Ethical Issues in the Use and implementation of ICT

Conference Paper · February 2015

CITATION
1

READS
35,632

1 author:

Zdzislaw Polkowski
Jan Wyzykowski University
68 PUBLICATIONS **147** CITATIONS

SEE PROFILE

Journal Article, Pólkowski Z., **Ethical Issues in the Use and implementation of ICT**, in: *Sankalpa: Journal of Management & Research*, ed. R. Khajuria, R. Banerjee i K. Sinha, 4th International Conference on "Business Ethic for Good Corporate Governance & Sustainability", Gujarat Technological University, Ahmedabad, 6-7 February 2015, pp. 2-5, ISSN 2231-1904.

Dr. Zdzislaw Polkowski
The Higher Vocational School of Zaglebie Miedziowe
ul. Odrodzenia 21, 23
59-300 Lubin, Poland
tel. +48 76 749 89 29
fax. +48 76 749 89 28
mobile +48 512084372
z.polkowski@uzzm.pl
www.uzzm.pl
Abstract code: CBE06

Ethical Issues in the Use and Implementation of ICT

Abstract:

The paper contains a description of activities concerning ethical issues in the use and implementation of ICT (Information and Telecommunication Technology) in Poland, especially in the perspective of Small and Medium Enterprises (SMEs). The explosive growth of ICT has had major impacts on society and thus serious ethical questions may be raised concerning individuals and companies, as well as public institutions. The pressing issues raised by ICT include the invasion of individual and corporate privacy, intellectual property rights, individual and societal rights, values preservation and accountability for the consequences arising from the use of ICT, etc. Significant aspects of ethical issues in ICT are discussed, e.g.: using ICT systems in Poland at present and ethical and legal aspects, as well as limitations to using ICT. Also, security issues in ICT are an important element, taken into account by the author of this paper. The research described is based on scoping review to identify relevant studies published in the literature recently. The main method used in this research was case study. In addition, the work contains assumptions regarding further development of ICT implementation in Poland, with particular emphasis on ethical aspects. The results of the research described here are of much importance both for practical and academic reasons. The resulting recommendations may constitute the basis of positive changes and improvement in the ethical aspects of computer based business activities. It is worth noting that although the study focuses on selected Polish enterprises, the resulting contents reflects the situation in Poland and probably in part of SMEs and municipal

companies in the EU as well, thus it may be a starting point for analysing other regions worldwide.

Keywords: computer ethics, cyber ethics, ICT, SMEs, municipal companies

Contents of the article

Introduction

Businesses have adopted information and telecommunication tools in their daily activities and ICTs are very quickly changing the way companies work in. Starting in 1999, 93 % of the information entered and created in companies worldwide became digital. In Poland, 47 % of companies use almost exclusively electronic documents (Mejssner 2014). The effects tend to be relevant to the sphere of material and spiritual: decisions, choices and responsibility. They concern the sphere of morality, ethics dealt with. Ethical aspects of science are increasingly of interest to researchers, developers and users of ICT, who have vast expertise and enjoy the authority and respect among ICT users. Furthermore, they have a significant impact on people's behavior and their values. For these reasons, further research on computer ethics is essential. Users and ICT professionals should be guided by certain moral and ethical principles which might prevent a lot of serious problems and abuses in the use of computer technology, such as loss or destruction of important data, loss of business or a positive image. It may be helpful to analyze the negative cases, and create positive models and patterns of behavior. The main reasons why research in the field of computer ethics is needed, are the advances in computer technology and the lack of adequate and universal practice. Anyone, whether employees, managers or IT specialists, should know what ethical standards and rules

to follow. Below, selected areas of research are shown, which may relate to computer ethics: computers in the workplace, ownership of software (licenses, patents), privacy and anonymity, professional loyalty among specialists, computer crime, ethical standards in the implementation and use of information technology The most important part of the article, however, is a description of the research on ethical problems in implementation and utilization of ICT systems in business. This paper is structured as follows: After the introduction, in Section 2 the literature review is provided. Section 3 describes the current research gap, the purpose of article and methodology. The next section contains the description of the case study on computer ethics in municipal companies, as well as in SMEs. Finally, conclusion, research limitations and scope for future study are provided.

