ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

Ethical Aspects of Information and Communication Technologies (ICT)

Dheya Al-Othmany[1*]

[1] *Faculty of Engineering, King Abdulaziz University, Jeddah, SAUDI ARABIA.*
**Corresponding Author (Email: dothmany@kau.edu.sa).*

Paper ID: 13A3L

Volume 13 Issue 3

Received 14 October 2021
Received in revised form 21 January 2022
Accepted 30 January 2022
Available online 05 February 2022

Keywords:
ICT; IFIP code of ethics; Privacy protection; Data security; Plagiarism; Virtual university; Absolute security; Lisbon Treaty; Freedom of Speech; Translated plagiarism; Codes of ethics.

Abstract

This paper discusses and analyzes various aspects of ethics in ICT, and the IFIP (International Federation for Information Processing) code of ethics. The focused aspects of ethics in ICT include privacy protection, data security, Lisbon Treaty, freedom of speech, intellectual property, virtual university (ICT and education), virtual experiments and surveys, plagiarism: how to use ICT to detect and prevent it, ICT availability & problem of inequality, and ethics in the Business classroom. It has further shed light on the Lisbon Treaty and the African Commission on Human and Peoples' Rights. Referring to the IFIP, the author supports only a generic framework for the codes of its member societies, recommending that they develop their own codes within that framework. The author holds the view that any violations of ethics should be made punishable within the parameters of each culture and society.

Disciplinary: Information Ethics, Law, and Policy.

Cite This Article:

Al-Othmany, D. (2022). Ethical Aspects and Information and Communication Technologies (ICT). *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 13*(3), 13A3L, 1-10. http://TUENGR.COM/V13/13A3L.pdf DOI: 10.14456/ITJEMAST.2022.33

1 Introduction

The main objective of this paper is to discuss and analyze various aspects of **ethics in ICT**, and the IFIP (International Federation for Information Processing) code of ethics. It focuses on the following aspects of ethics in ICT: privacy protection; data security; Lisbon Treaty; freedom of speech; intellectual property; virtual university (ICT and education); virtual experiments and surveys; and plagiarism: how to use ICT to detect and prevent it; ICT availability & problem of inequality; and ethics in the Business classroom. It further sheds light on the Lisbon Treaty and the African Commission on Human and Peoples' Rights.

The Information and Communication Technologies (ICT) sector is faced with the fact that there are very different ideas of what is a "good" or "bad" use of ICT, e.g. concerning privacy issues,

intellectual property rights, or the freedom of information. Only an open discourse can create a common understanding of common principles. For this reason, the IFIP (International Federation for Information Processing) has never tried to define a "global standard" but only a generic framework for the codes of its member societies, recommending that they develop their codes within that framework. Under the diversity of histories, cultures, social and political backgrounds of IFIP member Societies, the IFIP regards it as essential that Codes of Ethics or Conduct (or Guidelines) should always be developed and adopted within the member Societies themselves. [1] Finally, the paper will seek to answer the following question: Is the teaching of ethics in the classroom feasible?

2 Ethical issues

In this paper, the author has reviewed and analyzed some of the issues involved in ethics in ICT.

2.1 Privacy Protection

Database technology and various surveillance technologies have given rise to a broad discussion about the right to one's own data. Privacy protection has now been included in the laws of most countries. The debate over basic issues, however, such as under what conditions sensitive data can be stored, processed and passed on to others and which data are considered sensitive could go on for a long time yet. A new challenge for privacy protection is pervasive computing, which can be used for such purposes as highly efficient surveillance.

Information Technologies have invaded many aspects of people's daily lives, creating new possibilities but also raising concerns in terms of privacy and trust. Protecting the privacy of individuals is one of the main challenges of the Information Society but it is difficult to achieve as individuals constantly leave digital traces of their lives, often without even being aware of this. If an unauthorized entity gathers these digital traces, he (or she) can use them for malicious purposes ranging from targeted spam to profiling, and even identity theft. From the technology viewpoint, several Privacy Enhancing Technologies (PETs) and Privacy-Aware Architectures have been proposed. So far, these technologies have not stimulated a strong public interest and are not widely used yet. However, the European Commission is putting forward the "privacy by design" principle, which integrates the privacy issues in the design phase of a system or application.

