FRAUD IN ELECTRONIC COMMERCE

Lecturer **Valentin – Stelian BĂDESCU**[1], PhD

Abstract

Electronic commerce is experiencing a great extent, and about the same extent fraud seeks - and sometimes is the place to impressive levels. Moreover, computer fraud and, the actors' they do not seem to suffer from the global economic recession and get as sophisticated as a legitimate business model and one of the most important dimensions of the work of modern organizations is the manipulation of information (collection, processing, storage, distribution, etc.). This component informational increasingly involves broader and more complex, with the technological advancement of computer science and globalization of human society, special measures to ensure the security of information. Cyber-crime is an illegal act committed by using a computer network (especially Internet). Cyber-crime is a subset of cybercrime.

Keywords: *e-commerce, cybercrime, system vulnerability, criminal business law*

JEL Classification: *K14*

1. Argumentum

Today, more than ever, the world is changing rapidly, globalization and internationalization are forming determinants of contemporary developments. In addition, this development is supported by digitization (software) and computerization (equipment) economic and social life, two trends that have monopolized the last decade . Companies operating internationally are made in the fortunate position of no longer prevent the natural borders of each country in their business processes. Moreover, we have a shift in trade flows, capital and production, from national to international channels. Operating campaigns, in such systems, are often large companies, and even multinational companies.

Use intensively, IT resources supporting companies, managers of any kind, which gives generous opportunities to improve performance. The production process can be organized more efficiently and economically by taking activities and their implementation by computer. Electronic forms achieved flexibility and the option to request assistance, as required, and resources search, ultimately leading to an increase in information quality. As a natural consequence, require digitization and computerization , economic, appeared commerce. This was possible due to the scale , the last time in use, the most important vehicle for information transmission " - the Internet. It represents the most extensive and complex way of communicating and a simple, but fast access to information around the globe.

2. Internet support - electronic fraud

Multiplication and expansion of e-commerce can not be separated from the challenges of fraud , money laundering , tax evasion and the like. Thus, it can put a number of questions , whether electronic forms of money will lead to an increase or decrease in these activities. Fraud, in general, has always been a major problem, but joining the Internet, e- mail and electronic banking operations have developed interest offenders to behave in a new environment , bringer of money easier and impressively large.

Risk analyzes performed so law enforcement authorities specialists , as well as those of the various institutions involved in the use of IT services , in particular electronic commerce, confirms the existence of forms of fraud which include Internet auctions, commodity supplies, cards credit, investment and international letters.

[1] Valentin – Stelian Bădescu - „Lumina” - University of South-Eastern Europe, Bucharest, Legal Research Institute of the Romanian Academy, Lawyer in the Bucharest Bar, valentinbadescu@yahoo.com

In terms of revenues, ecomerț activities can be found with ease, underground activities within legal but unreported , thus subject to taxation (tenders , delivery of goods, investments, etc.) And less in the area of illegal, which however are non-taxable and tax (child pornography). Retrieving e- commerce activities in the informal economy and their extent, remain largely unnoticed and unnoticeable because, in terms of mobility, adaptability, they outrun economic reality and even grow at rates which can hardly be achieved in the official.

Electronic commerce is experiencing a great extent, and about the same extent fraud seeks - and sometimes is the place to impressive levels . However, computer fraud and , the actors ' they do not seem to suffer from the global economic recession and get as sophisticated as a legitimate business model taking advantage of vulnerabilities in information systems.

3. Vulnerabilities of computer systems

One of the most important dimensions of the work of modern organizations is the manipulation of information (collection, processing, storage, distribution, etc.). This component informational increasingly involves broader and more complex, with the technological advancement of computer science and globalization of human society, special measures to ensure the security of information. The main threats to information held in the computer system of an organization they represent:

- Accidental or intentional destruction of information carrier (your HD, CDs, tapes, etc.).
- Unauthorized access to information.

These dangers are enhanced by the existence of computer networks (including the Internet) in which security means: Privacy (maintaining the privacy of information), integrity (proof that the information has been changed), authenticity (proof of identity of what the message) non - repudiation (the assurance that he who generates the message can not deny it later).

A rational approach to the security of a computer system involves the following steps:

- Risk Assessment - Defining areas of vulnerability
- Securing System - Actions to isolate and protect the system
- Recovery (recovery) - Make a plan for recovery verified incident
- Research - Concern and Results
- Definition and implementation of a security policy

Next we examine all safety issues and potential solutions both technically (at different levels of system and information) and from an organizational viewpoint.