Literature review

Computer ethics, as a branch of applied ethics, deals with how computing professionals should make decisions concerning professional and social conduct. It is also referred to by terms, such as "cyber ethics", "information ethics", "information communications technology ethics", "global information ethics" and "internet ethics" (Jamal 2014). Consideration of computer ethics is recognized to have begun with the work of Wiener in the early 1940s, which resulted in Wiener and his colleagues creating what Wiener called cybernetics (Herold 2014). Wiener defined the concept of computer ethics in a book called "The Human Use of Human Beings" which laid out the basic foundations of computer ethics and made him the father of computer ethics (Jamal 2014), even though Wiener never used the term “computer ethics”. In 1966 Weizenbaum created ELIZA - an early example of chatterbot software using natural language processing to construct a computer - human dialog. ELIZA was able to respond to some predefined queries with a semblance of awareness, but otherwise responded with a generic prompt to give more information (Malmgren, Ahammar 2014). Concerned about the ethical implications, Weizenbaum wrote “Computer Power and Human Reason” (1976), a book now considered a classic in computer ethics. Donn Parker provides the first theoretical basis of computing ethics, but like Wiener, he never uses the term (Moor 2014). The term “computer ethics” was first introduced by Walter Maner in the mid 1970s (ABA Security 2014). By the late 1970 Parker, Weizenbaum, and Maner had raised the computer ethics consciousness of a number of American scholars. By the 1980s, certain social and ethical consequences of IT (Information Technology) had become public issues: computer-enabled crime, software ownership, disasters and invasions of privacy cause by computer

systems. In the mid-80s, James Moor of Dartmouth College published his influential article "What Is Computer Ethics?". During the 1990s, new courses, conferences, journals and scientific articles appeared, and a wide diversity of scholars and topics became involved, among others: Donald Gotterbarn, Keith Miller, Simon Rogerson, and Dianne Martin. Deborah Johnson, Gorniak Kocikowska (Zalta 2014), (Tagacay Wilson 2014). Nowadays, the pinnacle of ICT, the coming together of computers, telecommunications and media, with the Internet and WWW have brought a seemingly endless set of ethical issues such as legal jurisdiction, free speech, virtual community and others (Tagacay Wilson 2014). From the present to the near future, computer technology will feature the convergence of ICT. Crucial issues will focus on decision-making capabilities, biochip implants, genomic research (Tagacay Wilson 2014). A necessity for the future will be to look at government and public responsibility and how proactive systems might impact the open society given the fact that their functionality may be hidden from the users. James H. Moor sees computer ethics as the analysis of the nature and social impact of IT and the corresponding formulation and justification of policies for the ethical IT use. The term "computer technology", or "information technology", is used here in a broad sense, including computers and associated technology, software, as well as hardware, also networks connecting computers, as well as computers themselves (Moor 2014).

Current research gap

A literature review, analyzes of current research, the author's practical experience and the increasingly common business trends show that at present, both private SMEs and municipal companies have to confront computer ethics issues, with unprecedented pressure to improve their computer ethics while progressively lowering their costs. What is more, they are expected to become more accountable, transparent, customer focused and responsive to stakeholder needs. The main problem in the area of computer ethics is the lack of model solutions and recommendations that could be immediately applied in SMEs.

The purpose of the article

The problem described above definitely leads to a considerable need for research in this area. Since the process of using and implementing new ICT solutions has already started, the author decided to check the current situation on computer ethics in SMEs in Poland. The goal of this study is to critically examine rules, procedures which employees and owner of private SMEs

apply in fields such as: computer use in workplaces, respect for ownership of software (licenses, patents), privacy and anonymity, professional liability, computer crime, and to determine the ethical standards in the implementation and use of information technology, forming relevant recommendations. As it is mentioned above, the study was based mainly on a case study. The research results may be used by IT and business leaders, as they plan and develop ICTs following ethical principles.

