Legal protection in the field of information technology in the EU

A. Ciurea

***Abstract*—**The information and comunication technologies represent an essential side of the economy and European society. Apparently, their evolution has determined complex consequences also in the legal field, because the access and use of information technology have created new rights and obligations for the beneficiaries of this technical progress. This paper aims at presenting the most important legal consequences that arose from the activities through computer systems, according to EU and Romania regulations.

***Keywords*—**cybercrime, information technology, legal, protection.

I. Introduction

„Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures (in short, ICT infrastructures) form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal functions. Recent examples include the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008" – here is how it starts Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (Brussels, 30.03.2009)

Nowadays, it is quasi-unanimously accepted that information represents a fundamental element in the structure of the universe along with matter and energy.

Therefore, information technology has an overall major impact on daily life, seriously influencing all its facets: social, political, economic as well as private life.

However, this impact has both positive, beneficial effects and negative, harmful ones; the latter are equally difficult to predict and stop as the technology expansion of the last decades.

Under these circumstances, the regulation of new rights and obligations has become an issue of global concern, not only national, that led to the access and use of information technology for the beneficiaries of this technical progress.

Legislation in this field has not been easy at all, because the legal consequences are very complex; consequently, it was necessary to create new legal concepts, which were challenging for jurists, IT specialists and engineers.

We will present below some of the most important legislations of EU and Romania.

II. Legislation of EU

Over time, the European Union bodies have taken steps to regulate activities in cyberspace, especially in the issue of cyber-crime which brings great loss in the economic, social and political fields.

We mention here that cyber-crime is reflected in the following activities:

- activities that affect the private life: the collection, modification or disclosure of personal data;
- activities to disseminate pornographic, racist, violent materials;
- crime and economic sabotage;
- activities of infringement of intellectual property.

Thus, a very important document is Recommendation no. (89)9 on computer-related crime which was formulated in 1989 by the Council of Europe, recognizing „the importance of an adequate and quick response to the new challenge of computer related crime» and taking into account „that computer-related crime often has a transfrontier character". Thus, the Member States were recommended to: „1. Take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime elaborated by the European Committee on Crime Problems, and in particular the guidelines for the national legislatures; 2. Report to the Secretary General of the Council of Europe during 1993 on any developments in their legislation, judicial practice and experiences of international legal co-operation in respect of computer related crime." In 1995, was developed Recommendation R(95)13 concerning Problems of Criminal Procedure Law Connected with Information Technology.

This recommendation was prompted by the unprecedented development of information technologies and their application in all sectors of contemporary society, and the risk that electronic information systems can be used to commit criminal offenses. Council of Europe noted that the laws of criminal procedure rights of Member States provided us these systems suitable for searching and collecting evidence during criminal investigations.

Thus, using these recommendations, a set of principles and rules were established that must be included in criminal legislation for states to carry out the investigations into electronic information systems. Specifically, the recommendations concern a search and seizure, electronic surveillance, electronic evidence, working with the investigating authorities, international judicial cooperation, etc. An important moment was at the G8 summit in Denver in 1997. At the end of the summit a release was presented that includes 10 principles and 10 lines of action to combat cyber-crime. First, it was found that this type of crime has two forms: „First, sophisticated criminals are targeting computer and telecommunications systems to obtain or alter valuable information without authority and may attempt to disrupt critical commercial and public systems. Second, criminals, including members of organized crime groups and terrorists, are using these new technologies to facilitate traditional offenses."

We emphasize that these ideas were later incorporated into Recommendations and Guidelines. Because of their importance, we will present these fundamental principles.

Thus, the 10 principles are: I. There must be no safe havens for those who abuse information technologies. II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred. III. Law enforcement personnel must be trained and equipped to address high-tech crimes. IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized. V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime. VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime. VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides. VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed. IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence. X. Work in this area should be coordinated with the work of other relevant international fore to ensure against duplication of efforts.

In support of these principles the following work plan has been developed:

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.

2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.

3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.

4. Consider issues rose by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.

5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.

6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.

7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.

8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.

9. Encourage internationally-recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.

10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions. The climax was that of adoption of Convention on Cyber-crime (Budapest 2001).

The Convention and its Explanatory Report have been adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001) and the Convention has been opened for signature in Budapest, on 23 November 2001, on the issue of the International Conference on Cyber-crime. The Explanatory Report states that:

« 1.The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. Many tasks have become easier to handle. Where originally only some specific sectors of society had rationalized their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities.

