12th NISPAcee Annual Conference

"Central and Eastern European Countries inside and outside the European Union: Avoiding a new divide"

Vilnius, Lithuania, May 13 – 15, 2004

VI. Working Group on e-Government

PREVENTING AND FIGHTING AGAINST CYBERCRIME (Romanian case)

Razvan VIORESCU, Lecturer PhD*

Abstract

Romania has a well-developed communications infrastructure, which offers great potential for introducing new services and also facilitates the reduction of the digital divide within the country. The total liberalization of the telecom market on January 1st, 2003 set the conditions for the availability of better and diversified services at lower costs for all citizens.

e-Government was aggressively promoted in the past two years as it is considered the best way of organizing public management in order to increase efficiency, transparency, accessibility and responsiveness to citizens, as well as to reduce bureaucracy and corruption, through the intensive and strategic use of Communications and Information Technology in the inner management of the public sector, as well as in its daily relations with citizens and users of public services.

Since 2001, approximately 30 pilot projects were finalized, projects that aimed, in the first phase, to simply prove the benefits of a solution to be extended according to a precise calendar in order to assure better ways of solving problems for as many people as possible. One of these projects, the payment of local taxes via the Internet, is currently used in 50% of the Romanian municipalities.

Today, the laws concerning the protection of individuals with regard to the processing of personal data, processing of personal data and the protection of privacy in the telecommunications sector, the electronic signature, the cyber crime, the electronic commerce, e-procurement and e-tax are already in force. Also, a new legislative package regarding electronic communications was approved in 2002, which is in line with the newest European Directives in domain - an European premiere.

Also, by the adoption of the anti-corruption Law, a financial disclosure solution is used in Romania since some months ago. By publicizing on line the financial statements of public officials, two objectives are served: the first is to monitor changes over time in the economic situation of public officials; the second is to detect and prevent potential conflict of interests between public officials and the private sector.

Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks and taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the EU Convention on Cybercrime is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence, Romanian authorities have adopted a Legal framework on preventing and fighting cyber-crime.

Romanian legal framework on preventing Cybercrime

The new legislation (**Law no.** 161/ 2003 **on Certain Steps for Assuring Transparency in Performing High Official Positions, Public and Business Positions, for Prevention and Sanctioning the Corruption** (**Title III Preventing and Fighting Cyber Crime)** regulates prevention and fighting cyber crime, through specific prevention, identification and sanctioning measures of offences committed through computerized systems, by ensuring the observance of human rights and the protection of personal character data.

* Lecturer Phd., Department of Public Administration, University "Stefan cel Mare" Suceava, Romania

The Convention on Cybercrime was signed by Romania at 23 11 2001 and will be ratified by the Parliament in the future.

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the Convention on Cybercrime is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence.

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (CDPC) on cybercrime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences, as well as to Resolution N° 3, adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime.

According to provisions of the European Convention on Cybercrime, Romanian Law defined the specific terms as follows:

- ***computerized system*** any device or aggregate of devices interconnected or being in a functional relation, one or more of which endure the automatic data processing, with the help of an computer program;
- ***automatic data processing*** - the process through which data of a computerized system are processed through a computer program;
- ***computer program*** - a set of instructions that can be executed by an computerized system for the purpose of obtaining a previously determined result;
- ***electronic data*** - any representation of facts, information or concepts in a form that can be processed through a computerized system. In this category, any program that can determine the execution of a function by a computerized system shall be included;
- ***service provider:*** any natural person or legal entity providing users with the possibility to communicate through computerized systems; or any other natural person or legal entity processing or storing electronic data for persons provided by point 1 and for the users of services provided by them ;
- ***data referring to the informational traffic-*** any electronic data referring to a communication performed through a computerized system and produced by it, which represents a component of the communication chain, indicating the communication source, destination, route, time, date, amount, volume and duration, as well as the type of service used for communication;
- ***data referring to users-*** any information that can lead to the identification of a user, including the type of communication and the used service, his/her e-mail address, mail address, geographic location, phone numbers or any other access numbers, and the way of payment of the respective service, as well as any other data that can lead to the identification of a user;
- ***security measures-*** the use of specialized procedures, devices or programs, with which help access to a computerized system is limited or prohibited for certain categories of users;
- ***Juvenile pornography materials*** - any material presenting a juvenile who has an explicit sexual behavior or an adult person presented as a juvenile, who has an explicit sexual behavior, or images which, even though do not show a real person, simulate, in a credible way, a juvenile having an explicit sexual behavior.