Methodology - the case study method

As an example of how Polish SMEs treat computer ethics aspects, an analysis of a specific case study is presented here: selected SMEs and the way they handle computer ethics. Cases are intended to confront readers with specific real-life problems that do not lend themselves to easy answers. Case discussion demands critical and analytical skills and, when implemented in small groups, also fosters collaboration (Pimple 2002 191-205). An empirical inquiry concerns a contemporary phenomenon (e.g., a "case"), set within its real-world context - especially when the boundaries between the phenomenon and context are not clearly evident (Kimmel 2009a: section 12). The case study method has its strengths and weaknesses. For the purpose of the paper municipal companies are described together with other SMEs, although the situation in either sort of units is different, which results from the fact that they are usually regarded as belonging to the same category, mainly because of their size. Municipal companies are considered to be state companies, as they are owned by the local commune. Thus, the value of the information obtained increases with the variety of the units analyzed.

Strengths of the case study approach

The case study method involves detailed, holistic investigation and it may utilize a range of different measurement techniques. Research was conducted in 2013- 2014 by the author experienced in computerization of SMEs and public institutions since 1990. In this research the author had unlimited access to all data in companies with ICT systems in Polkowice in Poland. The research was a multiple case in SMEs and municipal SMEs (similar in size but of different fields of activity).

Weaknesses of the case study approach

In this research the case study involves an analysis of small data sets - about 10 SMEs and 6

municipal companies in a selected Polish town, which may lead the researcher to gain some insights about trends in relevant companies.

Research questions

During the study the following aspects were checked:

1. What differences and similarities exist in the computer ethic values of private SMEs' and municipal companies' employees?
2. Which ethical rules are used by managers, employees and IT specialists in implementing and applying ICT?
3. What further development and recommendations of ICT implementation ethics, with particular emphasis on private SMEs and municipal companies may be expected?

To deal with the first and second issue, the ICT systems in SMEs and municipal companies systems were examined, subsequently reflecting on the development of computer ethics. The data for the study has been collected from primary sources: audits of ICT systems, interviews with managers and IT specialists and employees, official and confidential documents on computerization, company reports, as well as from secondary sources such as: books, articles and journals. Some data were also collected by means of telephone conversations with representatives of ICT solutions providers, companies offering ICT security solutions. Moreover, the author's twenty-five years of personal experience in running a small IT company constitutes a much relevant source of valuable, reliable and actual information on the functioning of computer rules and procedures. To answer the last question, the article presents the findings and then implications and recommendations of the research, with pre-determined and defined areas of ICT ethics taken into account.

Findings

The investigation confirmed that ICT provides a whole new set of ethical challenges. Computer networks can be breached, personal data can be compromised, critical confidential corporate information or classified commercial secrets can be stolen by employees, Web sites can be hacked and keystroke loggers can be surreptitiously installed etc. Both SMEs as municipal companies are aware of these risks. However, the work ethics of employees

working in SMEs and municipal SMEs differ in fields such as: computers in the workplace, ownership of software (licenses, patents), privacy and anonymity, professional liability specialists, computer crime. Municipal companies generally have internal computer ethics, but not many yet have relevant experience. The reason is that managers not securing the systems they are responsible for, employees using information they should not have access to, and system users finding shortcuts around established security procedures may incur significant penalties from the government institutions. As for SMEs, hardly any procedures or documentation regarding relevant policies may be found (Relkin 2014).Despite the threat of punishment, business owners do not pay attention to these issues until a problem occurs. Preventive measures are not applied. Businessmen are not willing to invest in solutions to ensure high safety and application of codes and ethics. What is important for most of them is as much as possible, and immediate, profit. Investing in the area of computer ethics is often considered a waste of money. This approach follows an unstable business environment. Below the results of research in relation to specified areas are presented.

Computers in the workplace

Introduction of computer technology in the workplace involves hardware, software, network, safety and ways of use. In this case, the analysis was focused on presenting the rules for using computer equipment by workers and small business owners in Poland. The structure of IT systems in private SMEs is simple, sophisticated IT tools are not common there, while IT systems in municipal units are more and more advanced. Many units have their own servers on the premises, some of them even more than one. Moreover, some possess protect the network and data with NAS (Network Attached Storage) and UTM (Unified Threat Management), . They use UTM because of some regulations introduced by GIODO (the Inspector General for Personal Data Protection). In part of municipal companies employees are not allowed to use private emails, pen drives, laptops, tablets etc at work time. Company pen drives should be protected with secure software (e.g. truecrypt). All computers have a BIOS password and a password to the operating system, changed every 30 days. The access to places with servers is redistricted and only for designated persons. They use Wi-Fi only with VLAN solutions, for network access safety reasons. In private SMEs both managers and employees do not use the solutions mentioned above.

