Annals of the Academy of Romanian Scientists
Series on Science and Technology of Information
ISSN 2066-8562 Volume **1**, Number **1**/**2008**

SOCIAL IMPACT OF THE INFORMATION AND COMMUNICATIONS TECHNOLOGY

Ştefan IANCU[1]

Rezumat. *Autorul prezintă în această lucrare puncte de vedere controversate privind impactul social al utilizării tehnologiei informaţiei şi comunicaţiilor (TIC), caracterul privat al informaţiei, necesitatea reglementărilor juridice privind circulaţia informaţiei prin Internet, protecţia drepturilor de proprietate intelectuală şi încălcări ale drepturilor, ilegalităţi etc. Concluzia lucrării este necesitatea unei reglementări juridice internaţionale, cel puţin la nivelul tuturor ţărilor participante la Internet, care să ţină seama de caracterul intangibil al informaţiei şi care să difere de legislaţia specifică bunurilor materiale.*

Abstract. *The Author presents in this paper controversies points of view on the social impact of the information and communications technology (ICT): privacy character of information, the necessity of juridical regulations on dissemination of information by Internet, protection of the intellectual property rights, offenders of law, unlawful acts and so on. The conclusion of this paper is the necessity of the juridical, international regulations, at least at the level of all countries that participate in the Internet, that take in view the intangible character of the information and that should be different from the specific juridical regulations for the material goods.*

Key words: information and communications technology, protection of personal data, intellectual property, infringements.

1. Introduction

At the beginning of the third millennium, "Information and Communication Technologies" (ICT) are no more just a technology, but form part of our daily life. ICT now put people around the world in touch with each other to an extent, which was difficult to imagine just a decade ago [1].

School students from Bucharest or Paris can and do correspondence daily about evolution and intellectual liberty with librarians from Kansas or Norway and even professors from South Africa. Large companies consider it quite routine to have a head office in one country, production plants in two or three others, administered from a fifth and a sixth, while customer support is based in three more convenient time zones.

1 Prof. Dr. Eng., Scientific Secretary of the Information Science and Technology section of the Romanian Academy; full member of the Academy of Romanian Scientists (stiancu@acad.ro).

No other time than ours has had more of the future in it – and less of the past. The civilization we are entering in no promised land. It is realm of challenge, with hurdles to overcome and frustrations to live with. Don't confuse it with the latest in techno-gewgaws and acronym babble. Or with the obsession for instant gratification by which we seem to live more and more [2].

The symbol of the convergence between telecommunications, computer and control industries, the Internet, has established itself as one of the main building blocks of the Global Information Infrastructure and as an essential enabler of the Knowledge-based Information Society in Europe.

The potential of the Internet to inform, educate, entertain and conduct business on a global scale is considerable. But, like any other new technology, the ICT carries an amount of potentially harmful or illegal contents or is misused as a vehicle for criminal activities.

To analyze and evaluate the impact of a new technology can be difficult. Some of the changes are obvious. Some are subtle. Even when benefits are obvious, their costs and side effects may not be, and vice versa. Changes in technology usually require adaptive changes in laws, social institutions, business policies, and personal skills and attitudes and even mentalities. A new technology makes possible harmful actions that were not considered when existing laws were written and, for this reason, they are not illegal or criminal [3].

Many issues and problems that arise from the ICT development are not fundamentally different from issues and problems with which the society has been confronted before and this fact suggests that the root is not always or only ICT, but may be human nature, ethics, politics, instruction and education.

In strategic thinking, dependence soon becomes vulnerability and then by extension a potential target. In the last decade, the same translation from dependence to target has been made via information. Viruses can destroy vital systems in a surprise attack. Small campaigns of information warfare are becoming quite commonplace.

All this has led to anxieties that new opportunities are opening up for hostile states or terrorists. Information warfare might involve disabling air-defence systems, sending missiles off course, leaving local commanders in the dark and senior commanders confused by interfering with software or hardware.

Television images might be distorted to make an enemy leader appear ridiculous; misleading signals could be sent to top commanders; false orders might be delivered to key units.

Civilian life might be disrupted through attacks on the information systems supporting the financial or transportation systems.

Any author of a paper has some personal opinions, positions, or biases. I have a strong bias in favour of the Bill of Rights. I also have a generally positive view of technology, including computer technology. I think that technology, in general, has been a major factor in bringing physical well/being. Let think about the products we use, the food we eat and the people we talk to in a day – and consider how different a day would be without modern communication, transportation, refrigeration and plumbing. In the same time, we should take in view that the technology can provoke, by unlawful utilization, unpleasant problems. [4].