2. A conspicuous feature of information technology is the impact it has had and will have on the evolution of telecommunications technology. Classical telephony, involving

the transmission of human voice, has been overtaken by the exchange of vast amounts of data, comprising voice, text, music and static and moving pictures. This exchange no longer occurs only between human beings, but also between human beings and computers, and between computers themselves. Circuit-switched connections have been replaced by packet-switched networks. It is no longer relevant whether a direct connection can be established; it suffices that data is entered into a network with a destination address or made available for anyone who wants to access it.

3. The pervasive use of electronic mail and the accessing through the Internet of numerous web sites are examples of these developments. They have changed our society profoundly.

4. The ease of accessibility and search ability of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical distances, has lead to an explosive growth in the amount of information available and the knowledge that can be drawn there from.

5. These developments have given rise to unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behavior can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries. The recent spread of detrimental computer viruses all over the world has provided proof of this reality. Technical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behavior.

6. The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society."

More specifically, The Convention aims principally at (1) harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation. The Convention, accordingly, contains four chapters: I. Use of terms; II. Measures to be taken at domestic level – substantive law and procedural law; III. International co-operation; IV. Final clauses.

We mention that Romania ratified the Convention from Budapest through Law no.64/2004.

We enumerate other regulations of the EU bodies regarding information technology: Directive 2009/24/CE of the European Parliament and the Council in 23 April 2009 on the legal protection of computer programs, Commission Communication to the European Parliament, Council, the European Economic and Social Committee and the Committee of Regions - "Protecting Europe from cyber attacks and major disturbance: improving the training, security and resistance" (2009), 2005/222/JAI Framework Decision of the Council in 24 February 2005 regarding attacks against information systems etc.

Here are the challenges for Europe raised in Commission Communication to the European Parliament, Council, the European Economic and Social Committee and the Committee of Regions - "Protecting Europe from cyber attacks and major disturbance: improving the training, security and resistance" (2009):

"1. Uneven and uncoordinated national approaches

Although there are commonalities among the challenges and the issues faced, measures and regimes to ensure the security and resilience of CIIs, as well as the level of expertise and preparedness, differ across Member States.

A purely national approach runs the risk of producing a fragmentation and inefficiency across Europe. Differences in national approaches and the lack of systematic cross-border cooperation substantially reduce the effectiveness of domestic countermeasures, inter alia because, due to the interconnectedness of CIIs, a low level of security and resilience of CIIs in a country has the potential to increase vulnerabilities and risks in other ones.

To overcome this situation a European effort is needed to bring added value to national policies and programmes by fostering the development of awareness and common understanding of the challenges; stimulating the adoption of shared policy objectives and priorities; reinforcing cooperation between Member States and integrating national policies in a more European and global dimension.

2. Need for a new European governance model for CIIs Enhancing the security and the resilience of CIIs poses peculiar governance challenges.

While Member States remain ultimately responsible for defining CII-related policies, their implementation depends on the involvement of the private sector, which owns or controls a large number of CIIs.

On the other hand, markets do not always provide sufficient incentives for the private sector to invest in the protection of CIIs at the level that governments would normally demand.

To address this governance problem public-private partnerships (PPPs) have emerged at the national level as the reference model. However, despite the consensus that PPPs would also be desirable on a European level, European PPPs have not materialised so far.

A Europe-wide multi-stakeholder governance framework, which may include an enhanced role of ENISA, could foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures. This framework would bridge the gap between national policy-making and operational reality on the ground.

3. Limited European early warning and incident response capability

Governance mechanisms will be truly effective only if all participants have reliable information to act upon. This is particularly relevant for governments that have the ultimate responsibility to ensure the security and well-being of citizens.

However, processes and practices for monitoring and reporting network security incidents differ significantly across Member States. Some do not have a reference organisation as a monitoring point. More importantly, cooperation and information sharing between Member States of reliable and actionable data on security incidents appears underdeveloped, being either informal or limited to bilateral or limitedly multilateral exchanges. In addition, simulating incidents and running exercises to test response capabilities are strategic in enhancing the security and resilience of CIIs, in particular by focusing on flexible strategies and processes for dealing with the unpredictability of potential crises. In the EU, cybersecurity exercises are still in an embryonic state. Exercises running across national boundaries are very limited. As recent events showed, mutual aid is an essential element of a proper response to large-scale threats and attacks to CIIs.