Ownership of software (licenses, patents)

Other significant ethics-related issues are legality and software licensing rules. The study has shown that software piracy is still common and socially acceptable in Poland. In both SMs and municipal companies there were cases of possession of illegal movies and music but also very expensive commercial programs. In 2013, up to 51% of the software installed on personal computers in Poland was unlicensed. (Arczewska 2014). There are cases of unauthorized software installation by employees, hidden installations made through a "pop-up" windows and poor management of software licenses. Recently, an increased activity has been seen on the part of BSA (Business Software Alliance) which takes reports of piracy, pays for the disclosure of pirates, cooperates with law enforcement agencies. High activity manifests itself in the media by frequently organized actions. BSA in Poland frequently sends official-looking requests to companies (Maj 2014). Very frequently those responsible for IT resources in the company are convinced that the software in their company is fully licensed. Unfortunately, in practice, it appears that they do not know exactly what software is installed, in what quantities, by whom, and how to use it. In SMEs managers seldom take an activity concerning software licenses . In Poland the police and BSA officers have checked selected companies . Such a situation has not taken place in case of the companies analyzed here. The majority of the examined private SMEs do not have IT departments and thus, they do not have enough knowledge on this topic. In municipal companies the situation is different, because they have to have a plan of an internal audit. Some of them employee special companies to conduct an external audit.

Computer crime

Research carried out in Poland shows that more and more often the victims of attacks in the network are small and medium-sized enterprises. Meanwhile, nearly 70 % representatives of small businesses are not aware that a data security breach may have negative impact on the finances or reliability of their business (Gajewski 2014)**.** According to a survey by Ipsos Reid, 40 % of small companies do not have any data destruction procedures or mechanisms. Only 18% have appropriate provisions within their regulations. 48 % do not have a designated person responsible for the management of this area (Broniatowski 2014a). Past experience clearly shows that very often the weakest link in securing the data are the employees. Some companies train their teams. Unfortunately, as it was mentioned earlier,

more than 1/3 of small businesses do not. Almost half of the companies (48 %) did not have a designated person responsible for the data security management (MATP 2014). The report (Raport o zagrożeniach, 2012) also shows that Poland is ranked 7th in the world in terms of the number of bots -networks of computers of regular Internet users under the remote control of the cybercriminals and used for various types of attacks (Wojtalik 2014).The research conducted for this paper discovered a case of unauthorized access to the server by a person from outside the company, as well as a few cases of the former company data or disloyal employees transferred to their businesses competitors.

Privacy and anonymity

Principles of operation in the field of privacy and anonymity are strictly regulated in Poland by the government institution GIODO (The Inspector General for Personal Data Protection). Following these provisions, the Inspector General for Personal Data Protection is entitled to:

- Supervise ensuring the compliance of data processing with the provisions on personal data protection,
- Issue administrative decisions and consider complaints with respect to the enforcement of the provisions on protection of personal data,
- Keep the register of data filing systems and provide information on the registered data files,
- Issue opinions on bills and regulations with respect to the protection of personal data,
- Initiate and undertake activities to improve the protection of personal data,
- Participate in the work of international organizations and institutions involved in personal data protection (Kałużyńska 2014).

To fulfill the requirements of GIODO, IT specialists in municipal companies had to change the structure of IT systems to protect personal data. For reasons concerning the security of data, IT specialists and managers are concerned about implementing UTM, NAS and others solutions. In private SMEs the owners do not really care about it.

Professional loyalty* of *specialists

This field is one of the most important for the owners of private SMEs. The investigation has shown that managers do not trust employees and very often they protect data against their competitors. They are convinced that employees can steal data on contracts and clients. For this reason usually employees have limited access to data on sales, money transfer and obtained profit. It is worth noting that in three cases, former employees acting against a former employer used their own data. It is a very serious problem in small businesses in Poland.

Managerial implications

ICT may have far-reaching and sometimes hard to predict implications for a firm that adopts such systems. ICT specialist and business managers should predict the ethical implications of an ICT implementation and to increase the success of it, they may therefore need to have the opportunity to solve potential ethical problems beforehand . Below, Managerial Implications are presented in relation to specific areas.