Security and trust can be seen as complementary requirements to privacy. Large-scale adoption of digital devices, like in eHealth and smart cities, requires trustworthy products and communication. These requirements are not (always) completely understood and off-the-shelf solutions could not fulfill the security, trust, and privacy needs. There is a large gap between what is applied, usability requirements, and the right level of security. This gap represents a strategic opportunity where European players have recognized know-how and where leadership should be leveraged and nurtured [2].

Mobile devices play an important role in our everyday lives, not only by enabling us to communicate but also by providing access to a large variety of pervasive services. While the scope of mobile security is wide, the project is focused on the application of mobile devices to secure access to services, such as financial and e-government services, or pervasive ones such as e-health for personal monitoring. The focus is on the protection of the device itself to ensure secure access to the services.

Cloud-based infrastructures enable seamless access to services and global availability of information, giving enormous potential for improved levels of services as well as cost reductions. Data security concerns form one of the main hindrances for cloud-based solutions. In this activity, we aim to provide privacy protection and establish trust in the cloud by providing trust and security mechanisms suitable for heterogeneous distributed service networks.

2.2 Scalable Security Intelligence

The main objective of this activity is to develop a new security service, based on the application of business intelligence technology to the field of security. This service will provide personalised security analysis and reports that can help a company to plan the deployment of security patches based on its own risk assessment and not on generic security warnings. The service will be offered also to smartphone users to detect and report in real-time attacks on normal user activity.

2.3 Security and Privacy Location-based Services

The advent of ubiquitous devices equipped with geo-located capacities such as smartphones has led to the growing development of location-based services (LBS) and the massive collection of the mobility data of individuals. In this activity, we address questions of secure and privacy-preserving implementations of location-based services, for instance in traffic monitoring, and the development of tools that help users to prevent/limit privacy leaks [2].

2.4 Data Security

When networks were connected to the Internet, the door was opened for outsiders to intrude into computer systems. Because there is always someone who has to try out every technical possibility, hacking, viruses and other forms of intrusion have become a daily appearance. One consequence of the trade-off between security and usability is that because of the unmastered complexity of large software systems (especially operating systems), it will not be possible to have absolute security. No other issue in ICT ethics shows so clearly that the challenge is to find consensus about the borderline between "good" and "bad" in formerly undeveloped fields of action. When does fun turn into criminal abuse? Is hacking without the intention to gain a material advantage destructive or useful for society? Should information about safety gaps in operating systems or the anatomy of computer viruses be published or not?

Viruses, Spyware, Trojans and Worms are all forms of malware that replicate, spread, steal personal information, and inflict damage to computers. The private firewall detects activity

characteristic of malware infection such as attempts to access protected file objects, execution of WinAPI functions, and initiation of unknown processes, among others. Once detected, a private firewall blocks the malware and alerts you of the security incident [3].

By simple definition, a rootkit is a collection of software tools that an intruder can install on a computer to execute whatever criminal activity they have in mind. Rootkits are a particularly tricky form of malware to detect and defend against, as they are nearly invisible to most types of systems monitoring software. They allow an attacker to execute malicious programs invisibly as the rootkit is able to conceal files, running processes, and/or system data. Rootkits are a growing problem. According to Microsoft, approximately 20 percent of the malware deleted by its malicious software removal tool are rootkits.

A private firewall can guard against rootkit-related attacks on many levels. A private firewall can detect when a rootkit is being installed by identifying when a registry key value is being modified. A private firewall can also detect rootkit activity based on the process, WinAPI call, or executable that is launched as an output of the rootkit's payload. [3]

2.5 Hacker Defense

Hackers are criminals who leverage system vulnerabilities, social engineering, and other techniques to break into computer systems for amusement, theft, vandalism, or other crime. The private firewall prevents hacker attacks by restricting access to unauthorized areas of your computer and controlling how applications, processes, and other system features operate. In addition, a private firewall provides additional layers of protection through system and email anomaly detection components that baseline normal computer operation and detect unacceptable deviations from typical use caused by intrusion (hackers) and viruses, spyware, and other forms of malware. Hackers and their techniques continually evolve and become more effective at hiding. No security solution provides 100% protection from attacks, but a private firewall offers unique capabilities focused on deviations of typical behavior and can therefore adapt and evolve along with the threats themselves. [3]

2.6 The Lisbon Treaty: Taking Data Protection into the 21st Century?

The Lisbon Treaty, which has been described as the Treaty that takes Europe into the 21st century, can be said to represent at the same time success and challenge for data protection. On the one hand, its provisions are not revolutionary but mark an important and visible consolidation in the European Union primary law of the data protection *acquis* developed in Europe over the last 27 years. In this perspective, the Lisbon Treaty pinpoints some crucial elements of the fundamental right to the protection of personal data, within the context of the increased protection of fundamental rights. Also, the need for independent supervision is solidly carved in primary law.

