The Ethics of Internet World

Chapter includes:

- Types of infringement in the digital space
- Internet ethics
- The impact of computers and the Internet on society
- Internet and information security

4-1 Introduction:

Technology in all its forms and types, from computers, the Internet, regular and smart mobile phones, digital cameras and video games, exists to facilitate and facilitate the lives and well-being of people and society. But the current reality confirms that there are problems that have arisen with it. There are those who are ignorant or ignorant of the basic goals of inventing and developing this technology, and they do not know how to use it in a sound ethical use. An example of this is the unethical use of the Internet such as:

Assaulting privacy, information espionage, stealing personal identities, violating intellectual property rights, and some stealing the intellectual products of others from research and articles and attributing it to themselves.

Theft of bank funds and funds via electronic transfer, or theft or reproduction of programs.

Destroying, removing and distorting data and information, tampering with them, or sabotaging and electronic destruction of information systems.

Promote non-targeted harmful material and content via e-mail messages or through websites or chat rooms (chat), or in offending and defaming people, as some work to transform the Internet into a means of threatening psychological information operations, such as lying, distorting information, Misrepresentation of facts, public criticism, and slander.

- Using cell phones to annoy others with contempt, or posting immoral pictures on these phone's cameras, or using them to spread rumors.
- Harassment through hate and harassment messages (spam, which is considered fraud, and others for visiting pornographic sites, and only about 5% of it are advertisements and advertisements for legal work.

Accordingly, the Internet has formed a new channel for exporting problems to the information society in developed countries and the Arab world alike, which required the development of new laws that would control this network by controlling the pattern of dealing with its technologies and contents. Many international bodies and organizations specialized in the field have sought to impose legislation and laws to regulate the vast amount of information flowing on the Internet. For this purpose, many terms have appeared, whose meaning still exists until now. Despite the different technologies and practices on the Internet, the forms of controlling Internet ethics remain the goal of making its use the protection of the public good and directing the use towards good.

These ethics may be to control the relationship between the individual using the technology and him or between him and others, in addition to controlling the existing ethics between the user and the physical components of technology, which includes ensuring the safety of devices and their contents from sabotage and destruction.

4-2 Internet law and types of violations in the digital space

Internet law is a set of legal rules related to Internet information technology systems, and it is called the term Cyber law, and it differs in term from old terms such as computer law and informatics law (the latter does not concern Internet issues, but rather were launched as labels in the pre-establishment of Internet law in 1998). Internet law includes all laws governing the Internet and its use around the world, as well as enacting a wide range of cases, new laws and courts to keep pace with new developments in the world of the Internet, for example the Internet law includes laws that deal with rights of defamation, content and expression, copyright, trademarks, electronic contracts, violations of privacy and marketing ....

As for infringements in the digital space (the Internet), they are:

Online defamation can be a serious problem for both individuals and companies as it can quickly reach a wider audience. In order to determine who is responsible for defamation, there is a need to use technical expertise to locate the server used, as well as to protect the right to express an opinion and respond.

- Intellectual property crimes and the theft and reproduction of software: includes the theft of software and its illegal reproduction, whether commercial, scientific or military, as this software represents a cumulative research effort, and its theft causes a great loss to the original companies and huge profits for copyists.

- Fraud and theft of assets: This includes marketing fraud, identity theft, fraud in communications, and theft of money through electronic transfer of individuals and banks.

- Espionage: Espionage for the purpose of obtaining important information of a personal and confidential nature.

- Illicit gain: through fake ads and pornography.

- Hacking and damaging the computer and electronic sabotage: This includes electronically booby-trapped messages, sabotaging and destroying information, wiping and distorting data, and disrupting the computer using viruses by computer hackers.

- Emotional fraud: Fraud and fraud by pretending to love and wander through the Internet is one of the easiest acts of deception, and publishing data for fictitious characters who wish to have emotional encounters to encourage site readers to subscribe to its services and to attract clients, and by soliciting humanitarian and satisfactory campaigns for the purpose of material gain.