Computers in the workplace

UTMs (unified threat management) seem to be appropriate tools to protect networks in SMEs. They offer a lot of useful options and they guarantee a high level of security. Employees, however, should be told to what extent their behavior is monitored by means of UTM. Therefore, many companies in the SME sector need a closed security system in one box. An "all-in-one" solution could simplify management of network security, which is particularly important when there is not enough IT personnel. The next issue is to consider installing an own server which could operate in the domain. This may increase the level of data security. Some companies can rent servers in CC (Cloud Computing). Year by year, in Poland there are more and more offers of CC solutions. Managers, however, do not trust CC, concerned about their data security. To protect data some companies should use NAS with backup software. Moreover, managers should limit the use of private e-mail, personal laptops or Wi-Fi. Additionally, IT specialists should control computers together with the employee and teach them how to properly use ICT systems. In SMEs appropriate regulations on computer ethics should be applied.

***Ownership of software* (licenses, patents)**

Hiring new employees, the employer must ensure that the contract contains provisions requiring the employee to observe ethical rules and respect the ownership of software in the

workplace. A good practice is to implement regulations to utilize corporate resources and make every employee familiar with them. In some companies, the document is part of the agreement of employment. Additionally, it must be emphasized that allowing employees unlimited access to the Internet is the primary source of problems concerning license for software and of additional threats. It must be ensured that each employee receives regulations to use the software and is familiar with their contents. Additionally, IT specialists should control software in computers together with the employee. IT specialists can provide instructions how to keep the software in accordance with the applicable rules. They may also use specialized software which enables hardware inventory, software records, and records of the legality of the basic functions of a computer system, which shows a new dimension to the conduct of audits. (e.g. E-auditor).

Computer crime

To achieve security against computer crime it is necessary to follow such procedures: to upgrade the operating system, to update the web browsers and to use antivirus software with enhanced protection. Another recommendation is to raise the level of awareness of employees on computer crime, which is why small business owners should invest in training employees and develop procedures to ensure compliance with the security of the network. IT specialists must continually analyze both internal and external data flow. Besides, it is necessary to implement appropriate security measures, but also to develop business culture that will allow the prevention of potential computer crime problems. Is also extremely important to exchange experiences related to cybercrime in the framework of professional organizations and academics. It may be interesting to note at this point, that statistics show that more than 80 % of stolen data is the result of low tech “dumpster diving”, whereas approximately the same percentage of organizational crime is the result of an “inside job” (Relkin 2014).

Privacy and anonymity

Corporations collect massive amounts of data on individuals and organizations and use it for commercial reasons; to increase business, control expense, enhance profitability, gain market share, etc. Seemingly, various sources of data can be cross-referenced to gain new meanings when one set of data is viewed within the context of another. Systems that track this data can be secured but, at some point, data must leave those systems and be used (Relkin 2014). European Union (EU) and Polish legislators, facing new challenges, have adapted the

existing IT regulations to the new cyberspace, and formed new ones, often resulting from accessing EU structures. The need to develop an EU-wide strategy on Cloud Computing is highlighted in the Digital Agenda for Europe (DAE). Additionally, some issues on benefits, risks and recommendations for information security were published by the European Network and Information Security Agency (ENISA) in 2009. Bearing in mind that the report is for the European audience, it has a useful checklist of questions to ask before outsourcing into the cloud (Sorell 2010).

Professional loyalty of specialists

The research results show that there is a lack of principal rules necessary in the field of computerizing, as well as when recognizing the role of the computer ethics in particular SMEs. It is surely a result of incomplete coordination of IT actions between IT specialists, managers and academics (Walczak, Pólkowski 2013). The situation is much better in the municipal companies that are committed to the principles of proper maintenance of ICT systems. In private enterprises, the main concern for IT systems is the threat of data loss and in particular the threat of competition accessing and using data with the help of disloyal employees. Hence, the recommendation in this field could be to increase the role of computer ethics during classes at universities and during trainings for employees.