On the other hand, it develops instruments for stronger and more homogeneous data protection across the different activities of the European Union, with greater involvement of the

European Parliament, also with regard to international agreements. When it comes to finding a delicate balance between conflicting values in crucial areas such as police and judicial cooperation, political negotiations are now likely to play a more important role than litigation before the Court of Justice.

In this perspective, the new tools laid down by the Lisbon Treaty represent a challenge for data protection in the 21st century. Many horizons are possible with a view to building a data protection legal framework that is comprehensive and general but at the same time able to accommodate the specificities of certain areas. Many efforts are required to address the growing demand for security and the immense possibilities offered by new technologies. Dialogue and communication, also at the global level, are needed to involve citizens and explain to them the important political choices made about their privacy.

Therefore, the new legal framework of the European Union is a challenge for the legislator, but also for data protection authorities, that will be called not only to supervise rules having an increasing degree of complexity but also to advise the legislator in making difficult and important choices in new fields of activities. [4]

2.7 Freedom of Speech

In many countries today, individuals now have an unprecedented ability to exchange ideas and information that bypass traditional media and communications controls. SMSs and instant messaging allow for easy and quick sharing of information. Chat rooms and blogs provide people with opportunities to meet and discuss current topical issues in a way that had never been available before except in small rooms or under tight supervision. Easy access and sharing of photographs and video can convey information in more powerful ways than before. These can have significant impacts on how current events are understood and discussed. For example in Kenya, Internet forums and SMS were widely used to disseminate information about the disputed 2007 election that the mass media was prevented from discussing.

In an attempt to prevent these technologies from undermining their control, many governments have imposed existing restrictions on speech, or adopted new legal and technical measures on these new communications technologies.

Under international standards as set by the UN Human Rights Committee, any limitations on freedom of expression must satisfy that the interference is provided in law and is clear and accessible. The interference must pursue a legitimate aim as set out under Article 19 (3) of the ICCPR and the restrictions must be necessary and proportionate.

This recognition of the importance of the right is echoed in regional instruments in Africa, Europe, and the Americas. Article 9 of the African (Banjul) Charter on Human and Peoples' Rights states: 1. Every individual shall have the right to receive information. 2. Every individual shall have the right to express and disseminate his opinions within the law. The African Commission on Human and Peoples' Rights set up under the charter has similarly held that freedom of expression is fundamental: [5]

Freedom of Expression is a basic human right, vital to an individual's personal development, political consciousness, and participation in the conduct of public affairs in his country. The African Commission further detailed these rights in the Declaration of Principles on Freedom of Expression in Africa. The principles adopt a broad recognition of freedom of expression across technologies and borders: Freedom of expression and information, including the right to seek, receive and impart information and ideas, either orally, in writing or print, in the form of art, or through any other form of communication, including across frontiers, is a fundamental and inalienable human right and an indispensable component of democracy.

The African Commission on Human and Peoples' Rights has also appointed a Special Rapporteur on Freedom of Expression with a mandate to investigate and promote freedom of expression across the continent.

The right of freedom of expression is also found in nearly every national constitution in Africa. For example, Article 32 of the Constitution of Angola (1992) states: (1) Freedom of expression, assembly, demonstration and all other forms of expression shall be guaranteed. (2) The exercise of the rights set out in the foregoing clause shall be regulated by law. (3) Groupings whose aims or activities are contrary to the fundamental principles set out in Article 158 of the Constitutional Law and penal laws, and those that, even indirectly, pursue political objectives through organizations of a military, paramilitary, or militarized character, secret organizations and those with racist, fascist or tribalist ideologies shall be prohibited.

Article 35 further states: (1) Freedom of the press shall be guaranteed and may not be subject to any censorship, especially political, ideological, or artistic. (2) The manner of the exercise of freedom of the press and adequate provisions to prevent and punish any abuse thereof shall be regulated by law.