The ICT utilization does not exist in a legal vacuum, since all people involved are subject to the laws of the respective State. In the studying the potential infringements we have to differentiate the illegal acts and the harmful ones**.** In facts, in our days, INTERNET has become the country of the four horsemen of apocalypse: violations of the private character of the personal data, economic crimes, dissemination of the materials of illegal substance and violation of the intellectual property rights.

2. Violations of the private character of the personal data

As a result of the rapid ICT development large quantities of information relating to individuals ("personal data") are routinely collected and used by public administrations and in every business area.

Computers make the collection, analysis, storage, access and distribution of large amounts of information much easier than before. A sector of data on a disk can be accessed in roughly 5 milliseconds - faster than we can turn a page in a book. Computers have increased both the speed and anonymity with which a person can do searches. In the past, our conversations disappeared when we finished speaking, and only the sender and recipient normally read our personal communications.

Now that we communicate by e-mail and electronic discussions groups, our words are recorded and can be copied, distributed, and read by others.

Some of the risks that arise from the existence of the many government and private databases are the following: unauthorized uses by "insiders", the people who maintain the information; inadvertent leakage of information through negligence or carelessness, and access by intruders (e.g. hackers); propagation of errors and the harm caused by them.

New telecommunications technology and encryption methods make it possible to keep communications secret from others. For efficiency, for observance the privacy and for increasing the competitiveness of communications systems, we should act for existence of law enforcement agencies to intercept and monitor communications of suspected criminals.

Generally speaking, it's clear that we cannot expect complete privacy. In a small town, everyone knows everything about all. In a big city, we are more anonymous. But if people know nothing about you, they may be taking a big risk making business with you. To be with full knowledge of the case, it's necessary to give up some privacy. Thus privacy involves a balancing act and the factors that can be balanced are: safeguarding personal and group privacy, in order to protect individuality and freedom against unjustified intrusions by authorities; collecting relevant personal information essential for rational decision-making in social, commercial and government life; conducting the constitutionally limited government surveillance of people and activities necessary.

Since the advent of smart cards (cards containing a microprocessor and memory) there are increasing intentions for establishment of a computerized national identification card system. There is currently used a social security number for identification for getting numerous services. Thus smart cards resolve a lot of problems with the social security number and it could generate much worse new problems.

Some states use the social security number as the driver's license number and if there is someone who knows a name and corresponding social security number can get access to the respective man work and earning history, credit report, driving record, bank account, and all other personal data. With the social security number a person can be followed by the checks he writes. There are some banks and brokerage firms that have automated telephone access to accounts using the personal identification number (PIN) and so the potential for both privacy invasion and fraud is clear [5].

People react quite differently to issues of privacy from government. Some are horrified at any mention of social security number, or of personal identification number. Others are indifferent, whereas others view these changes as expansions of government services and capabilities that are necessary and appropriate to reduce crime, make sure everyone pays their taxes and enforce various laws.

Our health and medical information are personal. Some are very sensitive: information about alcoholism, sexually transmitted diseases, psychiatric treatment, and suicide attempts. In general, people desire to keep other health problems private even if they do not have negative social connotations. For example, someone may not wish others to know he had cancer so that his friends do not feel awkward around him or treat him differently. In fact, there is little legal protection for confidentiality. Some laws control information about specific diseases, for example AIDS, rather than medical information in general [6].

Medical information can be used for marketing purposes. Underground data dealers and other individuals can obtain or release medical information for various

purposes. One factor that diminishes our control over our medical records is that most of us do not pay directly for our medical care. The insurer needs access to the records to verify eligibility and amount of payments and to check for fraud (by patients or doctors). A vast amount of medical information is collected by government agencies to plan programs, compile public health statistics and do medical research. The anonymity and impersonal nature of a system of third-party payers make it an inviting target for fraud.

The benefits of a national database containing everyone's medical record include accessibility when ones travelling or moves to a new area and the ease with which government and medical researchers can get complete data on diseases and health issues they are studying.

3. Economic crimes

Computers make many activities easier for us. They also make many illegal activities easier for criminals. Computers provide new ways to commit old crimes: fraud, embezzlement, theft, forgery, vandalism, industrial espionage and they provide new challenges for prevention, detection, and prosecution of crimes.