Information security and the system can be understood as the ability to resist system with a certain level of security, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and services offered by or accessible via these networks and information systems. As mentioned, this involves the following characteristics: authenticity, confidentiality, integrity, availability, access control, key management, non-repudiation , security management.

Authenticity is purported to confirm the identity of entities or users. Authentication process should include the possibility of user anonymity for some cases of electronic transaction services . Authentication can take place on the parties to the communication and/or data source. Thus, we can distinguish two distinct categories of authentication , authentication entities pair: an entity of a pair is claimed and data origin authentication: is the alleged source of the data received.

Confidentiality is the protection of communications or stored data against interception and reading by unauthorized persons (information is not available or disclosed to persons, entities or unauthorized processes). This feature is strictly connected with the intimacy and privacy.

Integrity is confirmation that the data was sent, received or stored are complete and unaltered. This feature, in combination with authentication is very important to conduct transactions on the Internet.

Availability is defined by the fact that the data is accessible and services are operational, despite disruptive events (eg, loss of power supply, natural disasters, accidents or attacks).

Availability is a vital feature especially in a context where disturbances and disruption of communications network to disturb other critical networks (such as air transport or power supply). Access control is characteristic of the prevention of unauthorized use of a resource , including the use of resources in an unauthorized manner . Key management is characteristic that the encryption keys are generated , stored, distributed , changed , shall be stored and applied in accordance with a given security policy .

Non-repudiation refers to responsibility messages or commands to their authenticity. This feature is important for contracts between companies through electronic messages, in the sense that a contract/order shall not be later repudiated by one party (in the sense that it eliminates this possibility).

Security Management is the feature used for applying security policies in a communication network or a computer system. Securing data in an organization is through the development and implementation of security policies implemented by some security mechanisms.

A security policy is a statement of what is rational and what is not allowed in an organization. Policies are administrative directives that establish goals and responsibilities and also substantiates the interpretation and resolution of conflicts that may occur . A security policy should be conducted, concise and easy to understand and to achieve a balance between security and productivity. Such a policy must explain why it is necessary, that the areas covered, explain the consequences and define who should be contacted and who is responsible . You can define several types of policies: policies for users, physical security policies , policies for servers, network policies, etc. Once developed a security policy must be defined security mechanisms. A security mechanism is a method, a tool, a procedure for achieving a security policy. A security device is defined as a logic or algorithm that implements a security function in a particular physical device or a program. In general, there are several options for implementing a given security mechanism (eg block cipher and encryption streams for encryption). With all the security cybercrime grew in size and perfidy.

4. Cybercrime

4.1. Preliminary Issues Cybercrime

Cyber - crime is an illegal act committed by using a computer network (especially Internet). Cyber - crime is a subset of cybercrime and material specific regulation is established in Title III of Law no. 161/2003 on measures to ensure transparency in the exercise of public dignities , public functions and in the business environment , the prevention and punishment of corruption. This legislation contains provisions on combating new forms of crime occurring in the field information , ie cybercrime . Articles of harmonizing with the European Convention on Cybercrime. In Title III of the law are caught in the 5 main chapters of the computer crime and general provisions on cybercrime prevention provisions on international cooperation.

The specific regulations are found in Chapter VIII of Law . 365/2002. on electronic commerce, law transposing into our internal main provisions of Directive 2000/21/EC of the European Parliament and the Council. From the legal text are four principles: the free movement of information society services, commercial communications, conclusion of contracts by electronic means civil, liability of service providers acting as intermediaries.

Necessarily these special rules are added to the Criminal Code and Criminal Procedure Code. We dwell in the below typology of cybercrime but also issues and cybercrime prevention, through specific measures for the prevention, detection and punishment of offenses committed through computer systems, ensuring respect for human rights and protection statement.

The concept Romanian legislator, in the legal sense above defined, terms and expressions have the following meaning:

- System: any device or group of devices interconnected or related devices, one or more automatic processing of data by a computer program;

- Automatic Data Processing: the process by which data in a computer system are processed through a computer program;

- Software: a set of instructions that can be executed by a computer system to achieve a specific result ;

- Computer data: any representation of facts , information or concepts in a form that can be processed by a computer system. This category includes any software that can bring about a function by a computer system ;

- Service Provider:

1. any person or entity that provides users the ability to communicate through a computer system;

2. any other person or entity that processes or stores data for the persons referred to in section 1 and the users of these services;

- Data related to traffic information : computer data relating to a communication made by a computer system and its products, which is part of the chain of communication , indicating origin, destination, route, time, date, size, volume and duration and the type of service used for communication;

- User data: any information that may lead to the identification of a user, including the type of communication and service use, mailing address, geographic, phone numbers or other access numbers and manner of payment of the service and any other data that can lead to identifying the user;

- Security measures: use of procedures, tools or specialized software with access to a computer system which is restricted or prohibited for certain categories of users;

- Child pornography: any material that shows a minor with an explicit sexual behavior or an adult who is presented as a minor with an explicit sexual behavior or images which , although not representing a real person, simulated reliably, a sexually explicit conduct with a minor.