A strong European early warning and incident response capability has to rely on wellfunctioning National/Governmental Computer Emergency Response Teams (CERTs), i.e. having a common baseline in terms of capabilities. These bodies need to act as national catalysers of stakeholders' interests and capacity for public policy activities (including those related to information and alert sharing systems reaching out to citizens and SMEs) and to engage in effective cross-border cooperation and information exchange, possibly leveraging existing organisations such as the European Governmental CERTs Group (EGC).

4. International cooperation.

The rise of the Internet as a key CII requires particular attention to its resilience and stability.

The Internet, thanks to its distributed, redundant design has proven to be a very robust infrastructure. However, its phenomenal growth produced a rising physical and logical complexity and the emergence of new services and uses: it is fair to question the capability of the Internet to withstand the rising number of disruptions and cyber-attacks.

The divergence of views on the criticality of the elements making up the Internet partly explains the diversity of governmental positions expressed in international fora and the often contradicting perceptions of the importance of this matter. This could hinder a proper prevention of, preparedness for and ability to recover from threats affecting the Internet. For example, the consequences of the transition from IPv4 to IPv6 should also be assessed in terms of CII security.

The Internet is a global and highly distributed network of networks, with control centres not necessarily following national boundaries. This calls for a specific, targeted approach in order to ensure its resilience and stability, based on two converging measures. First, achieving a common consensus on the European priorities for the resilience and stability of the Internet, in terms of public policy and of operational deployment. Secondly, engaging the global community to develop a set of principles, reflecting European core values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations. These activities would build upon the recognition by the World Summit on Information Society of the key importance of the stability of the Internet."

The Commission proposed five pillars to tackle these challenges:

"1) Preparedness and prevention: to ensure preparedness at all levels;

(2) Detection and response: to provide adequate early warning mechanisms;

(3) Mitigation and recovery: to reinforce EU defence mechanisms for CII;

(4) International cooperation: to promote EU priorities internationally;

(5) Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures."

III. Legislation in Romania

We will present bellow the most important Romanian legislation on information technology. These regulations cover both positive aspects - the regulation of services which make use of electronic devices and facilitate activities and people communication in different sectors, and negative aspects - the incrimination of infractions in relation to cyber-crime.

Thus, it is worth to be mentioning: Law no.365/2002 on electronic commerce, Government Ordinance no.113/2009 on Payment Services, Law no.8/1996 on copyright, Law no.455/2001 on electronic signatures, Regulation no. 6 of 11 October 2006 on the issue and usage of electronic payment instruments and relationships between participants in transactions with these instruments, Law no. 677/2001 on people protection regarding personal data processing and free movement of such data, Law no. 506/2004 on the processing of personal data and privacy in electronic communications sector, Law no.102/2005 on the establishment, organization and functioning of The National Supervisory Authority For Personal Data Processing and protection of personal data, Law no.161/2003 on some measures to ensure transparency and the exercise of public dignities, public functions and business community, preventing and sanctioning corruption, Government Resolution no.195/2010 on approving the National Strategy "e-Romania".

A recent and controversial legislative act, especially given the costs involved for the Romanian State is Government Resolution no.195/2010 on approving the National Strategy "e-Romania". Ministry of Communications and Information Society (MCSI) propose a national strategy, together with an action plan which will lead soon to guide the entire public sector to the information society towards knowledge-based society, the main instrument of action being the e-Government system. The strategy will be implemented during 2010-2013, three components are considered:

- the broad understanding of the term "e-Government", here are the various technologies that help improve the quality of public services (not only refers to the Internet, expanding coverage area but also to telephone interaction of the citizen or company with the administration, payment of fees by telephone messages, informing through TV networks etc.);
- integration strategy in the broader concept of 'Digital Romania", here are also the elements related to increasing participation, permanent access, increase of public confidence in Government, contribution to economic growth;
- implementation is still regarded as being continuous, covering a great period of time, permanently adapted to new technologies. It is suggested a unified vision for developing a coherent and integrated national system for online public services dedicated to citizens and the business community.

On the other hand, regarding the cyber-crime field, Law no.161/2003 is highly significant on measures to ensure transparency and the exercise of public dignities, public functions and the business community, preventing and sanctioning corruption. It contains a chapter entitled "Prevention of cyber-crime." In this chapter are described and incriminated a range of offenses, crimes against the confidentiality and integrity of data and information systems, child pornography through computer systems.

