunities in education and employment. Another negative impact is the spread of misinformation and fake news, which can lead to social unrest.

Example: During the COVID-19 pandemic, misinformation about the virus and vaccines spread rapidly on social media, causing confusion and fear among the public. This highlights the need for digital literacy, so people can critically evaluate the information they encounter online.

Privacy concerns are also a significant issue, as the increased use of computing systems has led to the collection and storage of vast amounts of personal data. Without proper regulations, this data can be misused, leading to breaches of privacy and security. In Pakistan, incidents like the leakage of citizens' data from the National Database and Registration Authority (NADRA), underscore the importance of robust data protection measures.



Computing technology has enabled "Internet in a Box" projects that provide offline educational resources. In Pakistan, such initiatives have brought digital learning to remote areas without internet access, demonstrating how technology can bridge educational gaps in underserved regions.

7.5 Digital Citizenship and Ethical Considerations

Digital citizenship involves understanding how to behave responsibly and ethically when using digital technologies and the internet. It encompasses a range of behaviors and practices that help ensure a positive and secure online experience for everyone. By practicing good digital citizenship, individuals can protect themselves and others from harm, respect the rights of others, and contribute to a safe and inclusive digital environment.

Example: In Pakistan, students should learn to communicate respectfully in online forums and social media platforms. This means avoiding bullying or harassment and not spreading false information. It also involves understanding the importance of digital privacy and securing one's online accounts to prevent unauthorized access.

7.5.1 Responsible Digital Behavior

Responsible digital behavior means using technology and the internet in ways that are respectful and safe. This includes:

1. **Using Strong Passwords:** Create passwords that are difficult for others to guess.
   Example: Instead of using "password123", use a combination of letters, numbers, and symbols.
2. **Avoiding Phishing Scams:** Do not click on suspicious links or open emails from unknown sources that ask for personal information.
   Example: If you receive an email claiming to be from a bank asking for your account details, verify its authenticity before responding.

7.5.2 Ethical Use of Information

Ethical use of information involves handling data and content in a fair and lawful manner.

7.5.2.1 Responsible Data Sharing

Responsible data sharing means only sharing personal or sensitive information when absolutely necessary and ensuring that it is shared with trusted entities.

Example: When applying for a school scholarship online in Pakistan, students should provide their personal details only on secure and verified websites to prevent misuse of their information.

7.5.2.2 Ethical Issues

Ethical issues in information use include:

1. **Respecting Copyright:** Do not copy or use someone else's work without permission.
   Example: When writing a research paper, students should not copy text from online articles without citing the source.
2. **Avoiding Plagiarism:** Properly attribute ideas and information to their original authors to avoid plagiarism. This means mentioning the source of any quotes or ideas used in assignments.

7.5.3 Cybersecurity Awareness

Cybersecurity awareness involves understanding and implementing practices to protect oneself from online threats.

A Cyber Crime can be reported at NR3C-FIA available at https://www.nr3c.gov.pk

7.5.4 Collaborative Problem Solving

Collaborative problem solving involves working together with others to address challenges and achieve common goals.

7.5.4.1 Human-Machine Collaboration

Human-machine collaboration is about working with technology to solve problems. This includes:

1. **Using Tools:** Leverage software and digital tools to assist in tasks.
   Example: Students might use spreadsheet software to analyze data for a group or individual project.
2. **Combining Skills:** Integrate human skills with machine capabilities for better results.
   Example: Using data analysis tools to interpret complex data sets while applying human judgment to make decisions.

7.5.4.2 Teamwork and Knowledge Sharing

Teamwork and knowledge sharing involve collaborating with others and exchanging information:

1. **Group Projects:** Work together on assignments or projects, each contributing your expertise. Example: In a group project for a science class, students should collaborate and share their research findings to complete the assignment.
2. **Sharing Insights:** Exchange ideas and knowledge with peers to enhance learning. Participate in study groups or discussions to broaden your

understanding of the subject matter.

7.5.5 Creating Accessible Digital Content

Creating accessible digital content means designing and producing content that everyone can use, including people with disabilities.

7.5.5.1 Design for Accessibility

Designing for accessibility involves making digital content usable for all individuals, including those with disabilities:

1. **Readable Fonts:** Use clear and large fonts that are easy to read.
   Example: Choose fonts like Arial or Times New Roman and avoid overly decorative styles.
2. **Alternative Text for Images:** Provide descriptions for images so that visually impaired users can understand the content.
   Example: Include descriptive text for charts or graphs in a report.

7.5.5.2 User Feedback

User feedback is about gathering opinions from users to improve digital content:

1. **Surveys and Forms:** Use surveys to collect feedback on digital content and make necessary improvements.
   Example: After creating a website, ask users to provide feedback on their experience and make adjustments based on their suggestions.
2. **Direct Communication:** Engage with users directly to understand their needs and preferences.
   Example: Ask classmates for their input on a presentation and use their feedback to enhance its effectiveness.

In 2020, Pakistan introduced the Personal Data Protection Bill, which aims to protect citizens' data and ensure their privacy. This bill requires organizations to obtain explicit consent before collecting personal data and mandates the secure storage of such data.

EXERCISE

Multiple-Choice Questions (MCQs)

1. Option typically included in common Terms of Use clauses:
   a) User obligations
   b) Privacy and data use
   c) Product advertising
   d) Termination of service
2. The purpose of the "Limitations of Liability" clause in Terms of Use:
   a) Ensures full company responsibility
   b) Limits company's liability
   c) Provides user rights for damages
   d) Guarantees constant service availability
3. The type of harmful software that secretly monitors user activity:
   a) Spam
   b) Cookies
   c) Spyware
   d) Pharming
4. The threat involving user redirection to fake websites:
   a) Phishing
   b) Spam
   c) Spyware
   d) Pharming
5. The impact of the digital divide on education:
   a) Improves learning for all
   b) No educational impact
   c) Creates inequality in digital resource access
   d) Replaces traditional teaching methods
6. The reason for understanding bias during information evaluation:
   a) Ignoring other viewpoints
   b) Recognizing the source's agenda
   c) Validating all sources equally
   d) Avoiding evaluation altogether
7. The positive societal impact of computing systems:
   a) Spread of misinformation
   b) Improved information accessibility
   c) Heightened privacy concerns
   d) Widened technology gap
8. The practice considered ethical when using information:
   a) Copying content without permission
   b) Respecting copyright and avoiding plagiarism
   c) Ignoring source attribution
   d) Using unverified information

9. The behavior considered responsible digital conduct:
    a) Using secure websites
    b) Spreading false info online
    c) Respecting online privacy
    d) Reporting suspicious activity1

Short Questions

1. Why is it important for users to understand Terms of Use?
2. Differentiate between phishing and pharming.
3. Identify two impacts of the digital divide on social and civic participation.
4. What are the key steps involved in evaluating information sources?
5. How does responsible data sharing contribute to ethical use of information?

Long Question

1. Explain the common clauses found in Terms of Use and describe how they protect both the service provider and the user.
2. Explain the concept of bridging the digital divide and discuss the roles of government initiatives in addressing this issue. Provide relevant examples from Pakistan.
3. Explain how critical thinking skills contribute to responsible information utilization. Provide examples of how these skills can be applied in real-life scenarios.
4. Discuss the importance of collaborative problem solving in a digital environment and provide examples of how human-machine collaboration can enhance this process.