4.2. Offences against confidentiality and integrity of data and systems

Unauthorized access to a computer system is a crime punishable by imprisonment from 3 months to 3 years or a fine . Act in para . (1) committed in order to obtain computer data, shall be punished with imprisonment from 6 months to 5 years. If the act in para. (1) or (2) is committed by infringing security measures , the punishment is imprisonment from 3 to 12 years (art. 42).

Interception without right, of a data that is not public information and is intended for a computer system, such a system comes from or within a computer system performs an offense and shall be punished with imprisonment from 2 to 7 years . The same punishment is sanctioned interception without right of electromagnetic emissions from a computer system that contains data that is not public information (art. 43).

An act to amend, delete or damage data or restrict access to this data is considered a crime and punishable by imprisonment from 2 to 7 years. (2) unauthorized transfer of data from a computer system shall be punished with imprisonment from 3 to 12 years. (3) The penalty provided in par. (2) is sanctioned and unauthorized transfer of data from a data storage means (art. 44) .

The act of severely disrupt without right, of a computer system by inputting, transmitting , modifying, deleting or damaging data or by restricting access to data is a criminal offense punishable by imprisonment from 3 to 15 years (art. 45) .

An offense and shall be punished with imprisonment for 1-6 years:

a) The production, sale , import , distribute or make available in any other form , without right, of a device or software designed or adapted for the purpose of committing one of the offenses referred to in art . 42-45 ;

b) failure to produce , sell , import , distribute or make available in any other form without the right password, access code or other such computer data allowing full or partial access to a computer to commit an offense set forth in Art. 42-45 .

The same punishment is sanctioned possession, without right, of a device , software, password , access code or computer data provided in par. (1) the purpose of committing any of the offenses referred to in art . 42-45 (art. 46).

4.3. Cybercrime

The input, modify or delete, without right to restrict computer data without right, access to these data , resulting in inauthentic data in order to be used in order to produce legal consequences, constitutes a crime punishable with imprisonment from 2 to 7 years (art. 48).

The act of a person because of the loss of property by adding, changing or deleting computer data, by restricting access to such data or by impeding in any way the operation of a computer system in order to obtain a benefit for himself or another constitutes a crime punishable by imprisonment from 3 to 12 years (art. 49).

4.4. Child pornography through computer systems

An offense and shall be punished by imprisonment from 3 to 12 years and the prohibition of the production rights for distribution, offering or making available, distribution or transmission, procuring for himself or for another child pornography through computer systems or detention without law, child pornography in a computer system or data storage means (art. 51).

4.5. Forgery of electronic payment instruments

Forging an electronic payment instrument shall be punished with imprisonment from 3 to 12 years and the prohibition of certain rights. The same punishment is sanctioned release , in any manner, electronic payment instruments forged or stocking them for circulation . The punishment is imprisonment from 5 to 15 years and the prohibition of certain rights if the facts committed by a person who , by virtue of his duties :

a) carry out technical operations necessary to issue electronic payment instruments or perform the types of operations referred to in art. 1 section 11, or

b) has access to the security mechanisms involved in issuing or using electronic payment instruments , or

c) access to identification data or the security mechanisms involved in the types of operations referred to in art. 1 pt 11 .

4.6. Possession of equipment to forge electronic payment instruments

Manufacture or possession of equipment , including hardware and software, in order to serve the falsification of electronic payment instruments shall be punished with imprisonment from 6 months to 5 years.

4.7. For issuing false statements or use of electronic payment instruments

Inaccurate declaration, made by a bank, credit or financial institution or any other legal entity authorized by law to issue electronic payment instruments or accept types of operations referred to in art. 1 pt 11 the issuance or use of an electronic payment instrument, for himself or for another, when the law or the circumstances , the declaration serves to issue or use that instrument, is punished with imprisonment from 3 months to 2 years or a fine.

4.8 . Performing financial operations fraudulently

Perform one of the operations referred to in art. 1 pt 11 by use of an electronic payment instrument , including identification data that allow its use, without the consent instrument , shall be punished with imprisonment from 1 to 12 years. The same punishment is performing one of the operations referred to in art . 1 pt 11 the unauthorized use of any identification data or by using false identification data and the unauthorized use by any person of any identification data in order to perform one of the operations referred to in art. 1 pt 11.

