Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime

Ph. D. ***ANDREEA VERTEŞ-OLTEANU****,*
The West University of Timisoara, Law Faculty

Abstract:

The dynamism of cyberspace brings along, incessantly, new challenges for many professions, especially for legal practitioners. "The law cannot follow in real time the technological progress". It is essential, that it always keeps up and not stay too far behind.

For a long time, cybercrimes have not found themselves incriminated in express legal provisions, except for Law no. 8/1996 on copyright and related rights, which criminalizes software privacy, covering only a small part of this hazardous phenomenon, and Law no. 16/1995 on the protection of topographies of semiconductor products. Law no. 21/1999 on preventing and sanctioning money laundering has introduced for the first time in the Romanian legislation the concept of "offenses committed via computers".

Until the entry into force of the new Penal Code, the main regulatory act regarding cybercrimes was represented by Law no. 161/2003, with its subsequent amendments and completions, which dedicates its Title III to issues related to cybercrime. In Chapter 3 of this Title, the offenses are structured and categorized into 3 sections: Section I, Offences against the confidentiality and integrity of computer data and systems, including: illegal access to a computer system, illegal interception of computer data transmission, alteration of the integrity of computer data, hindering the functioning of information systems, illegal operations with computer devices or software; Section II, Computer crimes: computer forgery and computer fraud; Section III, Child pornography through computer systems.

In order to create the necessary legal framework for the prevention and control of cybercrime, as well as with a view to the ratification of the European Convention relating to this field, the Romanian legislator thought it was absolutely necessary to draft Title III, on the prevention and combat of cybercrime.

Keywords: *cybercrime; information technology; telecommunications technology; computer system; computer data; service provider; European Convention on Cybercrime.*

Nowadays, to try and present the Internet is almost useless since it has already become deeply enrooted in our daily lives and habits. This international communications network has given rise to new possibilities and forms of expression and creation, education and training, cultural and information exchanges, trade, and, last but not least, entertainment, fun, games and relaxation. Internet brings added value in the lives of all of us. Undoubtedly, the Internet has upon our social lives consequences as important as the appearance of the telephone or the industrial revolution of the nineteenth century, radically transforming human behaviour. This mutation in society is so deep that the term that future historians will use to describe this period will be, most likely,

* E-mail: andreea.vertes@yahoo.com.

"revolution": the Internet revolution. And this revolution is far from being over. The Internet wins every day new areas, ever more numerous, of everyday life. The Internet is not a mere fleeting "fashion" and, although we can not know for sure whether it will remain forever part of our lives, we can be certain that it will represent the starting point of telecommunications systems henceforth.

The Internet is often referred to as the new "Wild West" since it brings with it real dangers. A web surfer is exposed to dangers which are new, difficult to police, and difficult to prevent. The only significant difference may be that the Internet is a virtual society rather than a tactile one; a virtual society existing only in networks and information packets. However, the harms committed against both individual citizens and businesses are very real. These citizens are extremely vulnerable as criminal activity on the Internet continues to run rampant.[1]

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. 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. The ease of accessibility and searchability 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.[2]

In addition to these benefits, Internet expansion has fostered new kinds of crimes, additional means to commit existing crimes and increased complexities of prosecuting crimes. It seems that today, computer crimes affect everyone. A common example is credit card theft whereby a perpetrator illegally obtains the victim's personal information by "hacking" into a website where the victim maintains an account or makes purchases. The perpetrator may steal or charge thousands of dollars to the victim's credit card before he is apprehended, if ever. The problem persists because a perpetrator can easily remain anonymous by instantaneously manipulating or deleting data.[3]

Internet investigations are inherently difficult to conduct because a maze of interconnected computer networks can transmit information instantaneously. Criminals can delete or alter data as quickly as they create it. The ability to destroy or alter data quickly makes it difficult to obtain evidence and perform investigative procedures.

The first international initiative on computer crime in Europe was the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976. Several categories of computer crime were introduced.[4]

---

[1] Keyser, M., "The Council of Europe Convention on Cybercrime", in *Journal of Transnational Law and Policy*, 12, 2003, p. 287.