Computer crimes against businesses and organizations include offences committed by "insiders" (usually employees) and outsiders (hackers, competitors, criminal gangs). Computer as a criminal tool is a powerful one. It makes some crimes not only easier to commit, but also more devastating and harder to detect. Global networks extend the reach of thieves and make arrests and prosecutions more difficult. A thief who steals a credit card gains access to a much larger amount of money than the thief who steals a wallet with some cash. Confidential business information can be stolen from computers and voice mail systems without any signs of "forced entry". The complexities of modern financial transactions increase the opportunities for embezzlement. The complexity and anonymity of computers 70 add to the problem and help hide scams. The victims of some of the most costly scams are banks, brokerage houses, insurance companies and other large financial institutions.

Employees can create fake purchase orders for purchases from phoney companies and cash the checks themselves. Employees can also steal data from their employer's computer and sell it to competitors. Three employees of the Encyclopaedia Britannica sold the customer list (containing two millions names and addresses) to a direct mail company [7]. It is not easy to get reliable data on the amount of computer crime, in part because banks and other victims prefer not to publicize their losses and weak customer confidence.

Credit cards, automated teller machines (ATMs) and telephone calling cards illustrate many aspects of the computer crime problem. They give us convenience,

but expose us to risks we did not take before. Most people would not casually carry around many hundreds or thousands of lei, dollars or EURO, in cash, but a credit card, an ATM card, or calling card gives the holder access to such large sums. When we had to go to a bank to withdraw cash, we did so during bank hours /in the daytime/ and put the cash away before leaving the building. Now people have the possibility to use ATM machines at night to, outdoors, where they can be observed and robbed.

Solutions for credit card, ATM and phone fraud illustrate the continual leapfrogging of increased sophistication of security techniques and increased sophistications of the techniques used by criminals. These also illustrate the use of technology itself to solve problems created by technology.

Industrial espionage is not new, but it used to require the physical infiltration of the victim's business, theft of documents, physically copying documents or paying off an insider to provide critical information. In computer technology an insider is paid for passwords. Now the spying can be accomplished from a remote location using a computer network. Large quantities of digital information can be copied quickly. There may be no clues to indicate that a theft took place; nothing is missing [8].

A hacker considers that he is a bright, inquisitive young, who explore computer systems for fun and intellectual challenge. In the opinions of the hacker's victim, a hacker is an irresponsible criminal who invade privacy, steal information and money and destroy files and crash computer systems. Hackers argue that systems should be open, that information should be free. What they didn't explain is why they steal values or destroy files.

Thus, hacker is now used to nominate people who explore the intricacies of computer and telephone networks and carry out mild pranks – and people who intentionally destroy files, release computer viruses; reroute phone calls; change credit files; interfere with business and personal activities; steal software, passwords and other information, expose personal information; steal other values.

There are some people who consider that the problem of the hackers is the extent of their activities and the amount of damage they do. Some people consider that the problem is the potential damage that they could do using their skills. Others consider that the problem of the hackers is a problem of the level of security or vulnerability of vital computer and communications systems. In my opinion, the problem is poor security. The administrator's responsibility is to protect the system and its data. The job of a computing system' administrator is not to stop an intrusion; his job is to prohibit it [9].

Another problem is that a lot of credit card companies are willing to absorb a large amount of fraud losses as part of doing business. Retail stores, some banks

have accepted some amount of losses rather than offend and inconvenience customers [10]. In my opinion, publicity of all hacking incidents will encourage companies to improve protection for sensitive data.

4. -Dissemination of the materials of illegal substance;

The new computer communications technologies (Internet, the Web, bulletins for distribution of news, information and opinion services, commercial online information services e.g.) has become major arenas for distribution news and may guarantee freedom of the press for all of us. But, there's a whole range of rules which limit for different reasons the use and distribution of certain content. The infringement of these rules leads to the illegality of the content. Various types of material may offend the values and feelings of other persons.

What is an offensive speech? What should be prohibited or restricted on computer networks. It depends on who you are. It could be political or religious speech, pornography, sexual or racial slurs, libellous statement, depictions of violence, or information about how to build bombs. Although there is a disagreement over the standards for what material adults have the right to view, most people agree that a tighter standard is appropriate for children. There is no generally accepted legal definition of "indecent" or "filthy" words used in free messages. There is pornography on the INTERNET.

There are numerous INTERNET sites from which users can download sexually explicit images. There are discussion groups where people discuss sexual activity including paedophilia, in graphic detail. It is illegal to create, possess, or disseminate child pornography. It is also illegal to lure children into sexual acts. But the INTERNET is used to commit such facts.

Discussion of sexual activity, even unusual or illegal sexual activity, is usually not illegal. Distribution of obscene material is sometimes illegal. Some people are shocked that pornography is common in cyberspace, especially on the Internet, which began as a forum for research and scientific discussion

Computer networks are changing the meaning of word "community". An obscene file send through INTERNET from a town to another can be accessed by anyone, from anywhere. The Net is also changing the meaning of "distribution". A couple in one region of the country can form an Association that made sexually explicit images available on the Net.