The Constitution of Sierra Leone similarly has a broad recognition of the rights of expression. Article 25 (1) states: (1) Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, and the said freedom includes the freedom to hold opinions and to receive and impart ideas and information without interference, freedom from interference with his correspondence, freedom to own, establish and operate any medium for the dissemination of information, ideas and opinions, and academic freedom in institutions of learning. [5]

2.8 Intellectual Property

The World Wide Web has simplified the use of text, images, and sounds and thus made it questionable as to whether intellectual property rights can still be enforced. It is hard to distinguish pirated copies and plagiarism from legitimate uses of information. One reaction to this problem is a trend to stronger regulation, as can be seen in how the EU Directive 2001/29/EG of the European Parliament on "Harmonization of Certain Aspects of Intellectual Property Law..." is turning out. It is feared that regulation that is too strong will run contrary to the "primary interest of science,

namely to let knowledge become public." (Kuhlen, 2001) Then, the excitement about the contribution of the Internet to free access to information and knowledge could become negative in the long run. The "innovation commons" referred to by Lessig [12] would be destroyed or severely hampered. In the United States, the 1998 Digital Millennium Copyright Act (DMCA) has come up against serious criticism, as have its provisions for Digital Rights Management (DRM).

2.9 Virtual University: ICT and Education

Voronkov [6] examines the use of ICTs in education and associates ICTs with expanding new cultural, social, cognitive, and professional horizons of education at national, regional, and global levels. (p. 10) Rapid growth in the use of ICTs in education, the establishment of open and virtual universities offering courses to hundreds of thousands of students worldwide provide ample proof of global integration. (p. 19) He argues that many hundred thousand students engaged in virtual forms of education may serve to undermine the academic process, erode the academic culture, and lessen the quality of education. The nature and scale of these existing and potential pitfalls and possible ways to overcome them require concerted efforts at every organizational level ranging from individual universities and their consortia to the world community. A qualitatively new type of international cooperation is required – not only to define and analyze the situation but also to take action such as by developing specific projects that radically reform education to ensure sustainable development. [6]

2.10 Virtual Experiments and Surveys

Is it possible to conduct virtual experiments and surveys? On traditional university campuses, there are "ethics committees" to ensure the following issues: ethical principles, safe research, consent and confidentiality, and obtaining ethical approval. These bodies are comprised of academics from within the institution and they monitor research activity at undergraduate and graduate levels. In addition to approving applications to conduct research, they also hear appeals where approval has not been granted, provide guidance on unclear cases, and refer cases of research misconduct to higher institutional authority. Their procedures are recorded in writing and are available for public scrutiny. The question arises as to how to ensure ethical is research (experiments and surveys conducted via e-mail) in online university education. [7]

The validity of data can be questionable. Further, Walther [8] raises the issues such as research methods and human subjects.

The widespread use of the Internet provides new vantage points from which to observe conventional behavior, views of new kinds of behavior, and new tools with which to observe it all. Accompanying these opportunities come two specific concerns about research approaches: how new research methods using the Internet may or may not affect the ethical protections to which human subjects are entitled, and the validity of data collected using the Internet.

2.11 Plagiarism: How to use ICT to Detect and Prevent It?

With the development of ICT, plagiarism becomes an ever more serious problem in the academic community. According to Pupovac [9], plagiarism rates among students are quite high and students mostly ignore or allow plagiarism because of a lack of knowledge, lack of consequences, or simply because ICT makes plagiarism easy to commit.

The findings of the studies presented in this paper indicate that strict policies against plagiarism need to be introduced at universities. We believe that the problem of plagiarism should be brought to public attention and discussed at a higher level and that effective measures against plagiarism should be implemented. The prevalence of plagiarism among students and their attitudes towards plagiarism are influenced by the cultural environment as well as the academic setting. In multicultural communities, such as the European community, it is necessary to investigate and compare academic behavior in different countries to establish equivalent standards in education across Europe.

The studies revealed that plagiarism is deeply rooted in the academic environment of some European universities. Students are generally aware that plagiarism is a form of dishonest behavior, but they still commit it, especially if they have a tight deadline or too much work to do and not enough time. In such circumstances, most students exploit the benefits of ICT and commit cyber-plagiarism. Easily accessible information on the internet, the development of IT and the simple copy/paste command facilitate plagiarism [9].

Websites that sell student essays, master's theses and doctoral dissertations as ready-made commodities are a new and increasingly worrying problem.