Conclusion

In the world today, all companies should have their own policy concerning ICT ethics. Otherwise, sophisticated equipment and advanced software will become useless for the reasons mentioned in the article. However, although the results of research, particularly in relation to private SMEs, appear rather negative, there are some positive signs in computer ethics. This is evident in one of the two groups of respondents, municipal enterprises. Considerable pressure from the Inspector General caused significant issues regarding computer ethics. Most companies in this group have and apply procedures related to information security and information, as well as notes on the ethical use of ICT in their daily work. Another positive result of the analysis is the growing role of computer ethics in education of students. Numerous Polish universities already have curricula items entitled Information Ethics. Moreover, it is expected that in the near future there will be courses of study devoted entirely to ethical issues of ICT. As in the past from one computer profession a lot of related ones developed, in the same way the emergence of computer ethics for IT professions is expected.

Research limitations and scope for future study

Computer ethics is rapidly evolving into a broader and even more important area - global information technology ethics. For this reason, attempts are made to establish a truly global context of generally accepted standards of behaviour and the improvement and protection of human values.

As a suggestion for the future research on computer ethics, the study creates an opportunity towards the model of solutions for SMEs, which could be implemented in companies regardless of the type and of their activity.

Since the study focuses on Polish enterprises, the resulting contents reflects the situation in Poland and probably in some SMEs and municipal companies of the EU as well, thus it may be a starting point for analysing other regions all over the world.

References

1. ABA Security, Computer ethics, December 2014, http://abasecurity.blogspot.com/
2. Arczewska, A., *Mimo zagrożenia dla bezpieczeństwa informatycznego ponad połowa oprogramowania zainstalowanego w Polsce to oprogramowanie nielicencjonowanie*, December 2014, http://ww2.bsa.org/country/News%20and%20Events/News%20Archives/global/06242014-GlobalSoftwareSurvey.aspx
3. Bynum, T.W., *Etyka a rewolucja informatyczna*, December 2014, http://mumelab01.amu.edu.pl/Wprowadzenie-HTML/KO-03-01.html#34
4. *Firmy na bakier z rozpoznawaniem cyberprzestępczych zagrożeń*, edited by Broniatowski, M., [in:] *Forbes*, December 2014, http://www.forbes.pl/firmy-z-sektora-msp-nie-rozpoznaja-cyberprzestepczych-zagrozen,artykuly,166944,1,1.html
5. Gajewski, M., *Małe firmy lekceważą cyberzagrożenia*, December 2014, http://www.chip.pl/news/bezpieczenstwo/technologie-bezpieczenstwa/2013/07/male-firmy-lekcewaza-cyberzagrozenia
6. Genova, G. and Gonzalez, M.R. and Fraga, A., *Ethical Responsibility of the Software Enginieer*, December 2014, http://ceur-ws.org/Vol-240/paper4.pdf
7. Herold, R., *Introduction to Computer Ethics*, December 2014 http://www.infosectoday.com/Articles/Intro_Computer_Ethics.htm

8. Holleyman, R., *Legalne oprogramowanie, zmniejszenie ryzyka, zwiększenie oszczędności*, December 2014, http://ww2.bsa.org/country/~/media/Files/Tools_And_Resources/Guides/SoftwareManagementGuide/2009/SAM_pl.ashx
9. IAR, *Małe przedsiębiorstwa najbardziej narażone na atak cyberprzestępców*, December 2014, http://m.onet.pl/biznes/kraj,8h3jm
10. Janoś, T., *Zintegrowane zabezpieczenia dla small businessu*, December 2014, http://www.crn.pl/artykuly/raporty-i-analizy/2014/05/zintegrowane-zabezpieczenia-dla-small-businessu/article_view?b_start:int=2&-C
11. Jamal, A., *Computer Ethics*, December 2014, http://iraj.in/up_proc/pdf/41-139038002801-06.pdf
12. Kaczyński, M., *BTC. E-Auditor*, December 2014, http://www.e-auditor.eu/
13. Kałużyńska-Jasak, M., *Responsibilities of the inspector General for personal data protection*, 2014, [in:] http://www.giodo.gov.pl/426/j/en/.
14. Kimmel, A.J., *Ethics and Values in Applied Social Research*, [in:] *Case Study Research*, edited by Yin, R.K., Design and Methods, 2009.
15. *Legalne oprogramowanie*, edited by Pieńkowski R., December 2014, http://mojafirma.infor.pl/tematy/legalne-oprogramowanie/
16. Maj, M., *BSA chce od Twojej firmy oświadczenia o legalności programów? Najlepiej to zignoruj*, December 2014, http://di.com.pl/news/49142,0,BSA_chce_od_Twojej_firmy_oswiadczenia_o_legalnosci_programow_Najlepiej_to_zignoruj.html
17. Malmgren, M. and Ahammar, U., *Chatterbot with common sense*, December 2014, http://www.csc.kth.se/utbildning/kth/kurser/DD143X/dkand13/Group6Gabriel/opposition/Erik_Odenman.pdf
18. *Małe firmy lekceważą cyberprzestępczość*, edited by Broniatowski, M., [in:] *Forbes*, December 2014a, http://www.forbes.pl/male-firmy-lekcewaza-cyberprzestepczosc,artykuly,157867,1,1.html#
19. MATP, *Mały biznes łatwym łupem hakerów*, December 2014, http://www.ekonomia.rp.pl/artykul/1027701.html?print=tak&p=0
20. Mejssner, B., *Niezbite cyfrowe dowody*, December 1014, http://www.klubcio.pl/artykuly/321458_3/Niezbite.cyfrowe.dowody.html?test=yesinfo_ochrona.html?test=yesinfo_ochrona.html