Punishment is imprisonment from 3 to 15 years and interdiction of certain rights if the offenses were committed by a person who, by virtue of his duties :

a) carry out technical operations necessary to issue electronic payment instruments or perform the types of operations referred to in art. 1 section 11 , or

b) has access to the security mechanisms involved in issuing or using electronic payment instruments, or

c) access to identification data or the security mechanisms involved in the types of operations referred to in art. 1 pt 11.

4.9. Accepting transactions made fraudulently

Accepting any of the transactions referred to in art. 1 section 11, knowing that it is performed by using an electronic payment instrument forged or used without the consent of the proprietor, shall be punished with imprisonment for 1-12 years. The same punishment is knowing acceptance of any of the operations provided that it is performed through the unauthorized use of any identification data or by using false identification data. The attempt is punished for these crimes.

5. Procedural provisions

In urgent and duly justified cases, if data or clues about the preparation or commission of an offense committed through computer systems, the purpose of gathering evidence or identifying the perpetrators, may have immediate preservation of computer data or data on traffic information, to which there is danger of destruction or alteration.

During prosecution prosecutor preserve ordering by reasoned order , at the request of the criminal prosecution body or office , and during the trial , the court settlement. The measure has a duration not exceeding 90 days and may be extended once for a period not exceeding 30 days.

The prosecutor or the court decision shall be transmitted immediately by any service provider or any person in possession of the data, which is required to preserve them in confidence. If traffic data information in the possession of several service providers, service provider referred to in para. (4) has the obligation to make, without delay, to the criminal prosecution body or the court the information necessary to identify other service providers in order to know all the elements in the chain of communication used.

Pending the prosecution , the prosecutor is obliged to inform in writing the person to whom the criminal investigation and whose data were preserved. In the period prescribed prosecutor, based on the authorization motivated prosecutor designated by the general prosecutor of the court of appeal or, where appropriate, the General Prosecutor of the Supreme Court of Justice or the court orders on lifting objects containing computer data data data traffic or users , from the person or service provider that you have in order to make copies that can serve as evidence.

If objects containing computer data on traffic information are made freely available to back the judiciary, the prosecutor or the court has forced lifting. During trial, the prosecutor shall notify the forced lifting , taking action for completion by the criminal investigation body . Copies are made with technical means and procedures that will ensure integrity of the information contained therein. Whenever the discovery and collection of evidence is necessary to observe a computer system or data storage media , the statutory body responsible may order a search.

If the criminal prosecution body or the court considers that lifting objects containing data required would seriously affect the activity of persons holding these items may order copies, which may serve as evidence and shall be according to art. 55 para. (3). If , during the investigation of a computer system or data storage media , it appears that computer data sought are contained in another computer system or data storage medium and accessible support system or initial may be ordered at once to perform the search in order to investigate all systems or data storage media sought. The provisions of the Code of Criminal Procedure relating to searches at home are properly applied.

Access to a computer system and interception and recording of communications conducted through computer systems occurs when useful to find the truth, and to establish the facts and identify the perpetrators can not be made on other samples. The measures provided is done with the authorization motivated prosecutor designated by the general prosecutor of the court of appeal or, where appropriate, the General Prosecutor of the Supreme Court of Justice or the Attorney General of NAPO, the criminal procedure , with the support of specialized persons who are obliged to keep secret operation performed . Necessary authorization is given for a maximum of 30 days and be extended under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum authorized the measure may not exceed 4 months.

Pending the prosecution , the prosecutor is obliged to inform in writing to people who have ordered measures taken . The provisions of the Criminal Procedure Code relating to audio or video recordings shall apply accordingly. For offenses committed through computer systems to ensure the fulfillment of special confiscation referred to in art. 118 of the Criminal Code may take precautionary measures provided for in the Criminal Procedure Code.

In case of any dispute concerning the provision of information society services , triggered between the service provider and a recipient of the service, the burden shifts to the service provider if the recipient is a consumer.

6. A new approach to cybercrime investigation

6.1. Cybercrime prevention

To ensure the security of information systems and data protection authorities and public institutions with competence in the field , service providers, NGOs and other civil society joint activities and programs for the prevention of cybercrime. Public authorities and institutions with competence in the field, in cooperation with service providers, NGOs and other civil society promotes policies, practices, policies, procedures and minimum standards of security of information systems.

Public authorities and institutions with competence in the field , in cooperation with service providers , NGOs and other civil society organizes information campaigns on Cybercrime and the risks they are exposed to users of computer systems. Ministry of Justice , Ministry of Interior , Ministry of Communications and Information Technology, the Romanian Intelligence Service and the Foreign Intelligence Service established and continuously updated database on Cybercrime. National Criminology Institute under the Ministry of Justice performs regular studies to identify the causes and conditions that favor cybercrime.