[2] Council of Europe, Committee of Experts on Crime in Cyber-Space, Explanatory Memorandum to the Convention on Cybercrime, EST No. 185 1 (May 25, 2001), available at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (26.05.2014).

[3] Hopkins, S.L., Cybercrime Convention: A Positive Beginning to a Long Road Ahead, in *Journal of High Technology Law*, 2, 2003, pp. 101-121.

[4] A Paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, pp. 225-229.

Then, in 1985, the Council of Europe appointed another expert committee in order to discuss the legal issues of computer-related crime. A summary of the guidelines for national legislatures with liability for intentional acts only, was presented in the Recommendation of 1989.[5] It included a minimum list of computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer program and unauthorized reproduction of a topography.

The Council of Europe adopted this Recommendation on September 13, 1989. It contains a minimum list of offences necessary for a uniform criminal policy on legislation concerning computer-related crime, and an optional list.

In this respect, the Council of Europe has initiated a series of regulations regarding cybercrime. Thus, in 1995, was adopted Recommendation no. R (95) 13 concerning problems of criminal procedural law connected with Information Technology. This Recommendation introduces 18 principles categorized in 7 chapters: search and seizure; technical surveillance; obligation to co-operate with the investigating authorities; electronic evidence; use of encryption; research; statistics and training; international co-operation.[6]

On November 23rd 2001, the member states of the Council of Europe (with the help of Canada, U.S.A., Japan and South Africa, as observers) have drafted and signed the "Convention on cybercrime".[7] Subsequently, on January 28th 2003, was submitted for signature by the member states the "Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of racial and xenophobic nature committed through computer systems".[8] Romania has signed this Additional Protocol on October 9th 2003.

The Convention and the Additional Protocol establish the basic framework for the investigation and sanctioning of criminal offenses committed with the help of the computer, as well as for the interstate cooperation required to stop this phenomenon.

The Convention brings to the fore the need for criminalization of criminal acts such as: illegal access to computer systems, illegal interception of computer transmissions, computer forgery, computer fraud, child pornography on the Internet, violations of property rights and other related rights etc.

The Convention was ratified by Romania through Law no. 64/2004 for the ratification of the Council of Europe's Convention on Cybercrime.

---

[5] Recommendation no. R. (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime, adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies

[6] Recommendation no. R (95) 13 of the Committee of Ministers to Member States concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies.

[7] Council of Europe, *Convention on Cybercrime*, Budapest, November 23rd 2001.

[8] Published in the Official Journal of Romania, Part I, no. 279 from 21.04.2003.

The Convention on Cybercrime of the Council of Europe[9] is the most elaborate regulation of the existing international instruments addressing cybercrime because it includes provisions on substantive criminal law, criminal procedure and international cooperation. This historic milestone in the combat against cybercrime entered into force on July 1st, 2004. The number of signatures not followed by ratifications are 23 States and the number of ratifications/accessions are 23 States (December 2008). An Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems of January 2003 has also been adopted.

In the field of substantive criminal law (Chapter II Section I), Articles 4 and 5 deal with "the damaging, deletion, deterioration, alteration or suppression of computer data without right" and "the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data". They cover all types of interference in data and computer systems which – as shown – are a prerequisite for terrorist attacks on the electronic systems made via the Internet. As Article 4 is not limited to the deletion of data, but also includes the alteration and suppression of data (and is extended to the hindering of a computer system in Article 5), such interference is not limited to IT attacks on information systems, but occur also in the context of the IT attacks mentioned hereabove on other infrastructures, physical property or the lives and well-being of the people.[10] This consequence of the concept underlying the Convention on cybercrime concerning the comprehensive protection of the integrity and availability of the information systems is confirmed in the Explanatory Report of the Convention, which explains the fact that Article 5 is formulated "in a neutral way so that all kinds of functions can be protected by it".[11] Consequently, all the types of terrorist attacks on computer systems are covered by Articles 4 and 5.