Everybody who has access to Internet can have access to the sexually explicit images available on the Net. This case illustrates that applying old laws and judicial precedents to activities made possible by new technologies can have results that they were not meant to have.

Are new restrictions on freedom of speech needed to protect children on the INTERNET (and to protect adults from material that is offensive to them)? Are there other solutions that do not threaten to diminish free discussion of serious subjects or deny sexually explicit material to adults who want it?

The interested people can find, on the Net information about "The Availability of Bomb making Information on the Internet".

There are many similarities between the controversy about bomb-making information on the Net and the controversy about pornography Also, in both cases, there is a real, but often exaggerated, concern about access by children. For example information about how to make bombs can be found in the Encyclopaedia Britannica, to.

The ease that digital images can be modified raises other issues, some related to crime and some that are intriguing ethical and social issues. Many cameras now record digital images; they do not use film. Photos taken on film are scanned for storage and use in computerized publishing systems. How can we be sure the images we see have not been modified or faked?

There are numerous examples in history of photographs that were faked before digital technology. The ethical issues are not new, but much more people face them because image manipulation has become so easy; it is no longer reserved to the specialist with a darkroom.

The general public must become more aware of the possibility of fakery and learn to have a reasonable scepticism.

On the Internet, people can send e/mail anonymously and post messages to news/groups anonymously. The messages are processed by remailing services. The sender sends the message to the remailer, where the return address is stripped off, and the message is for sent with a coded user ID number. Replies go to the remailer site, where the message is forwarded to the intended recipient, with the replier's return address removed.

Thus people can have conversations where neither knows the identity of the other.

In the legal field a new doctrine should be elaborated in terms of information rights that will have as object protection of both the author and of the holder of the information; of the person the information refers to; of the society against the dissemination of illegal and harmful information**;** of the persons legal right to have free access to receive and send information.

The situation ICT users are facing now can be really expressed by Voltaire affirmation in terms of communication freedom:

"I disapprove of what you say, but I will defend to the death your right to say it".

5. Violation of the intellectual property rights.

The revolution in information technology is changing access to information in fundamental ways. Increasing amounts of information are available in digital form: networks interconnect computers around the globe and the World Wide Web provides a framework for access to a vast array of information, from favourite family recipes and newspaper articles to scholarly treatises and music, all available at the click of a mouse.

The value of a book or a song or a computer program is much more than the cost of the effort and materials used to print it or put it on disk. The value of a painting is higher than the cost of the canvas and paint used to create it. In general the value of intellectual and artistic works comes from creativity, ideas, research, skills, labour and other nonmaterial efforts and attributes provided by their creators.

Protection of intellectual property has both individual and social benefits: It protects the right of the creator of something of value to be compensated for what he or she has created, and, by so doing, it encourages production of valuable, intangible, easily copied creative work. Software is a relative new form of intellectual property.

Definitions and rules have been developed and are still developing gradually to extend the notion of intellectual property to software. There is disagreement about whether copyright is the appropriate protection mechanism for software. Some argue for patents, some for completely new rules designed specifically for software and others argue that there should be no restrictions on copying software [11].

The increasing use of electronic media and computer networks has created new problems for protection of literary, artistic and musical works, as well as computer software. Multimedia program spread by INTERNET has extrapolated the possibilities for violation of the intellectual property rights.

Transposition of one intellectual work in electronic form leads to new problems. The cost of imitation and distribution using computer network of a counterfeit product can be reduced a lot. The authentic producers of music, film, texts in digital form have problems in fixing the distribution price of their works in copies, competitors that offer substitutes of these works can, at any time, lower the price. New computer, storage and communications technologies have made copying extremely easy and cheap because the digital signals 1 or 0 can be sent around the world by some clicks of the mouse in fact without the cost. And unlike other copying technologies, the copy of a digital file is indistinguishable from the original.

Enforcement of copyright is becoming much more difficult; some say impossible. As more and more creative work, including novels, essays and movies are distributed digitally instead of in physical books, magazines and tapes.

Solving this problem in a way that maintains a reasonable balance between the interests of publishers and the interests of the public will not be easy.

In the digital world, even the most routine access to information invariably involves making a copy. Computer program are run by copying them from disk to memory and Web pages are viewed by copying them from a remote computer to the local PC.