Ministry of Justice, Ministry of Interior, Ministry of Communications and Information Technology, the Romanian Intelligence Service and the Foreign Intelligence Service conducted special programs for training and retraining of personnel involved in preventing and combating cybercrime. Owners or managers of information systems which is prohibited or restricted to certain categories of users to warn users about the legal conditions for access and use , as well as on the legal consequences of no right of access to these systems. Warning should be accessible to any user.

6.2. A new approach to cybercrime investigation

In electronic fraud investigations are by their nature complex and involves the use of sophisticated equipment and specialized personnel whose training is a long process. Also, computer fraud investigation has a number of features that distinguishes fundamentally from other types of investigations. It includes the following: the use of scientific methods and certain insurance, collection, validation, identification, analysis, interpretation, documentation and presentation of the digital evidence , from sources such as computer science, in order to facilitate the discovery of truth in criminal trials .

In terms of normative- legal and procedural background investigation has been completed and other elements designed to form a pertinent opinion, or nesăvârşirea on committing crimes. The nr.131/2006 Ordinance amending and supplementing Law no. 508/2004 regarding the organization

and operation of the Public Ministry of the Directorate for Investigating Organized Crime and Terrorism in Article 16 para. (1) states the purpose of gathering evidence or identifying the perpetrator , under the Code of criminal Procedure or special laws , the following measures:

a) surveillance of bank accounts and their related accounts;

b) surveillance , interception and recording of communications ;

c) access to computer systems.

However, by Law nr.161/2003, as amended and supplemented, was legalized in the investigative plan by article 56 ,, computer search . " By such procedure can be done checking the content of hard disks and data stored therein conservation . For an electronic fraud investigations on the experience gained so far , although small , requires covering mainly the following steps:

- Preparation of investigation , verification procedures , permits criminal procedure;
- Conduct a preliminary investigation , which involves inventory information technology used by suspicious entity with respect to information management and compliance record keeping and other accounting documents;
- An analysis of risk - after preliminary data collection and conversion and those obtained by external information sharing, detecting risks of standard software system, the completeness and accuracy of the data, including those transferred (orders and invoices are exchanged electronically).

Detection risk should be the process by which to determine whether or not their. The main risk profiles are located in the transfers of price , value added tax (carousel fraud, misapplication of zero export operations), excise tax, etc.

- Formulating a strategy approach, depending on the technology involved and the possible consequences for individuals and institutions involved ;
- The preservation and maintenance of the physical and digital;
- Photo recording and copying the physical environment of digital evidence using common legal practices and procedures;
- Identifying and documenting each sample in terms of credibility and tax consequences;
- Analysis of samples to determine the significance of the evidence and findings highlight on offense investigated ;
- Summarizing and presenting the conclusions of the evidence in a manner understandable to non-specialists. Summary should be based on documentation ;
- Restitution to the owners of the objects retained during investigation (when not needed evidences allegations), and if appropriate, measures will have a freezing or seizure of objects.

7. Special Liability of service providers

Liability of providers of information society services is subject to the general law relating to civil, criminal and administrative, to the extent that the special law provides otherwise, and may be employed in any field, including in the field of copyright, industrial property law, pornography, harm to human rights, etc. So in this matter, as a rule , apply the legal status of different categories of legal liability. As was natural , from common law liability regime there are some exceptions that are regulated by special law imposed by the specific nature of the activity providers.

Some hosting providers in the country and abroad who can afford to block access to content available on sites hosted by them on the grounds infringement of certain third parties. In the event of copyright infringement for example, they establish a specific procedure whereby alleged right holder may notify the company that provides the service , including requiring safeguard its affidavit about the fact that the material in question is not in indeed authorized by the rightful owner to use.

Realizing that such a procedure could not be determined by the service provider only by reason of any of its responsibilities regarding alleged abuse that content , we observe that including e-commerce law may be misinterpreted in this regard obliging hosting service providers in making measures violate the rights of their clients first, as owners of the materials available on the sites actually only able to intervene in such content to amend, etc.

Law 365/2002 , with subsequent amendments , established in Article 14 Liability content providers of information society services . Thus, if an information society service consisting in the storage of information provided by a recipient of the service , that service provider is not liable for the information stored at the request of a recipient if any of the following conditions is met:

a) the service provider is not aware that the illegal activity or information is stored and , as regards claims for damages , is not aware of facts or circumstances showing that the activity or information in question could violate the rights of a third party ;

b) having knowledge that the activity or information that is unlawful or facts or circumstances showing that the activity or information could violate the rights of a third party service provider acting quickly to remove or block access to it .