Most students believe that plagiarism will not be detected by their tutors, so they resort to it despite warnings and rules against it. According to the results of the Croatian study, only an objective plagiarism detection method and penalty for perpetrators will deter students from plagiarizing. This finding is consistent with the results of another study conducted among students in the USA. Although it is easier to plagiarize in the age of ICT, it is also easier to detect and measure plagiarism. Plagiarism detection software (e.g., WCopyfind) and internet-based search engines (e.g., iTechnicate or EVE) can be used effectively in anti-plagiarism strategies in the academic environment. Faced with the obvious limitations of internet-based search engines in non-English contexts, some tools can reveal blatant plagiarism by comparing two or more texts, such as WCopyfind. Translated plagiarism is also a growing problem [9].

One of the important findings presented was that more than three-quarters of students would not report plagiarism to their tutors, even if they witnessed it. Some of the students probably feel that plagiarism is not a big deal" and others do not want to be whistleblowers. In an academic and scientific context, the question of reporting unethical and immoral behaviour to tutors is especially sensitive. Whistleblowers are often scorned by other students. Tutors and teachers should find methods to deter students from plagiarizing. Allowing or ignoring plagiarism among students does not contribute to better knowledge or education; on the contrary, it allows students

to find the easy way out. Once this kind of behaviour is encouraged, it cannot be expected that those who plagiarized become honourable members of scientific and academic society. Plagiarized data are misleading and allow the perpetrator to gain undeserved benefits. This type of behaviour should be recognized with the help of ICT and strongly discouraged. [9]

According to the study on academic misconduct in Croatia, significant predictors of misconduct include attitude toward cheating, the behaviour of the group that the student belongs to, and the year of studies. Senior students tend to cheat more often than junior students. Cultural environment and attitudes within wider society have a great influence on the prevalence and attitudes toward plagiarism. The results of the studies presented, revealing that almost 20% of students in Bulgaria and Croatia vs.7% in the UK find cheating on exams acceptable behaviour, are consistent with findings of a study on attitudes toward plagiarism and reporting plagiarism in Russia, the USA, the Netherlands, and Israel, which indicated that the tolerance toward academic misconduct was more pronounced in post-communist countries (Magnus, 2002). The cultural environment of post-communist countries, with a high rate of corruption, is characterized by a high level of tolerance toward cheating, which in turn creates inappropriate attitudes toward academic and scientific integrity.

One of the characteristics of an authoritarian regime is the lack of individual responsibility – one is allowed to do anything that society or leaders tolerate; maturity, independence, and responsibility are not encouraged; and individuals do not do wrong not because of their inner beliefs, but because of fear of punishment or authority. Considering that Europe as a multilingual and multicultural community strives to create the best possible education and scientific practice in all European countries, it is important to ensure a solid basis for such a development. Attempts at eradicating academic misconduct and rewarding creativity and real acquisition of knowledge in universities and schools will undoubtedly contribute to achieving this goal. Due to the vast cultural diversity in Europe, it will not be easy to harmonize academic standards and attitudes among different countries. However, the results of research such as that presented in this paper may provide a valuable contribution to the development of proper ethical education policies. [9]

2.12 ICT Availability and the Problem of Inequality

Alexeyeva [10] analyzed ICT availability and problem on inequality. With personal computers and computer networks, ICTs became accessible to an enormous number of people. The problem of a user-friendly computer acute in the 70s, seemed to have been resolved successfully by the end of 20th century. “User-friendly” and “barrier-free” technologies were rapidly growing. Computer-based multimedia integrated graphic, print, audio, video, and computer technologies into an easily accessible delivery system. It gave new impetus to ICT implementation in education. Now computers are considered to be suitable not only in learning mathematics, natural sciences, and engineering but in humanities and arts as well. Interactive video and CD-ROM technologies are incorporated into instructional units and lessons; a lot of undergraduate and graduate courses rely on the resources available on CD-ROM and the World Wide Web.