Billions of dollars of software is copied illegally worldwide every year and unauthorized copying and use of software deprives publishers and developers of a fair return of their work, increase prices, reduces the level of future support and enhancement, and can inhibit the development of new software products. Purchasers and users of counterfeit or copied software face unnecessary risks: viruses, corrupt disks, or otherwise defective software; inadequate documentation; lack of technical product support available to registered users, and lack of software upgrades offered to registered users. [12]

Electronic information is volatile and easily reproduced. For this purpose respect for the work and personal expression of others is especially critical in computer environments. Violation of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and author' right violations should be grounds for sanctions against members of the community.

Conclusions

In order to successfully fight against the infringements done through ICT, a pertinent strategy at international level has to be established, as follows:

- The improving of the present legal framework in the information field;
- Technological improving – cryptography soft, to eliminate the possibility of deciphering;
- Increase of technological performances in hard manufacture, to diminish hackers possibility of action;
- Future measures against computer crime should aim at comprehensive solutions including non-legal measures and at extension of the preventive concepts, appreciated to be more efficient than the punitive ones;
- All solutions must be specified solutions between tangible and intangible property.

The strategy should be elaborated at international level and to include compulsory, at least all the countries connected at INTERNET. The adoption of different national strategy could constitute "information heavens" that, in exchange, could lead to market restrictions and national barriers in the way of information free circulation.

When elaborating the strategy it will be considered that the information is a new, different value that cannot be protected by analogy with the material items.

The more intensive use of the computers increase the separation of rich and poor, creating a two-class society, the information "haves" and "have-nots".

There is a need for government subsidies for people who cannot afford computers, or for "public spaces" on the Internet with kinds of information that commercial services may not provide.

The technological advances brought by computers and their extraordinary pace of development can cause dramatic impact on people's lives.

To some, who see computers as a de-humanizing tool that reduces the quality of life or as a threat to the status quo and their well-being, this is frightening and disruptive.

Others see the development of computer technology challenging and exciting opportunities.

Do computers have an overall positive or negative impact? In general, when we are evaluating a new technology like ICT, we should not compare it to some ideal of perfect service or zero side effects and risk.

That is impossible to achieve in most aspects of life. Instead, we should compare ICT to the alternatives and weigh the problems against the benefits.

I am an engineer and I think that the technology, in general, has been a major factor in bringing physical well-being, liberty, and opportunity for hundreds of millions of people to live better.

That does not mean that ICT - this relatively new wonderful technology - is without problems.

We must recognize and study such potential problems so that we reduce the negative effects of information and communications technology utilization and increase the positive ones.

Let us hope for the future.

R E F E R E N C E S

[1] Ştefan Iancu, *Some Social, Economical, Legal and Ethical Issues in Utilisation of the Information and Communications Technology*, "Information Society, The Proceedings of the Fifth International Symposium on Economic Informatics 10-13 May, 2001"**,** Editura Economică, Bucharest, 2001, pp. 746-750.

[2] Mihai Nadin, *The Civilization of Illiteracy,* Dresden University Press, Wuppertal, Germany, 1998, p. VII.

[3] **** Information technology: Transforming our Society*, http://www.ccic.gov/ac/interim/section1.html.

[4] Ştefan Iancu, *Impactul social al utilizării tehnologiei informaţiei şi comunicaţiilor,* Revista română de Sociologie, Serie nouă, Anul XVI, 2005, nr. 5-6, pp. 449-468.

[5] Mario Monti, *The Internet and privacy: what regulations?* http://europa.eu.int/comm/internal_market/en/speeches/rome0598.htm.

[6] Şt. Iancu, *Unele probleme sociale, economice, juridice şi etice ale utilizării tehnologiei informaţiei şi comunicaţiilor*, Volumul "Societatea Informaţională Societatea Cunoaşterii - Concepte, soluţii şi strategii pentru România", Coordonator *Florin Gh. Filip*, Editura Expert, Bucureşti, 2001

[7] Hugh Cornwall, *Datatheft: Computer Fraud, Industrial Espionage and Information Crime,* Heinemann, 1987, p.102

[8] **** Legal Aspects of Computer-Related Crime in the Information Society,* http://www2.echo.lu/legal/en/comcrime/sieber.html#1.

[9] **** Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime,* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41en.htm.

[10] **** Political agreement on a Common Position of the Council on a Framework for Electronic signatures* (22 April 1999), http://europa.eu.int/comm/internal_market/en/media/sign/composen/htm.

[11] Şt. Iancu, *Ingineria de la roată la inteligenţă artificială,* editura Performantica, Iaşi, 2007, pp. 343-349.

[12] **** The Digital Dilemma. Intellectual Property in the information age,* National Academy Press, Washington, D.C., 2000.