In addition, Articles 2 and 3 of the Convention on Cybercrime incriminate "the access to the whole or any part of a computer system without right", as well as "the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data" and, thus, cover the hacking intrusion techniques of the information systems and those of interception of computer data (*e.g.* through technical manipulations or the misuse of the intercepted information), which, in many cases, must be used to defeat the existing security measures in the victim's computer system so that the intruder might intervene and alter the data.

These provisions are expanded in terms of scope by means of rules regarding attempt and aiding or abetting (Article 11) and corporate liability (Article 12), and are

[9] Council of Europe's Convention on Cybercrime from November 23rd 2001 (ETS nr. 185).

[10] Council of Europe's Convention on Cybercrime from November 23rd 2001 (ETS nr. 185), Explanatory Report no. 65 of interpretation of Article 5 specifies that "the protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly".

[11] Council of Europe's Convention on Cybercrime from November 23rd 2001 (ETS nr. 185), Explanatory Report no. 65 of interpretation of Article 5. See also no. 60 and 61 describing the concept of Article 4.

supported by regulations which impose effective, proportionate and dissuasive sanctions, including imprisonment (Article 13). Furthermore, Article 6 on the "misuse of devices" wants the establishment as criminal offences of the actions preparing the intrusion, such as the illegal production, sale, procurement for use, import, distribution or otherwise making available of "a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5", with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. Article 6 also has in view the possession of such item with the intent that it be used for the purpose of committing any of the offences established in the articles mentioned above.[12] Thus, with respect to the terrorist attacks via the Internet, Articles 2, 3 and 6 provide an additional protection, allowing the indictment of the authors from an early stage.

As a result, the requirements for implementing the Convention on Cybercrime in the field of substantive criminal law provide a broad spectrum of incrimination of IT terrorist attacks on computers and on all other legal rights pertaining to the operation of computer systems. As noted above, the physical injury to property or life and well-being leads to the application of further offenses, in addition to the "traditional" ones from the national criminal law. Thus, the Convention on Cybercrime manages to criminalize the attacks on information systems through an "approach regarding data" which do not need, consider or evaluate the physical damage or (political) intent of the author.

The Convention on Cybercrime calls for the criminalization of nine offenses in four categories. The first category targets "offenses against the confidentiality, integrity and availability of computer data and systems". These include: illegal access, illegal interception, data interference, system interference, and misuse of devices. The second category, "computer-related offenses", includes provisions calling for the criminalization of computer-related forgery and computer-related fraud. "Content-related offenses" requires criminalizing offenses related to child pornography. This third category is ostensibly supplemented by a new protocol adopted November 7th 2002, making any dissemination of racist or xenophobic material through computer systems a criminal offense. However, the new protocol is a separate legal instrument from the treaty, and parties agreeing to the treaty are not obliged to adopt it. The fourth category, "offenses related to the infringements of copyright and related rights", criminalizes copyright violations. This section of the Convention also includes ancillary provisions that require the establishment of laws against attempt and aiding or abetting in the aforementioned crimes, as well as the establishment of a standard for corporate liability.[13]

Article 1 initially defines four terms vital to the treaty. These terms are vital because they are heavily relied upon throughout the treaty. The treaty first defines "Computer system" as a device consisting of hardware and software developed for automatic processing of digital data. For purposes of this Convention, the second term, "computer data," holds a meaning different than that of normal computer lingo. The data must be "in such a form that it can be directly processed by the computer system." In

[12] Furthermore, there is a provision against computer-related forgery (Article 7), which can be applied in case of preparatory electronic forgeries which might also facilitate the interference.

[13] Weber, A.M. "The Council of Europe's Convention on Cybercrime", in *Berkely Techology Law Journal*, Vol. 18, issue 1, 2003, p.431.

other words, the data must be electronic or in some other directly processable form. The third term, "service provider" includes a broad category of entities that play particular roles "with regard to communication or processing of data on computer systems." This definition not only includes public or private entities, but it also extends to include "those entities that store or otherwise process data on behalf of" public or private entities.