In many countries, governmental and non-governmental organizations pursue the policy aimed at widening the access to ICTs for larger numbers of individuals and groups; in this context, education is considered a sphere of special importance. Nevertheless, schools are unable to provide equal access to computer and communication technologies." [10]

2.13 Ethics in the Business Classroom

Although the inclusion of ethics in the business curriculum is becoming increasingly important, little is known about the impact classroom discussion of ethics has had on student sensitivity to ethical issues. Using both self-assessment and objective assessment measures, a study found that students who had been exposed to ethics in five or more classes considered themselves more knowledgeable about ethics and reported higher confidence in their ability to make ethical decisions than students who had less exposure to ethics in business courses. In addition, students with increased exposure to ethics in the classroom were found to be more sensitive to business ethics and consumer ethics than students with less classroom exposure. Areas for future research on this topic are suggested. [11]

3 Conclusion

In this paper, the author has reviewed and analyzed some of the issues involved in ethics in ICT, and the IFIP (International Federation for Information Processing) code of ethics. It has particularly focused on the following aspects of ethics in ICT: privacy protection; data security; Lisbon Treaty; freedom of speech; intellectual property; virtual university (ICT and education); virtual experiments and surveys; plagiarism: how to use ICT to detect and prevent it; ICT availability & problem of inequality; and Ethics in the Business classroom. It has further shed light on the Lisbon Treaty and the African Commission on Human and Peoples' Rights.

The author supports only a generic framework for the codes of its member societies, recommending that they develop their codes within that framework. The author holds the view that any violations of ethics should be made punishable within the parameters of each culture and society.

Further, the author views Ethics in ICT as growing in importance in a global society. The ICT sector as a driver of globalization contributes to removing geographical barriers between cultures and, in doing so, is faced with the fact that there are very different ideas of what is a "good" or "bad" use of ICT, e.g. concerning privacy issues, intellectual property rights or the freedom of information. Only an open discourse can create a common understanding of principles. Codes of ethics or of conduct (or guidelines) must always be developed and adopted within the member societies themselves. With regard to an IFIP code of ethics, Dr. Holvest comments as follows: "This does not mean that IFIP should do nothing. It only means that it is impossible for the 1990 Draft IFIP code of ethics to be accepted. IFIP needs general principles that will be accepted by all national societies. In my view, these principles must consist of deontological statements. One of the

statements might be the suggestion that every national society produces a national Code of Ethics, taking into account what has already been discussed by many national constituencies." [1]

4 Availability of Data and Material

Data can be made available by contacting the corresponding author.

5 References

[1] Berleur JJ, Brunnstein K, editors. Ethics of computing: codes, spaces for discussion and law. Springer Science & Business Media; 1996.

[2] EL. Privacy, Security & Trust in Information Society. 2021. http://www.eitictlabs.eu/innovation-areas/privacy-security-trust-in-information-society/

[3] Privacyware. PrivacyWare: The ultimate web server security. 2021. https://www.privacyware.com

[4] Scirocco A. The Lisbon Treaty and the Protection of Personal Data in the European Union. 2009. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2008/08-09-19_Scirocco_Lisbontreaty_DP_EN.pdf

[5] Banisar D. Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information. East African Journal of Peace & Human Rights. 2010;16(1):124-54.

[6] Voronkov Y. State-of-the-art in Ethical and Legal Aspects of ICTS in Education. Ethical, Psychological and Societal Problems of the Application of ICTS in Education. 2004:10. http://iite.unesco.org/pics/publications/en/files/3214629.pdf

[7] McMillan K, and Weyers J. How to Write Dissertations & Project Reports. 2nd Ed. London: Pearson. 2011:185-193.

[8] Walther JB. Research ethics in Internet-enabled research: Human subjects issues and methodological myopia. Ethics and information technology. 2002;4(3):205-16.

[9] Pupovac V, Bilic-Zulle L, Petrovecki M. On academic plagiarism in Europe: An analytical approach based on four studies. Digithum. 2008(10). http://www.uoc.edu/digithum/10/dt/eng/pupovac_bilic-zulle_petrovecki.pdf

[10] Alexeyeva I. History of the Problem. Ethical, Psychological and Societal Problems of the Application of ICTs in Education. 2004:21. http://iite.unesco.org/pics/publications/en/files/3214629.pdf

[11] Sojka J, & Gupta A. Teaching Ethics in the Business Classroom: Is Anybody Listening? The Institute for Applied & Professional Ethics Archives, Ohio University. 2009. http://www.ohio.edu/ethics/ethics-modules/teaching-ethics-in-the-business-classroom-is-anybody-listening/index.html

Professor Dr. Dheya Shuja'a Al-Othmany is a full professor of Nuclear Engineering in the Faculty of Engineering, King Abdulaziz University, Jeddah, Saudi Arabia. He holds a Ph.D. in Nuclear Engineering (Radiation Protection) from the University of Aberdeen, UK. He serves as a member of a lot of national and international societies. His research interest lies in Energy Engineering, Nuclear Engineering.