As consequence **a person being in the following situations shall act illegally**:

- is not authorized under the law or a contract;
- exceeds the limits of the authorization;
- was not granted the permission by the person competent to grant it under the law, to use, administer or control a computerized system or to conduct scientific research, or to perform any other operation in a computerized system.

Governmental Prevention Measures on Cyber Crime

In order to ensure the security of computerized systems and the protection of personal character data, public authorities and institutions having competencies in the area, service providers, non - governmental organizations and other representatives of the civil society shall carry out common activities and programs of prevention of cyber crime.

Public authorities and institutions having competencies in the area, in collaboration with service providers, non - governmental organizations and other representatives of the civil society shall promote policies, practices, measures, procedures, and minimum standards of security of the computerized services.

Public authorities and institutions having competencies in the area, in collaboration with service providers, non - governmental organizations and other representatives of the civil society shall organize awareness and information campaigns regarding cyber crime and the risks to which computerized system users are exposed.

The Ministry of Justice, the Ministry of Interior, the Ministry of Communication and Information Technology, the Romanian Intelligence Service and the Foreign Information Service shall create aid permanently update databases with respect to cyber crime. The National Institute of Criminology subordinated to the Ministry of Justice shall conduct periodically studies for the purpose of identification of the reasons determining, and of the factors favoring cyber crime.

The Ministry of Justice, the Ministry of Interior, the Ministry of Communication and Information Technology, the Romanian Intelligence Service and the Foreign Information Service shall conduct special training and development programs for the personnel having competencies in prevention and fighting cyber crime.

Owners or administrators of computerized systems, to which access is restricted or prohibited for certain categories of users, have the obligation to warn users with respect to the legal terms of access and use, as well as to the legal consequences in case of illegal access to such computerized systems. The warning shall be available to all users.

Offences

Offences against Confidentiality and Integrity of Data and Computerized Systems

Access without an authorization to a computerized system shall be considered an offence and shall be sanctioned by a jail sentence of between 3 months to 3 years or by a fine. This offence committed for the purpose of obtaining electronic data, shall be sanctioned by jail sentence of between 6 months to 5 years. If the offence is committed by violation of the security measures, the jail sentence shall be of between 3 to 12 years.

Interception without an authorization of a transmission of information, which has not a public character and which is intended for a computerized system, comes from such a system or is performed within a computerized system, shall be considered an offence and shall be sanctioned by a jail sentence of between 2 to 7 years. The same sentence shall be applied to interception without an authorization of an electromagnetic emission coming from a computerized system containing data which have not a public character.

The deed to modify, delete or alter electronic data or to restrict access to such data, without an authorization, shall be considered an offence and shall be sanctioned by a jail sentence of between 2 to 7 years. The unauthorized transfer of data from a computerized system shall be sanctioned by a jail sentence of between 3 to 12 years. Also, the unauthorized transfer of data from an electronic data storage device shall be sanctioned by the jail sentence provided by previous paragraph .

Serious disturbance, without an authorization, of a computerized system functioning, through introduction, transmission, modification, deleting or alteration of electronic data or through restricting access to such data shall be considered an offence and shall be sanctioned by a jail sentence of between 3 to 15 years.