The fourth defined term is "traffic data," which has created some controversy in this Convention. "Traffic data" is generated by computers in a "chain of communication in order to route" that communication from an origin to its destination.

Thus, it is auxiliary to the actual communication. When a Convention party investigates a criminal offense within this treaty, "traffic data" is used to trace the source of the communication. "Traffic data" lasts for only a short period of time and the Convention makes Internet Service Providers ("ISPs") responsible for preservation of this data. The increased costs placed upon ISPs as a result of the Convention's stricter rules regarding preservation of "traffic data" is one issue of concern for many ISPs. Another concern is the requirement of rapid disclosure of "traffic data" by ISPs. While rapid disclosure may be necessary to discern the communication's route, in order to collect further evidence or identify the suspect, some civil libertarians express concern over its infringement upon individual rights - namely the right to privacy.[14]

The drafters intended that "Convention parties would not be obliged to copy [the definitions] verbatim into their domestic laws…." It is only required that the respective domestic laws contain concepts that are "consistent with the principles of the Convention and offer an equivalent framework for its implementation."

After defining the vital terms, Article 1 lays out the Convention's substantive criminal laws. The purpose of these criminal laws is to establish a common minimum standard of offenses for all countries. Uniformity in domestic laws prevents abuses from being shifted to a Convention party with a lower standard. The list of offenses is based upon the work of public and private international organizations, such as the United Nations and the Organization for Economic Cooperation and Development. "All of the offenses contained in the Convention must be committed 'intentionally' for criminal liability to apply." In certain cases, additional specific intentional elements form part of the offense. The drafters have agreed that the exact meaning of "intentional" will be left to the Convention parties to interpret individually. A *mens rea* requirement is important to filter the number of offenders and to distinguish between serious and minor misconduct.

The criminal offenses in Articles 2 thru 6 were intended by the drafters "to protect the confidentiality, integrity and availability of computer systems or data."

At the same time, however, the drafters did not criminalize "legitimate and common activities inherent in the design of networks, or legitimate . . . practices."

---

[14] Keyser, M., "The Council of Europe Convention on Cybercrime", in *Journal of Transnational Law and Policy*, 12, 2003, p. 298.

There is no doubt that cyber crimes are potentially damaging offenses, with potentially serious ramifications. Since computer-related crimes affect practically all nations,[15] there is no question of a need for updated, harmonized laws that involve international cooperation to fight crime in cyberspace.[16] The international community cannot choose to ignore cyber crimes, as that would only encourage the attackers' greed and more serious criminal behaviors will result.[17] The Convention is an important step in the right direction and is the most significant treaty to address computer crimes. Although an international perspective in fighting cyber crimes is vital, it is, at the same time, difficult.[18]

The Convention convened representatives from many nations, both from their members and outside nations, to discuss and debate the definition of certain acts committed on the internet and then define what the most appropriate actions would be to institute a fair, yet effective, fight against cyber crimes. They recognized the need for a consistent international approach to fighting cyber crimes that included cooperation between law enforcement agencies to investigate offenses.

However, because the Convention is largely symbolic, its long-term effectiveness must be brought into question. There are problems relating to the definitions of terms in the treaty, privacy issues, and the investigatory powers created in the document. Further, international laws requiring cooperation between nations are difficult to enforce. Overall, the treaty leaves too many holes in terms of the lack of definitions and inconsistencies, and has many gaps that will allow criminals to continue to commit criminal offenses. There are many ways for criminals to continue to exist and operate even after the treaty is in force.

In order for the treaty to be effective, more countries will need to sign it and ratify it and turn it into national law. Until then, cyber crimes will not be impacted by the treaty in any significant way.

The Council of the European Union also had concerns in this direction. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[19] is based on the Convention on Cybercrime of the Council of Europe, and, just like the Convention, requires that the Member States ensure that the illegal access to information systems (Article 2), the illegal interference in the systems (Article 3) and the illegal interference on the data (Article 4) shall be punished as criminal offenses. In addition, it includes requirements regarding the criminalization of incitement, complicity and attempt. The European Commission is far from remaining indifferent to the phenomenon of computer crimes. Following a feasibility study

---

[15] Backhouse, J., & Dhillon G. "Manager Computer Crime: A Research Outlook" in *Computers and Security*, 14, 1995, pp. 645-651.