Privacy violations there are many companies and methods that can track a person's Internet use. Companies use cookies on their websites. Targeted emails and advertisements are electronically monitored based on the sites visited and the topics discussed in the emails and social media. There are Internet laws that govern the privacy rights of an individual or business that has a presence on the Internet that must be respected.

4-3 Techno-Ethics

Information technology has an ethic that everyone who uses or deals with it must adhere to. The use of technology of all kinds, including phones, computers, the Internet, televisions, videos, tapes, cameras ... must be subject to laws, regulations and ethics. Perhaps one of the simplest ethics of technology is not to use it to annoy others, harm them, corrupt them, or steal their money and attack their personal and social freedoms, as technology is only found to serve the person and his well-being, facilitate his life, work for his comfort, happiness and development, and raise The quality of his work and his industries, and speeding up the process of his communication and communication, whether with his family, relatives, friends or the world around him. Information technology has come to create ethical branches of a character that fit this new world, namely:

1. The values of the information age, Info-Ethics: related to science, media, education and culture, and deals with important issues such as: accuracy of data, nature and content of information, responsibility of software developers that their users need, and the dissemination of useful and public information.

2. Media-Ethics: Media ethics is a branch of applied ethics that relates to the ethical principles and standards of the media, and includes broadcast media, films, theater, arts, print media, the Internet, and matters related to the truthfulness and completeness of the content of the media message and ensuring the transparency of information.

3. Internet-Ethics: Internet ethics includes not exploiting remote dialogue for the purpose of camouflaging and disguising, and fueling hatred due to the multiplicity of beliefs and ideas, respecting the rules of civilized behavior and not distorting facts. The ethical rules of the Internet determine how to deal with the network to combat space crime of all kinds, and oblige Internet users to respect self-regulations and auxiliary regulations, while developing their moral values and their own sense of the need to exploit the network for their benefit and the benefit of others. Self-regulation regulations emerged with the transformation of the Internet into an ideology of linking cultures and languages, abolishing time and space boundaries and exchanging information in accordance with legal legislations.

The self-regulatory regulations include:

a- Internet Content Regulation Regulations La régulation de contenus: It means organizing the content of the sites and the information that they organize from forms of cultural, ethnic and ethical pollution to block the reception of virtual sex images of "Les pornographies", the exploitation of teenagers through pornographic images and the propaganda of religious and ethnic intolerance through Spam and sites prepared for that.

b- La régulation des techniques Internet regulations: The Internet depends on an infrastructure of technologies, so it requires protection from any attempt to sabotage such as controlling cookies, which is one of the interference with privacy on the Internet, and it requires setting up a regulation of technologies to modify the behavior of users.

c- The ethical rules for Internet users: Les règles Netiquette: It is a set of rules agreed upon for Internet users to ensure the proper use by them of the global network, and to ensure the security of the network from ethnic conflicts and encroachments. These rules differ from one country to another according to the cultural factor of each region, and despite the different forms of regulations governing Internet ethics, the purpose of them is the same, which is to protect the Internet from everything that tries to threaten its security and uses it against others.

4-4 Etiquette and ethics for dealing with the Internet:

Controlling the ethics of the Internet is a very important issue because of the guarantee it carries to maintain a safe, clean and free network from all encroachments, which may affect the dignity, reputation, privacy, expression and freedom of information flow on the World Wide Web. In addition to protecting it from all kinds of space crimes, it is imperative to continuously monitor the sites, establish Internet ethics enact laws and conclude international agreements appropriate to the content of the global network, which requires the development of site supervisors to monitor them. The responsibility for controlling Internet ethics relates to informatics professionals and then to community members through dialogue within the site, as well as to societies and organizations interested in the Internet. In general, the question of ethics of the network (the Internet) is based on the self-authority, which is the conscience of man and his first moral authority, which is based on the principle of compliance with laws. From this standpoint came the concept of Internet etiquette derived from Net Etiquette (i.e. polite behavior when using the Internet) and its aim is to make the Internet an effective and elegant means of communication and exchange of useful information and knowledge.