Other offences and shall be sanctioned by a jail sentence of between 1 to 6 years:

a) the deeds to produce, sell, import, distribute or make available, under any form, without an authorization, a computer device or program designed or adapted for the purpose of committing any of the offences above mentioned.

b) the deeds to produce, sell, import, distribute or make available, under any form, without an authorization, of a password, access code or any other such electronic data, which allow full or partial access to a computerized system, for the purpose of committing any of the offences above mentioned;

The same sanction shall be applied for unauthorized possession of an computer device, password, access code or of any other electronic data of the ones.

Cyber Offences

Unauthorized introduction, modification or deleting of electronic data, or unauthorized restriction of access to such data, resulting in data which do not correspond to reality, for the purpose to be used for producing a certain legal consequence, shall be considered an offence and shall be sanctioned by a jail sentence of between 2 to 7 years.

The deed of causing financial damages to a person through introduction, modification or deleting electronic data, through restricting access to such data or through preventing the functioning of a computerized system in any other way, for the purpose of obtaining material benefits for oneself or for other person, shall be considered an offence and shall be sanctioned by a jail sentence of between 3 to 12 years.

Juvenile Pornography through Computerized Systems Offences

Producing for the purpose of dissemination, offering or making available, spreading or transmitting, procurement, for oneself or for other persons, of juvenile pornographic materials through computerized systems, or unauthorized possession of juvenile pornographic materials in a computerized system or in an electronic data storage device, shall be considered offences and shall be sanctioned by a jail sentence of between 3 to 12 years and deprivation of certain rights.

Any attempt to commit the offences above mentioned shall be sanctioned .

Procedure Provisions

In emergency and well - grounded situations, if there are grounded data or evidence related to the preparation or commission of an offence through computerized systems, immediate preservation of electronic data or of data referring to informational traffic, which are in danger to be destroyed or altered may be ordered, for the purpose of producing evidence or of identifying the perpetrators. During a criminal investigation, data preservation shall be ordered by the prosecutor, through a motivated ordinance, at the request of the criminal investigation body or *sua sponte*, while during the trial, preservation shall be ordered by the court, through an intermediate decision. The measure provided shall be ordered for a period of time that shall not exceed 90 days, and may be prolonged just once, for a period that shall not exceed 30 days.

The prosecutor's ordinance or the court's intermediate decision shall be communicated immediately to any service provider or to any person in whose possession the data are, the latter having the obligation to preserve the data immediately, in terms of confidentiality. Until the criminal investigation is finalized, the prosecutor has the duty to notify in writing the persons against whom the criminal investigation is conducted and whose data were preserved.

Within the term of 90 days, the prosecutor, based on a motivated authorization issued by the prosecutor expressly assigned by the attorney general of the prosecutors' office by a court of appeal or, as the case may be, by the General Attorney of the Prosecutors' Office by the Supreme Court of Justice, or the court shall issue an order of taking all objects containing electronic data, informational traffic data or data on users, from the person or service provider having them in possession, for the purpose of making copies of them, which can serve as evidence.

If objects containing electronic data or informational traffic data are not voluntarily made available to the criminal investigation bodies, for making copies after them, the prosecutor or the court shall order seizure of those objects. During the trial, the seizure order shall be communicated to the prosecutor, who takes steps for its enforcement, through the criminal investigation body.

Anytime *the investigation of a computerized system* or a data storage support is necessary for identifying and producing evidence, the competent body provided by law may order a search.In the event when, in the investigation of a computerized system or a data storage support, it is found that the searched electronic data are contained by another computerized system or storage data support and are accessible from the initial system or support, authorization of a search may be ordered immediately, for the purpose of investigation of all the computerized systems or storage supports of the searched data.

Provisions of the Criminal Procedure Code with respect to conducting a domicile search shall apply accordingly.

Access in a computerized system, as well as interception and record of communications done through computerized systems may be done when they are useful for finding the truth, while finding of a factual situation or identification of perpetrators shall not be done based on any other evidence.