According to art.36, "in order to ensure the security of the computer systems and the protection of the personal data, the authorities and public institutions with competence in the domain, the service providers, the non-governmental organizations and other representatives of the civil society carry out common activities and programs for the prevention of cyber-crime".

More specially, the following are incriminated: the illegal access to a computer system, the illegal interception of any transmission of computer date that is not published to; the illegal alteration, deletion or deterioration of computer data of the access restriction to such data; the unauthorized data transfer from a computer system; the serious hindering, without right, of a computer system operation, by the introducing, transmitting, altering, deleting or deteriorating computer data or by restricting the access to these data. It also constitutes criminal offenses: the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer programme designed or adapted fro the purpose of committing one of the offences; the production, sale, import, distribution or making available, in any other form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of one of the offences; the input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to these data, resulting in inauthentic data, with the intent to be used for legal purposes.

Causing the loss of property to a person by the input, alteration of deletion of computer data, by restricting the access to such data or by preventing in any way the operation of a computer system, in order to obtain an economic benefit for oneself or for another is also punished.

« As an expression of international desideratum for prohibition of child pornography, art. 51 paragraph. 1 of Law no. 161/2003 is found reproduced, in part, unfortunately, the art. 9 of the Convention, article with marginal name "offences related to child pornography" ». [3]

More specially, the Romanian legislative defines « Child pornography through information systems» as: « Producing for the purpose of its distribution, offering or making available, distributing or transmitting, procuring for oneself or another of child pornography material, or possessing, without right, child pornography material within a computer system or computer data storing device is considered a criminal offence and is punished with imprisonment from 3 to 12 years.»

We emphasize that these regulations were the object of several reviews in legal doctrine and jurisprudence of Romania. Romanian authors sometimes criticized these texts as not sufficiently clear and comprehensive, failing to cover all situations arising in practice. [1,2,3,4]

IV. Case study

We will following present a widely promoted case in Romania, from the last 3 years, because it concerns the access without any right of the e-mail servers where messages of a known lawyer were stored.

This case concerns ordinary people and - at first sight - only their personal interests. However, it is a warning for the way computer fraud may affect at a very personal level the life of any person. Also, it is an example in which- even starting from personal (private) interests – a much larger number of people has been affected willingly or unwillingly.

On 05.09.2007 person A noticed the Police regarding the disappearance of his wife on 30.08.2007 who was a lawyer.

Before announcing the disappearance, on 02.09.2007, person B, friend of the couple suggested to A should access the Yahoo Messenger application in order to verify the contents of the discussions between the missing lawyer and other people.

Then the lawyer’s husband asked for help to a person specialized in IT services, C person, whom he “convinced” to access also the g-mail correspondence of the lawyer; he became known under the nickname “the hacker” given by the public opinion.

Moreover, after accessing the electronic correspondence, the lawyer's husband made public his wife's messages through television. These massages contained information about the personal life of the lawyer, but also her professional relations with her clients.

Under these circumstances, the lawyer's parents and the Lawyer Bar made a criminal complaint against the three persons A, B and C for committing the offenses of "accessing without right to information systems", "restricting without right the access to information data", and also "the unauthorized information data transfer".

As a consequence of these complaints, the criminal investigation body began search and decided on 15 January 2008, the beginning of criminal prosecution for the lawyer's husband, for committing the offenses of "incitement" to the access without right to information systems, instigating restriction with no right to the access to information data and instigating the unauthorized transfer of information data, deeds from the offences. Also, person B was accused of complicity in committing the mentioned offenses, and person C was indicted as the offenses' author without the right of access the information systems, restriction without right of the access to information data and unauthorized transfer of information data.

The perpetrators told the investigating bodies their purpose was to clarify where she could be found.

Initially, at the suggestion of friend B, the husband accessed the "Yahoo Mess" application and noticed that the Messenger ID was displayed, the password was stored; by pressing the "Sign in" button they opened the Messenger application and saw a box with 3 offline messages sent on the e-mail from the address having the ID abc@yahoo.com.

When they took this decision, the perpetrators took into consideration the possibility that the lawyer set the automatically log in, choosing the option that the username and password to be saved, a situations that allowed them to check the e-mail messages.