The provisions of paragraphs. (1) shall not apply if the recipient is acting under the authority or control of the service provider. Likewise, the provisions of this Article shall not affect the possibility of judicial or administrative authority to require the service provider to terminate or prevent data breaches and also can not affect the possibility of establishing government procedures to limit or disrupt access to the information.

The dispute could arise from the analysis of the conditions of b) of para. (1) , by a contrario interpretation, establishes the liability of the service provider where it „has actual knowledge that the activity or information that is unlawful "or" aware of facts or circumstances showing that the activity or information could violate the rights of a third party". It will be appreciated that a service provider can not be considered to have knowledge that a certain activity is illegal simply by information sent by a rightholder an alleged infringement of a third party is necessary to have in this regard final and irrevocable decision to establish the unfairness of a certain illegal activities of a particular material or information .

Even in the absence of paragraph text. (2), repealed by Act nr.121/2006 ("service provider has actual knowledge that the activity or information is illegal when its illegal character has been found by a decision of a public authority") can not be argued that a service provider may assign a judge to qualify the quality of being legal or illegal as an activity.

Notification to the alleged owner of the right can not be considered only as a provider notify an alleged infringement of a third party in any way an awareness of the illegality of certain conduct . An activity can be considered illegal in the absence of a final and irrevocable decision to establish this, that to qualify as such , the document represented by this device actually constitutes the only evidence that can be really sent the service provider in order to bring inform his qualification as an illicit activities. Only this time , the supplier has received the judgment can talk about responsibility, because only in this moment hosting provider is aware that the work is indeed "illegal", as it supports Article 14. (1) b), may then act in accordance with legal requirements (blocking public access to insider information, for example) . A wrong interpretation of these provisions could lead to many abuses in the information society, material belonging to certain individuals may be removed or modified by hosting providers on the grounds there is a simple notification issued by an alleged rights holder claiming infringement of its rights by informational material concerned.

Definitely, more problems arise when introduced by Article 14 b) of Law 365/2002, provisions appear to establish liability beyond the limits imposed by Directive no. 2000/31/EC. In this case one speaks of this time where the service provider is liable if "aware of facts or circumstances showing that the activity or information could violate the rights of a third party".

Presumption of illegality of a particular content can not be brought into the state of certainty than the conditions under which it is proven by a document issued by a court, but what happens when the by a law provides that the hosting provider to act quickly to remove or block access to content where it is informed of certain facts and circumstances showing that the content could violate the rights of a third party ? Of course, a simple notification of an alleged rights holder can prove in this respect , because of the time not talking about something certain, labeled as illegal by a court , but content that could violate the rights a third party. In other words, it establishes an obligation on service providers by the measures taken by them may seriously prejudice the interests of other holders of rights based on mere assumptions.

Article 11 para. (2) of Law no. 365/2002 provides that "service providers liable for information provided by them or on their behalf, "the text of the law intends to regulate the special responsibility of service providers in relation to the fact that part of the liability. Thus, if the service provider liability "offense" has a specific form that consists of an "information provided by them or on their behalf."

However legal wording should not be interpreted as meaning that providers are only liable for the information provided by them or on their behalf , for in this case would ineffectiveness legal provisions of par. (1) thereof which establishes the general applicability of general legal provisions on civil, criminal and contravention in this matter. This will engage the liability of the service provider only "information provided by them or about them", and for any act likely to attract one of the forms of legal liability (civil, criminal or administrative).

In other news, art. 11 para. (2) of Law no. 365/2002 should be read in conjunction with para. (3) thereof which contains a provision referring to cases of liability exemption. As we will see below, the criterion used by the legislature to tie special responsibility of the service provider in relation to other subjects of law is the very mode of transmission/storage/retrieval.

7.2. Duties of provider

Under the supervision and control providers have a number of legal obligations.

7.2.1. Duty to inform

Service providers are required to immediately inform the competent public authorities apparently illegal activities conducted by recipients of their service or the information provided by them apparently illegal and notify those authorities, upon request, information enabling the identification of recipients of their services with these suppliers have contracts on permanent storage of information.

7.2.2. Duty of service disruption

Service providers are required to discontinue temporarily or permanently, the transmission in a communication network or the storage of information provided by a recipient of the service , in particular by removing or disabling access to this information , access to a communication network or the provision of any other information society service if these measures were taken by the public authority as defined in Article authority. 17 para. (2) of Law no. 365/2002, the public authority may act on its own initiative or following a complaint or referral to an interested person .