Procedural measures provided shall be enforced by the criminal investigation bodies, assisted by specialized persons, who have the duty to maintain confidentiality on the performed operation, with a motivated authorization, issued by the prosecutor expressly assigned by the attorney general of the prosecutors' office by a court of appeal or, as the case may be, by the General Attorney of the Prosecutors' Office by the Supreme Court of Justice or by the Attorney General of the National Anti -Corruption Prosecutors' Office. The authorization shall be issued for maximum 30 days, with a possibility of prolongation under the same terms, for well - grounded reasons, on condition that each prolongation may not exceed 30 days. The maximum period of the authorized measure may not exceed 4 months. Until a criminal investigation is finalized, the prosecutor has the duty to notify in writing the persons against whom the measures were ordered.

Provisions of the Criminal Procedure Code referring to audio and video surveillance shall apply accordingly.

International Cooperation

The Romanian judiciary authorities shall cooperate directly, as provided by law and by observing the obligations originating from the international legal instruments to which Romania is part, with the institutions having similar competencies of other states, as well as with international organizations specialized in the area.

Cooperation may have as a subject, as the case may be, international legal assistance in the criminal area, extradition, identification, blocking, seizure and confiscation of products and instruments of offences, conducting common investigations, exchange of information, technical or any other kind of assistance in collecting and analyzing information, training of specialized personnel, as well as other such activities.

At the request of the Romanian or of other states' competent authorities, common investigations may be conducted in the Romanian territory, for tie purpose of preventing and fighting cyber criminality. Common investigations shall be conducted based on bilateral or multilateral agreements, concluded by the competent authorities. Representatives of the Romanian competent authorities may take part in common investigations conducted in the territory of other states, by observing the latter's legislation.

For the purpose of ensuring an immediate and permanent international cooperation in the area of fighting cyber criminality, the **Service for Preventing and Fighting Cyber Criminality** shall be created, as a permanently available contact agent, within the Section for Fighting Organized Crime and Anti - Drugs of the Prosecutors' Office by the Supreme Court of Justice.

The Service for Preventing and Fighting Cyber Criminality shall have the following competencies:

- to provide the similar contact agents of other states with specialized assistance and data on the Romanian legislation in the area;
- to order immediate preservation of data, as well as taking of objects containing electronic data or data referring to informational traffic, requested by a foreign competent authority;
- to enforce or facilitate enforcement of rogatory transfers of competency in cases related to fighting cyber criminality, by cooperating with all the Romanian competent authorities.

Within the international cooperation, foreign competent authorities may request the Service for Preventing and Fighting Cyber Criminality the immediate preservation of electronic data or of data referring to informational traffic, existing in a computerized system in the territory of Romania, on which the foreign authority is to submit an application of international legal assistance in the criminal area.

The request of immediate preservation shall contain the following:

- name of the authority requesting the preservation;
- a brief description of facts being subject to criminal investigation and their cause of action;
- the electronic data requested to be preserved;
- any available information, necessary to identify the holder of the electronic data and the location of the computerized system;
- utility of the electronic data and necessity of their preservation;
- the foreign authority intention to formulate an application of international legal assistance in the criminal area.

A preservation request shall be enforced for a period no shorter than 60 days, and shall be valid until the Romanian competent authorities make a decision on the application of international legal assistance in the criminal area.

If, while enforcing a request submitted, it is found that a service provider of another state is in possession of certain data on informational traffic, the Service for Preventing and Fighting Cyber Criminality shall inform without delay the requesting foreign authority on this, communicating at the same time the information necessary to identify the respective service provider.

A foreign competent authority may have access to the Romanian public sources of electronic public data, without being necessary to submit a request to the Romanian authorities for this purpose. A foreign competent authority may have access or may receive, through a computerized system existing in its territory, electronic data stored in Romania, on condition it has the approval of the competent authority, as provided by law, and to make the information available without being necessary to submit a request to the Romanian authorities for this purpose.

The Romanian competent authorities may deliver *sua sponte* to foreign competent authorities information and data in their possession, necessary for the detection of offences committed through computerized systems or for resolution of cases related to such offences by the competent authorities, in compliance with legal provisions on protection of personal character data.