Always remember that the Internet is a means of communication, through which it is possible to send messages, talk to others, present your opinions and ideas, and see the opinions and ideas of others. And when using any means of

The process of ethical dealing with the Internet can be summarized in:

1. Seeking beneficial knowledge, and working to find and nurture a good Internet user. The Internet and the data and information it provides change for the better in the economic, political and social fields ... etc. Internet information is for communication and knowledge of the national, regional and global levels.
2. Investigate truthfulness, reliability and honesty in requesting data and information. And take the necessary measures to protect individuals, institutions and society from harmful and polluting data and information.
3. Internet information for publishing, viewing and making use of, and not for silence.
4. Protection of intellectual property rights and compliance with cyber laws.
5. Ensuring the security and flow of data and information, and observing and respecting privacy. And documenting the information we get from the Internet by stating the location and the date the information was taken.
6. Respect others, respect their ideas and opinions, do not mock them, avoid insulting them or hurt their feelings when communicating via the Internet, and tolerate others in the event that they are offended.
7. Staying away from forgery and deception because they are two abhorrent matters that contradict religion, norms and good morals.
8. Observing the agreed conservative methods and words, especially as Internet users belong to a variety of civilizations and environments.
9. Avoid unwanted formulas when writing a letter in the English language (for example, writing the entire document in large letters, because this formula resembles a rebuke and severe reproach).
10. Deal honestly with electronic documents that arrive by mistake in the e-mail box, return them to the senders, and not exploit their contents.
11. Avoid harming others, such as sending viruses or harmful materials.
12. Provide assistance, advice and guidance to those who request it on the Internet.
13. Check the Internet sites' trends and ideas and the degree to which they maintain the privacy of their members.

4-5 Effects of Negative Internet Use on Life and Society:

Talking about the harms of the Internet does not mean ignoring it and reluctance to it, but what is required is rationalization and moderate use to achieve specific and clear purposes. It is also necessary to give the importance of family control and direct children towards the optimal use of the network, and set rules and controls for themselves before dealing with this virtual world. We include the most important areas that include the effects of negative Internet use on life and society:

A- Health effects:

1- Damage to hands and fingers from excessive use of the mouse and touch screens.
2- Damage to the eye as a result of radiation emitted by computer screens, phones and smart devices.
3- Damage to the spine and legs as a result of how to sit and how long it takes against the computer.
4- Damage to the ears of loudspeaker users.
5- Associated damages such as obesity and other diseases it causes.
6- Addiction disrupts the sleep of the owner due to the increased time of use of the Internet; Most addicts spend long hours at night surfing the Internet, which leads to a lack of sleep and this causes exhaustion in their work or studies for the next day, as this affects his immunity and makes him more susceptible to diseases.
The best protection for this is to stop working on the computer and the Internet from time to time, spread out the legs and ankles, and do some light exercise to speed up blood flow and limit working hours on the computer, especially at night.

b- Psychological effects:
1- Entering into an alternative imaginary world provided by the Internet, which causes short and long-term psychological effects, including tension and fatigue of the eye muscles, psychological anxiety, insomnia, psychological and social separation from the real world, and living in the midst of delusions and imagination for those who are addicted to the Internet.
2- Reducing the individual's ability to create a normal psychological personality capable of interacting with society and the reality around it.
3- Internet addiction, which is a disease that results from excessive use of the Internet that leads to disturbances in behavior. Friends or cafes provide him with internet use.
C- Social Effects:
1- Weak family control over children.
2- Influencing cultural identity, customs and values with this huge information invasion.
3- A marked withdrawal of the person from social interaction towards isolation, and this may lead to the loss of friends. Children especially suffer diseases as a result of their distance from the surrounding social circles, the most important of which is autism.
4- Family disintegration and rift due to the addict’s preoccupation with using the Internet and spending more time than spending with his family, which causes disruption in his family life.
5- Entry to sites such as drug sites, suicide education sites and sites of violence, and the resulting application of these things in our society by a group of community members, especially teenagers.