From the content of one of the offline messages between the lawyer with the ID abc@yahoo.com and another person with the ID xyz@yahoo.com, it resulted that a close relationship was between them. This thing determined the lawyer's husband to access the sent e-mails folder from the e-mail address abc@yahoo.com to xyz@yahoo.com.

The husband noticed that one of the emails had an attachment with a reservation voucher for two seats in a Dubai hotel for his wife and another man. Thus, the husband transferred these messages on the hard disk of his computer, creating a folder named "the cheaters".

The following days, at the husband's request, person B transferred on a stick the content of the mentioned above folder and sent the content of the messages to the email address of C's sister.

The statements of the three persons, during the criminal prosecution, were entirely different: the lawyer's husband refused to give statements, using "the right of silence", person B declared to be innocent, while person C recognized guilt and cooperated with the investigators.

The accomplice C defended claiming that the owners or the administrators of the information systems (to which access is forbidden or restricted to certain categories of users) had the obligation to warn regarding legal conditions to access and use, and also the legal consequences of this access without right, and the warning had to be accessible to each user.

Also, person B showed that in the case file there was evidence that proved C frequently used the "Yahoo Messenger" application using the wife's ID and password. These aspects should have led the prosecutors to the conclusion that C had the wife's agreement, so there was no access without right.

Criticism is not justified by reference to the fact that the access to a computer system, in order to be legal, requires that the person who uses any application is the owner of the ID and password. We emphasize that the particular legal subject of the offence of accessing without right to a computer system (provided by art.42, paragraph 1 in the Law no.161/2003) is the social relations aiming the information systems, its inviolability and which are capable of ensure confidentiality and integrity of data and computer systems.

The access without right to a computer system means regarding law, that person is in one of the following situations:

- is not authorized on the grounds of law or any contract;
- goes beyond the authorization;
- does not have the permission from the natural or legal person responsible by law to provide, operate, manage or control a computer system or to conduct scientific research or to perform any other operation in a computer system.

In this case, person C was not authorized – neither on the grounds of law nor any contract – to access "Yahoo Messenger" application using his wife's ID and password. The access was made with no right, even if the ID and password were automatically saved.

Moreover, person C obtained without right the informational data from his wife's messages and then transferred them unauthorized, on another data storage medium with the help of his friend B.

The accomplice B also claimed that the criminal prosecution body misinterpreted the concept of the unauthorized transfer of informational data. According to B, the transfer implies a relocation of data from a location to another.

This statement can not be sustained because the transfer can be done with or without relocation. Thus, the transfer can be done by copying, downloading, covering a large range of information operations; opposite to the accomplice's statement, the transfer does not mean only relocation of data in another information system and deleting information from the system from which was made the transfer.

It can not be argued that any action took place that made any material, tangible and verified change – as evidenced by the computer search and the technical-scientific finding reports in this field.

However, regarding B's complicity, the prosecutors decided that the prejudice to the social values is minimal. Regarding the actual content of B's deed, it is irrelevant and has no social threat. It was considered that the circumstances B's deed took place, the purpose and the consequences were not a social threat of an offense.

It was taken into account that at the time the deed took place by the accomplice B, he had been convinced by the lawyer's husband that the wife left the marital home, being involved in another relationship. At that moment, husband C was not yet investigated for the offense of first-degree murder of his wife.

Consequently, person B was not sent to trial for committing the previous mentioned offenses as complicity. But, it was decided that the accomplice's deed had to be punished with an administrative fine.

As far as the A and C defendants are concerned, the evidence given in the case proved that "the defendant A with the help of defendant B, accessed without right the computer system of the e-mail servers where the messages of the lawyer E were kept and determined defendant C access, also with no right, the computer system of e-mail servers, where were kept the messages from the lawyer E's e-mail address, so violating the security measures by fraudulently using the username and password autentification – without holding them – and transffering information data in other computer systems".

Under these circumstances, on 16.02.2009, the prosecutors ordered the suing of defendants A and C for committing the offenses of "accessing with no right the computer systems" from the art. 42 paragraphs 1, 2 and 3 in Law no.161/2003, with the procedure of art.41 paragraph 2 from the Criminal Code, „restriction with no right of access to information data" from art.44 paragraph 1 in Law no.161/2003, applying art.41 paragraph 2 in Criminal Code, „unauthorized transfer of information data" from art.44 paragraph 2 in Law no.161/2003, applying art.41 paragraph 2 in Criminal Code.

The case was submitted to the Criminal Section of Territorial Court, under jurisdiction, but the result was not delivered.