Government Antifraud cybercrime initiative

The portal **eFrauda (www.eFrauda.ro)** has the mission to address fraud committed over the Internet. For victims of Internet fraud, eFrauda provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected internet fraud. For law enforcement and regulatory agencies at all levels, eFrauda offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.

eFrauda is offered to provide a method for romanian citizens and from abroad to promptly and directly communicate their complaints to romanian government agencies that are interested in investigating and taking action against internet fraud that is reported**.**

eFrauda function is to protect the suppliers and consumers of information society services, respecting the law establishment, reducing the bureaucracy, preventing and fighting against cyber crime, increasing the transparency in relation between the citizens and authorities.

In order to ensure international cooperation in the cyber-crime domain is in function a cyber-crime fighting service as a contact point available permanently from 2004.

This information portal on Cybercrime reports has an american model : IFCC.

The Internet Fraud Complaint Center (IFCC), which began operation on May 8, 2000, is a partnership between

NW3C (National White Collar Crime Center) and the Federal Bureau of Investigation (FBI). IFCC's primary mission is to address fraud committed over the Internet. This mission is met by facilitating the flow of information between law enforcement agencies and victims.

The program served a critical role for the United States starting on September 11, 2001. On that date, just hours after the terrorist attacks in New York, Pennsylvania, and metropolitan Washington, D.C., the IFCC Web site served as the mechanism by which people filed online tips with the FBI regarding these attacks. Tens of thousands of tips were received and processed in real-time in the months following the tragedies, and some of the information received proved useful in the subsequent criminal investigation. In the early part of 2002, IFCC was recognized for their work when the program was honored with the *excellence.gov award* for innovation in Electronic Government.

Overall, the IFCC 2002 Internet Fraud Report is the second annual compilation of information on complaints received and referred by IFCC to law enforcement or regulatory agencies for appropriate action. The results provide an examination of key characteristics of 1) complaints, 2) perpetrators, 3) complainants, 4) the interaction between perpetrators and complainants, and 5) success stories involving IFCC. The results are intended to enhance our general knowledge about the scope and prevalence of Internet fraud in the United States.

General IFCC Filing Information

From January 1, 2002 to December 31, 2002, the IFCC Web site received 11,636,362 "unique" Web hits (down 32% from 2001)1. IFCC averaged 969,696 Web hits per month. The number of complaints filed during the year equaled 75,063. This is a 67% increase over 2001, when 49,957 complaints were received. There were 16,838 filings in 2000, although IFCC didn't begin taking complaints until May 8 of that year. The number of complaints filed per month averaged 6,255. There was a steady rise in the number of complaints filed for each quarter of 2002, culminating with 20,325 complaints filed between October and December.

During 2002, Internet auction fraud was by far the most reported offense, comprising 46.1% of referred fraud complaints. This represents a 7.7% increase from 2001 (42.8%) levels of reported auction fraud. In addition, during 2002, the non delivery of merchandise and payment comprise 31.3% of complaints (up 54.2% from 2001), and credit and debit card fraud make up an additional 11.6% of complaints (up 23.4% from 2001). The remainder of the top ten types of activity referred by IFCC (investment fraud, business fraud, confidence fraud, identity theft, check fraud, Nigerian letter fraud and communications fraud) makes up nearly 6% of complaints.

Perpetrator Characteristics

Equally important to presenting the prevalence and monetary impact of Internet fraud is providing insight into the demographics of fraud perpetrators. Please refer to Appendix II at the end of this report for more information about perpetrator statistics by state. Perpetrators also come from a varied international background, with significant representation in Nigeria, Canada, South Africa, Romania, and Spain (see figure 1). Please find the internet crime types (Fig.2).

The statistics also highlight the anonymous nature of the Internet in facilitating fraud. The gender of the perpetrator was reported only 65% of the time, and the residence state for perpetrators was reported only 72% of the time.