D-Moral Harm: The symptoms of moral harm appear by entering sites such as:
1- Gambling and alcohol sites.
2- Sites for calling for extremism.
3- Pornography and spreading homosexuality.
e-Economic damage: We can list the following economic damages, for example, but not limited to, and they are:
1- Internet money laundering.
2- Theft of bank accounts and credit cards.

3- Spoiling and destroying memories, programs and electronic systems, and spoiling information by spreading viruses.

F-Security damage: These damages are as follows:

1- Forgery and theft of information.

2- Espionage, fraud and fraud.

3- Teaching how to make bombs and explosives, and how to commit crimes against individuals and society.

i-Educational damages:

1- When technology is limited to obtaining information, this leads to depriving students of traditional educational methods whose effects include direct dialogue between teacher and student, and the emotional and mental response that occurs as a result of that.

2- Lack of order in information on the Internet, as well as the absence of a direct relationship between Internet information and school curricula.

-h Problems at work:

1- The employee or worker may waste some of his work time using the Internet outside his workplace.

2- Staying awake at all hours of the night, leading to a decrease in his performance at work.

4-6 Information and Internet Security

The Internet is a double-edged sword, as it is an entrance to many useful things, and also opens the way for many harmful things to enter the computer system, so the rapid spread of the computer and the Internet has led to the emergence of many problems related to how to protect data and secure protection against hackers and what are known as viruses, viruses. Those that cause the user to pay dearly from material and information damages, and how to prevent and deal with them through the acquisition of the latest security technologies and taking preventive measures to ensure comprehensive protection for programs, devices and data. There are many security issues that must be taken care of to maintain the safety of operating computers and networks.

4-6-1 Information Security:

It means keeping the information under the direct and complete control of the user or the party that owns it, that is, the inability to access it by anyone else without prior permission, and that the user is aware of the risks involved in allowing someone to access computer or network information, as most People want to keep their personal information like passwords and credit card information private and not accessible to others. Many people do not realize that some information may seem simple or meaningless to them, as it may mean a lot to other people, especially if it is combined with other information. For example, a company wishing to obtain personal information about you for marketing purposes can buy this information from a person who collects it through illegally accessing a computer such as the address of a postal account for the purpose of sending advertisements about their products. It is important to know that even if you do not give information to anyone over the Internet, some may be able to access the computer system to obtain the information they need without the knowledge or permission of the user.

4-6-2 Vulnerabilities in the Internet:

The Internet may be exposed to defects and weaknesses in its defenses, and this weakness may be caused by software errors and defects in the system design. The reason for some of the weaknesses is due to incorrect data entry, as it often allows the execution of direct commands or SQL statements, and vulnerabilities often allow the attacker to circumvent the program. There are a number of vulnerabilities that a computer or network is vulnerable to. Among the most common are data entry validation errors such as programming errors resulting from formatting text codes, wrong handling of program variable codes, entering SQL statements and embedding script texts, so these codes are interpreted incorrectly. Another common vulnerability is cache overflow, as well as symbolic link files (Symlinks). And sometimes the programmer fails to verify the size of the stored data, as this leads to a flood of data and may expose it to difficult access, and there may be weaknesses in all operating systems (Windows, Macintosh, Linux…) themselves. Vulnerabilities in the network and servers can be examined by conducting a special test on them through which servers, web pages and firewalls are examined to see the extent of their exposure to vulnerabilities, and programs can also be installed to check vulnerabilities from the Internet.

4-6-3 Security problems:

Spying on network data and intercepting information that travels between the server and the browser can become possible if you leave the network or servers open and their vulnerabilities exposed. The security problem occurs when a user's computer system is penetrated by a hacker or damaged by viruses or malicious programs. The most targeted people for security breaches are the people who surf the Internet, as the hack causes annoying problems such as slow and interrupted browsing movements at regular intervals, or inability to access data, and in the worst case, the user's personal information can be compromised.