The complaint may be filed by any aggrieved person who considers the content of the information. Claim or complaint shall be in writing, providing reasons on which it is based , and will necessarily be dated and signed . The complaint may be submitted if a trial on the same subject and the same parties , was previously introduced .

Decision shall be reasoned and notified to the interested parties within 30 days of receipt of the complaint or referral or, if acted on its own authority, within 15 days from the date of issue. Against a decision, the person concerned may appeal within 15 days from notification, under penalty of forfeiture, the competent administrative court. Application is judged emergency, summoning the parties. The sentence is final.

8. Mediation by simply sending

If an information society service consists of the transmission in a communication network of information provided by a recipient of the service or access to a communication network, that service provider is not liable for the information transmitted if the following conditions are met:

a) transmission was not initiated by the service provider;

b) the choice of the person receiving the information provider did not belong ;

c) the information sent was not influenced in any way by the service provider, in that it can be assigned to any selection and any possible changes to that information.

Transmission of information and access , include the automatic, intermediate and temporary information transmitted , provided that this operation takes place solely in order to pass through the

information communication network, and provided that the information is not stored for a period unreasonably exceeds the time required for its transmission.

The provisions of art. 12 of Romanian Law reproduce almost identical provisions of art. 12 paragraph (1) and (2) of Directive 2000/31/EC relating to the exemption from liability of service providers acting as intermediaries by simple transmission. In this case the disclaimer, the service provider must have a purely passive role, being only one channel for transmitting information to third parties, in which case he will not be held directly responsible , subsidiary or jointly.

Provided that "the service provider has not started transmitting" is satisfied if the provider has made the decision to transfer. If the supplier only runs automatically initiate a service receiver polled its condition is satisfied.

Provided that "the choice of the person receiving the information provider may not belong" is satisfied if the provider selects receptors as an automatic response to the request of the person who initiated the transmission. Storage activities covered in this article do not include copies made by the service provider in order to make the information of users of subsequent provisions , which are regulated by art. 13 of Law no. 365/2002 .

The term "automatic storage" refers to storage activities that occur in the normal operation of the technology and the "intermediate storage" refers to the fact that the storage of information takes place during transmission .

8.2. Temporary data storage (caching)

If an information society service consists of the transmission in a communication network of information provided by a recipient of the service, that service provider is not liable for the automatic, intermediate and temporary information transmitted, provided that this operation takes place exclusively in order to make more efficient transmission of information to other recipients, at their request, if the following conditions are met :

a) the service provider does not modify the information ;

b) the service provider meets the legal requirements for access to information;

c) the provider complies with rules or practices for updating information as they are widely recognized and applied in industry;

d) the service provider does not preclude the use by any person of legal technology, widely recognized and used by industry, to obtain data on the nature and use of information;

e) the service provider acts quickly to eliminate information that it has stored or to block access to it, since the owner knew that the information originally submitted was removed from the communications network or that access to it been blocked or that the removal or disabling of access has been the effect of the decision of a public authority.

These provisions replicate almost identical provisions of art. 13 para. (1) of Directive 2000/31/EC. The service provider provides this type of storage in order to improve the performance and speed of the network.

Copies of the information available online or transmitted to third parties are temporarily stored in the system or network operator in order to facilitate access to such information to a third party subsequently . These children are from a process automatically and are "intermediate" between the place in the network where the information was made available to first time user.

8.3. Permanent information storage (storage -hosting)

If an information society service consisting in the storage of information provided by a recipient of the service, that service provider is not liable for the information stored at the request of a recipient if any of the following conditions is met:

a) the service provider is not aware that the illegal activity or information is stored and , as regards claims for damages , is not aware of facts or circumstances showing that the activity or information in question could violate the rights of a third party ;

b) Having knowledge that the activity or information that is unlawful or facts or circumstances showing that the activity or information could violate the rights of a third party service provider acting quickly to remove or block access to it.

The above provisions shall not apply if the recipient is acting under the authority or control of the service provider. These provisions shall not affect the possibility of judicial or administrative authority to require the service provider to terminate or prevent data breaches and also can not affect the possibility of establishing government procedures to limit or disrupt access to the information. As can be seen to operate this disclaimer concerned, utmost importance is given factor "knowledge" of the information, and of the ' illegal' of information.

8.4. Criterion „acknowledgment”

Law no. 365/2002 does not define the notion of "being informed " and does not determine how the provider should be aware, which means that it can take the knowledge of illegal activity or information, i.e. facts and circumstances from which that the activity or information could violate the rights of a third party by any means, including by notice addressed to the person concerned.