[16] Walden, I. "Harmonising Computer Crime Laws in Europe" in *European Journal of Crime, Criminal Law and Criminal Justice*, 12(4), 2004, pp. 321-336.

[17] Wang, S. "Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crimes", in *Computer Standards and Interfaces*, 29, 2007, pp. 216-223.

[18] Marion, N.E., "The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation", in International Journal of Cyber Criminology, Vol. 4, Issue 1&2, 2010, pp. 699-712.

[19] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (OJ L 69/67 from 16.03.2005).

conducted by Rand Corporation Europe, the European Commission decided to establish a European Cybercrime Centre (EC3) at Europol in order to help protect the European citizens and businesses against IT threats. The Centre will be the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. It will support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners.

The centre is established within the European Police Office, Europol, in The Hague (Netherlands) and started its activity January 11th 2013, with a mandate to tackle the following areas of cybercrime: that committed by organised groups to generate large criminal profits such as online fraud, that which causes serious harm to the victim such as online child sexual exploitation, that which affects critical infrastructure and information systems in the European Union.

One of the objectives of the European Cybercrime Centre will be protecting the profiles on social networks against infiltrations by online criminals, thus supporting the fight against online identity theft. Moreover, the centre will also focus on those offenses causing serious injury to the victims, such as online sexual exploitation of children and attacks affecting the critical infrastructure and information systems in the European Union.

EU experts will also carry out activities aimed at preventing cybercrime affecting Internet banking and online reservation systems, thus increasing the level of consumer confidence online.

The European Centre will warn the EU Member States on major information threats and will draw attention to the biggest weaknesses in their defence systems online. The centre will identify the organized networks of cybercrime, as well as the leading offenders in cyberspace. It will provide operational support in concrete investigations, either providing legal assistance specialized in IT, or supporting the establishment of joint investigative teams in the field of cybercrime. The new centre will also serve as an information database for the national police services from the Member States and will bring together the European expertise and training initiatives in the field of cybercrime.

Given this international context, Romania could not have remained indifferent to computer crimes and its propagation speed.

A first reaction of the Romanian legislator, prior to the Convention from Budapest in 2001, was in the field of copyright law, by the incrimination through the provisions of Law no. 8/1996, of the offense of bringing, without right, to a work (intellectual creation protected by copyright) to the attention of the public[20] and the offense of reproduction, without right, of a work.[21]

There followed legal provisions with regard to cybercrime, which were introduced in the first regulations concerning money laundering. Thus, it was introduced for the

[20] Regulated by Article 140, letter (a) of Law no. 8/1996 on copyright and related rights.
[21] Regulated by Article 142, letter (a) of Law no. 8/1996 on copyright and related rights.

first time in the Romanian legislation the concept of "offenses committed via computers".[22]

Other legal provisions with applicability in the field of computer crimes were introduced by Law no. 365/2002 on electronic commerce.[23]

In applying the Budapest Convention (2001), were introduced in Law no. 161/2003 more specific regulations regarding cybercrime.

The latest regulations have been made on the drafting of the new Penal Code, which introduced more specific provisions.

The dynamism of cyberspace brings along, incessantly, new challenges for many professions, especially for legal practitioners. "The law cannot follow in real time the technological progress". It is essential, that it always keeps up and not stay too far behind.

For a long time, cybercrimes have not found themselves incriminated in express legal provisions, except for Law no. 8/1996 on copyright and related rights, which criminalizes software privacy, covering only a small part of this hazardous phenomenon, and Law no. 16/1995 on the protection of topographies of semiconductor products. Law no. 21/1999 on preventing and sanctioning money laundering has introduced for the first time in the Romanian legislation the concept of "offenses committed via computers".