In the event of software errors or misconfigured settings in the network server, it may allow unauthorized users to remotely access confidential documents containing personal information or obtain information about the server's host computer, allowing for a breach of the system. These people can also execute commands on the host server machine, which can modify the system and launch attacks called dumping attacks (DoS), which lead to the temporary disruption of the machine, and are also aimed at slowing down or paralyzing traffic over the network. Also, through DDoS attacks, the attacker uses a number of computers he has taken over to attack another computer or computers. The main program of distributed dumping attacks is installed on a computer using a stolen account.

4-6-4 Computer weakness (fragility):

Vulnerability refers to a vulnerability that allows a hacker to reduce the information integrity of an electronic system. The weakness here is the intersection of three elements:

1. Defect in the system.
2. A penetrator reaches this defect.
3. The ability of this hacker to exploit this defect.

A hacker is a person who creates and modifies software and computer components in order to damage or steal them. This term has become a negative connotation, as it came to refer to a person who exploits a computer system by obtaining unauthorized access to the systems and carrying out unwanted and illegal operations. However, this term (hacker) can be given to a person who uses his skills to develop computer software, manage computer systems, and what is related to computer security.

4-6-5 Computer and Information Protection:

The computer and the information inside it can be protected by using suitable programs to combat malicious programs, the consequences of which may be devastating to the computer. And constant caution and care to protect the computer system so that it is not vulnerable to attacks because of its weaknesses. Effective programs and means can be used to enhance the security of internet and computer use, including:

Physical protection measures: such as keeping the computer (especially the laptop) in a safe place.

- Protecting the computer with a password: With regular change of the password, especially if someone sees it, or even if he feels

The user has that someone has access to it. And not to write the user's passwords anywhere, but rather save them. It is a good idea to turn off the computer when the user is away from it.

Updates: Keep all software up to date, including the operating program in use. Including automatic updating, which checks daily for updates when the computer starts.

Antivirus use and update: It is a program used to prevent, detect and remove malicious software, including viruses, worms and Trojan horses. Such programs can prevent and remove spyware and other forms of malware.

Firewall: or what is known as a firewall, and it varies according to the user's needs, and it is either a program or a device that protects the computer while it is connected to the Internet from risks, as the firewall checks all the information and data coming from the Internet or from any other network, Then, it allows it to pass through and enter the computer, if it is compatible with the firewall settings, or it excludes and expels it if it is from malicious programs such as viruses and spyware, or if it is incompatible with the firewall settings, so the firewall is a limit Separator between the computer and the Internet.

The firewall is also used to protect the network and the server from hackers, and separates trusted areas in computer networks, and it is a dedicated tool or program on another computer, which in turn monitors the processes that go through the network and only allows the passage of a program according to certain rules. However, it should be ensured that it does an effective filtering of all the things you need, and if not, then a stronger firewall should be purchased.

- Packet Sniffers network data monitoring programs: An effective way to monitor traffic across the network using a network data monitoring program, through which data entering and leaving is collected, and it is a method that can be useful in detecting intrusion attempts across the network, and can also be used to analyze problems Network, filtering and blocking suspicious content from entering the network.

Coding: Encryption is the encoding of data so that it cannot be read from anyone who does not have a password to decode that data. Encryption processes the data using irreversible mathematical operations.

- Wireless network security: Wireless networks are spreading everywhere and expanding rapidly, and there are many security issues associated with these wireless networks, and anyone can access the wireless network from anywhere that the wireless connection is available. In addition to the general security measures used to protect wireless networks, it is necessary to follow general principles to provide the best level of security for your wireless network.

The wireless network is protected by using a different encryption protocol (such as WEP Encryption Protocol). This protocol works by including a 64 or 128-bit shared key between clients and the entry point, and then this key is used to encrypt and decrypt the data between them, and this provides sufficient security for home networks. Refer to the documentation for wireless devices to learn how to activate and set up the Wireless Encryption Protocol (WEP) on the network. As for corporate environments, this WEP should only be considered as a starting point for security arrangements, and companies should work to raise their wireless networks to the most secure WPA level.