Top Ten Countries by Count: Perpetrators (Number is Rank) :

1. United States – 76.7%
2. Nigeria – 5.1%
3. Canada – 3.5%
4. South Africa – 2.0%
5. Romania – 1.7%
6. Spain – 1.3%
7. Indonesia – .9%
8. Russia – .7%
9. Netherlands – .6%
10. Togo – .5%

Fig. 1. Details on the IFCC Internet Fraud Report . (http://www.ifccfbi.gov)

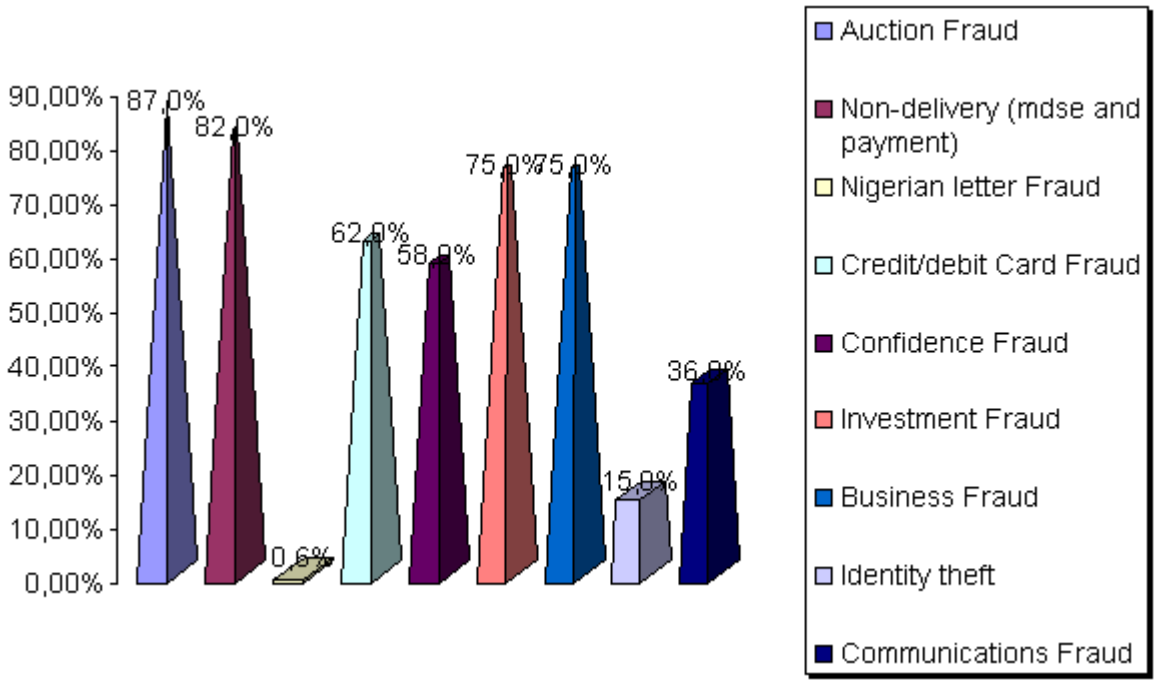

Fig.2 Details on the IFCC Internet Fraud Report .

References

*** The Convention on Cybercrime adopted on 23.XI.2001 at Budapest, Hungary

*** Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Comitted through Computer Systems

*** (Law no. 161/ 2003 on Certain Steps for Assuring Transparency in Performing High Official Positions, Public and Business Positions, for Prevention and Sanctioning the Corruption (Title III Preventing and Fighting Cyber Crime) published in the Official Gazette on 21 April 2003

- Web resources:
- **http://www.mcti.ro/** Ministry of Communications and Information Technology
- **http://www.usdoj.gov/criminal/cybercrime** Justice Department, Computer Crime and Intellectual Property Section (CCIPS)
- **http://www.fbi.gov/programs/nccs/compcrim.htm** Federal Bureau of Investigation, National Computer Crime Squad
- **http://www.dtsa.osd.mil/index.html** Defense Technology Security Administration (DTSA)
- **http://www.disa.mil** Defense Information Systems Agency (DISA)
- **http://www.ifccfbi.gov** IFCC Internet Fraud Report