The case of exemption referred to in art. 14 of Directive 2000/31/EC of the product op series of controversies regarding the practical implementation into national law of the Member States of the European Union and how to interpret the concept of "being informed.”

Thus, some Member States require a formal and official notification from the authorities in order to consider that the supplier is aware, while in other states the courts have full authority to determine how to „be aware„. A third approach offers two possibilities to determine the meaning of aware: a notification and termination of service delivery and the more traditional approach of providing notification under national law.

The question is whether the service provider is required to know the content they transmit information. The answer to this question is irrelevant in terms of establishing the burden of proof in a possible litigation.

According to art. 15, para. (1) of Directive 2000/31/EC , Member States shall not require providers offering services listed in art . 12, 13, 14 general obligation to monitor the information they transmit or store, nor a general obligation actively to pursue facts and circumstances indicating illegal activity. A similar provision is found in Romanian legislation. Specifically, art. 11, para. (1) Methodological Norms for applying Law no. 365/2002 on electronic commerce, approved by Government No. 1308/2002, states: „information society service providers that provide services under art. 12-15 of Law no obligation to monitor the information they transmit or store, nor obligation to actively seek data or information apparently illegal activities in the field of information society services they provide. „Therefore, under Romanian law and European law, a service provider can not be presumed to have been aware of the content posted by others.

Judicial practice, especially the European one, however, is more nuanced.

8.5. Notification procedure to the injured person

Closely related to the notion of "having knowledge" and its relevance in material liability of the service provider, there are art. 11 para. (3) Methodological Norms for applying Law no. 365/2002.

Service providers are required to implement a free procedure that is to be sent complaints and complaints from anyone about the apparently illegal activities conducted by recipients of their service or the information provided by them apparently illegal. The procedure should:

a) be available electronically;

b) to ensure receipt of complaints or complaints within 48 hours from the time of dispatch.

The supplier has the obligation to publish on its website the procedure. Such notice creates a presumption that the service „has learned „about the illegal nature of the activity or information and their harmful nature. Therefore, in a possible dispute, the service provider will not rely on ignorance, while he was notified.

But even when it is notified that procedure, the question will be conduct the service provider, in other words, may interrupt transmission of this service provider that receives a notification from an injured person? Distinctions are necessary. It should be noted that the service provider has no legal obligation explicitly specify that effect, which causes him to decide whether to stop or not those services and then decide to stop service provider following the notification of the injured person only if such the possibility is provided for in the contract of service entered into with its customers. Otherwise, you might contractual liability of the service provider.

9. Conclusions

In conclusion, the hosting provider is exempted from liability when no knowledge that is unlawful activity or information or facts or circumstances showing that the activity or information could violate the rights of a third party or you, although it has the knowledge, acts quickly to remove or block access to it. In assessing the „lawful" following situations can be distinguished:

a) There is a judgment or decision of a public authority stating unlawful nature of the activity / information stored;

b) Legal provisions are mandatory, especially criminal, which are violated by the activities/information stored (such as, for example, criminal law prohibiting child pornography), in such a situation unlawfulness not have "found" by a judgment or decision of a public authority;

c) There is a notice from a third party which provider acknowledges that the activity/information stored has an unlawful purpose, in situations other than those shown in the letter. a) and b) (e.g., third party claims a copyright message posted on its own), in such a case , proceed from case to case, a corollary to the service provider as the character "manifestly" unlawful activity / information stored.

Indeed often illicit nature of information posted on a website is not so obvious, and sometimes it is impossible to fully and timely check the legality of any information stored. In this situation, it would be excessive to claim the service provider to verify the legality of all the information prior to posting, and therefore illicit criterion „obviously" used by Directive 2000/31/EC is rational.

Bibliography

1. Dan Cimpoeru, *Dreptul internetului*, Editura CHBeck, Bucureşti, 2012;

2. Nicolae Plăiaşu, *Frauda şi comerţul electronic*, în Volumul Sesiunii de comunicări ştiinţifice cu participare internaţională, Editura Universităţii Naţionale de Apărare, Bucureşti, 9-10 aprilie, 2009;

3. Gheorghe Stancu, *Unele consideraţii privind comerţul electronic*, Revista de Drept Comercial nr. 7-8/2003;

4. M. Giuraniuc (Tudorache), *Răspunderea furnizorilor de servicii ale societăţii informatice în Romania*, Juridical Tribune, Volume 1, Issue 2, Academia de Studii Economice, Bucureşti, December 2011;

5. Valentin – Stelian Bădescu, *Dreptul afacerilor*, Editura Universul Juridic, Bucureşti, 2012.