21. Moor, J.H., *What is computer ethics?*, December 2014, http://web.cs.ucdavis.edu/~rogaway/classes/188/spring06/papers/moor.html
22. Patrzek, W., *Zawód informatyk - kodeks etyki i standardy postępowania*, December 2014, http://www.e-administracja.org.pl/konferencje/2005/fiwa4/pdf/PATRZEK-informatyk_samorzadowy.pdf
23. Pimple, K. D., *Six domains of research ethics: A Heuristic framework for the responsible conduct of research*, Science and Engineering Ethics 8:191-205, 2002.
24. Plemmons, D. and Kalichman M., *Case Studies*, December 2014, http://research-ethics.net/discussion-tools/cases/
25. Relkin, J., *10 ethical issues conforting IT managers*, December 2014, http://www.techrepublic.com/article/10-ethical-issues-confronting-it-managers/
26. Reszka, M., *Czy potrzebna nam jest etyka komputerowa, czy wystarczy zwykła etyka?*, December 2014, http://informatyka-wsksim.cba.pl/index.php/aktualnosci/starsze/32-etyka-a-informatyka
27. Sorell M., CRN, 2010
28. Strzałkowski, M.,. *Fundacja BezpieczniejwSieci.org, January 2013, http://bezpieczniejwsieci.org/*
29. Szynkiewicz, M., *Technologie komputerowe w perspektywie etycznej. Moralność w e-rzeczywistości - część II*, December 2014, http://www.czasinformacji.pl/archiwum/pazdziernik2012.php,
30. Tagacay, Wilson, *Defining Computer Ethics and History of Computer Ethics*, December 2014, http://wilsonmtagacay.blogspot.com/p/defining-computer-ethics-and-history-of.html
31. Walczak, M., and Pólkowski, Z., The e-health systems in Poland, December 2013, http://economic.upit.ro/repec/pdf/2013_2_6.pdf
32. Williams, M., *IT Matters: Ethics, Information Systems, and a steel Ax*, December 2014, http://gbr.pepperdine.edu/2010/08/ethics-information-systems-and-a-steel-ax/
33. Wojtalik, M., *Hakerzy coraz częściej atakują małe firmy*, December 2014, http://biznes.newsweek.pl/hakerzy-coraz-czesciej-atakuja-male-firmy,103726,1,1.html
34. Venter, L., Olivier, M.S. and Britz, J.J., *Interactive to Proactive: Computer Ethics in the past and the future*, December 2014, http://biblioteca.clacso.edu.ar/ar/libros/raec/ethicomp5/docs/htm_papers/65Venter,%20L.htm

35. Yin, R.K., *A (very) brief refresher on the case study method*, December 2014, http://www.sagepub.com/upm-data/41407_1.pdf
36. Zalta, E.N., *Computer Ethics Basic Concepts and Historical Overview. Stanford Encyclopedia of Philosophy*, December 2014, http://stanford.library.usyd.edu.au/archives/spr2006/entries/ethics-computer/