V. Conclusion

The easy access to information, speed of their dissemination and the possibility to store an impressive amount of data are just some of the advantages offered by the new technology. Currently, the areas of communications, transport of any kind (traffic control), banking, education, health apply the latest discoveries in the field.

Romania seeks to move towards knowledge-based society, building the information society, the aim is to achieve the e-Romania service, with its strategic component of e-Government. Achieving this objective means repositioning Romania and confers an advantage for sustainable economic growth, positive international image, rapid convergence in Europe, inclusion, strengthening areas of high competence. The concept of 'information society' is very large, covering practically all sectors of the government program. The main goal is to create a society that includes all citizens' access to public services provided in electronic form, by increasing capacity to use information society services, reforming the government operational models and increase operational efficiency through appropriate use of information and communications technologies, namely increasing competitiveness in the business environment by using advanced information technology and communications. The set of targets and national priorities is based on current needs and realities of Romanian society, while being consistent with requirements at European level, and is accompanied by financing mechanisms and cooperation mechanisms. To achieve a functional national system is particularly important to involve all decision-makers in public administration, organizations from business community and professional and scientific bodies, so projects of national electronic services and applications will be made in a clearly defined framework, with specific roles and responsibilities

However, we note that a certain dependence on these modern means of work and communication has developed, both in professional and private life.

More earnest is that the relatively easy access and mass use of these, generates vulnerability in the system. Cracks and minor errors in the system can cause widespread economic, political or almost incalculable human damage; opportunities initially unknown were created, unfortunately for intentionally committing new crimes and new frauds.

Therefore, jurists, IT specialists, engineers, and also sociologists, psychologists must work together in order to find tools for establishing a balance in the technical, legal, social and mental field, between beneficial and the extremely serious effects that can generate information technology for humanity. An interdisciplinary approach to this complex problem is the only solution for us to succeed in our attempt to avoid self-destruction by means originally created for a purpose essentially positive.

"Security and resilience of CIIs are the frontline of defence against failures and attacks. Their enhancement across the EU is essential to reap the full benefits of the information society. To achieve this ambitious objective an action plan is proposed to reinforce the tactical and operational cooperation at the European level. The success of these actions depends on their effectiveness to build upon and benefit public and private sector's activities, on the commitment and full participation of Member States, European Institutions and stakeholders … Lastly, enhancing the security and resilience of CIIs is a long term objective, whose strategy and measures need regular assessments. Therefore, since this goal is consistent with the general debate on the future of network and information security policy in the EU after 2012, the Commission will initiate a stock-taking exercise toward the end of 2010, in order to evaluate the first phase of actions and to identify and propose further measures, as appropriate." ("Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" Brussels, 30.03.2009)

ACKNOWLEDGMENT

The research was supported by the Grant „Parteneriate" no. D3: 21 062/2007, financed by the Romanian Ministery of Education.

REFERENCES

[1] Dobrinoiu, M., *Crimes in the information field,* C.H. Beck Printing House, 2006.

[2] Dobrinoiu, M., Illegal acces to e-mail, *Penal Law Review*, No.3, 2008, pp.122-128.

[3]] Spiridon, I., Reflections on Romanian Legislation in the cyber-crime field, *"Dreptul" Journal,* No. 6, 2008, pp.237.

[4] Fat, S., Remarks on some crimes in Law no. 365/2002 and in Law no. 161/2003, *"Dreptul" Journal,* No. 7, 2008, pp.231.

[5] A. Ciurea, „Legal Implications of Accessing and using Information Technology. Legislation in Romania and in the EU" in *Proc. of the 14-th WSEAS CSCC,* Corfu, 2010 pp. 256-260

[6] Hira Sathu, WarDriving: Technical and Legal Context*, Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics,* Istanbul, Turkey, May 27-29, 2006, pp162-167.

[7] Wasniowski, R. A., Data Base Support for Intrusion Detection with Honeynets, *Proceedings of the 6th WSEAS Int. Conference on TELECOMMUNICATIONS and INFORMATICS,* Dallas, Texas, USA, March 22-24, 2007.

[8] G. Rigopoulos, N. V. Karadimas, „Increasing Ethical Awareness of IT Students through Online Learning", in *Proceedings of the 6th WSEAS International Conference on Applied Informatics and Communications,* Elounda, Greece, August 18-20, 2006 (pp265-269).