Until the entry into force of the new Penal Code, the main regulatory act regarding cybercrimes was represented by Law no. 161/2003, with its subsequent amendments and completions, which dedicates its Title III to issues related to cybercrime. In Chapter 3 of this Title, the offenses are structured and categorized into 3 sections: Section I, Offences against the confidentiality and integrity of computer data and systems, including: illegal access to a computer system, illegal interception of computer data transmission, alteration of the integrity of computer data, hindering the functioning of information systems, illegal operations with computer devices or software; Section II, Computer crimes: computer forgery and computer fraud; Section III, Child pornography through computer systems.

As specified in the Explanatory motives of the law, in order to create the necessary legal framework for the prevention and control of cybercrime, as well as with a view to the ratification of the European Convention relating to this field, the Romanian legislator thought it was absolutely necessary to draft Title III, on the prevention and combat of cybercrime.

---

[22] According to the text of Article 23 of Law no. 21/1999, money laundering is represented by "changing or transferring goods, knowing that they come form committing of offenses, (…), offenses committed with the help of computers, (...) in the purpose of hiding or the dissimulation of the illicit origin of these or in the purpose to help the person that committed the contravention form which the goods came, withdraw himself from the pursuit, trial or execution of the punishment".

[23] The offenses provided by Articles 24-28 of Law no.365/2002 – forgery and placing in circulation of electronic payment instruments; possession of hardware or software for the purpose of forgery of electronic payment instruments; fraudulent financial operations etc.

The proposed Title, harmonized with the European Convention on Cybercrime, is structured in five chapters, which include general provisions, provisions on the prevention of cybercrime offenses, offenses and misdemeanours, procedural provisions and provisions regarding international cooperation.

The general provisions are devoted, mainly, to the establishment of the meaning of the terms and expressions used in Title III, which present a technical character, specific to the field of computer science. Thus, the legislator establishes the notions of "computer system", "automatic data processing", "computer software", "computer data", "service provider", "data referring to the information traffic", "data regarding users", "security measures".

In Chapter II are listed the rules regarding the prevention of cybercrime. These provisions relate to the cooperation between authorities and public institutions with competences in the area and service providers, NGOs and other representatives of the civil society in the development of policies, practices, procedures and standards for computer security, as well as to the organisation of the information campaigns regarding cybercrime and the risks to which are exposed the users of computer systems. Also, the provisions on cybercrime prevention provide the obligation of the Ministry Justice, Ministry of Interior and Ministry of Communications and Technology Information to create and update databases on cybercrime.

Chapter III has as main regulatory object the regulation of the offenses committed in the computer environment, grouped according to the same criteria as the ones set out in the European Convention on Cybercrime. Thus, the Romanian legislator provides offenses against confidentiality and integrity of computer data and systems, such as illegal access to an information system; illegal interception of the transmission of data information which are not public; modification, deletion or deterioration of the data information or restriction of access to such data, without right. This law also provides, as computer crimes, the acts of forgery committed in relation to data information and the facts which cause patrimonial damage as a result of operations upon computer data or systems, committed with the purpose of obtaining material benefits.

Moreover, the law provides severe punishment – such as the imprisonment for 3 to 12 years and the prohibition of certain rights – for child pornography through computer systems, also criminalizing the mere possession of materials containing child pornography in a computer or data storage system. In this way, the regulation responds not only to the provisions of the European Convention on Cybercrime, but also to the Recommendation of the Committee of Ministers of the Council of Europe, Rec(2001)16 on the protection of children against sexual exploitation.

The procedural provisions, enshrined in Chapter IV, regulate the measures and means of investigation specific to the computer field, while also achieving an adaptation of certain provisions from the Criminal Procedure Code to the specificity of this area. The legislator chooses to regulate, in principle, the immediate preservation of computer data or data referring to the information traffic, the procedure of forfeiture of those items which contain information data, the scrutiny of computer systems or data storage systems.

Chapter V contains provisions referring to international cooperation concerning international legal assistance in criminal matters, such as extradition, identification, freezing, seizure and confiscation of the results and instruments of the crime, the conduct of joint investigations, information sharing, technical or any other type of assistance for the gathering and analysis of the information, as well as for the training of specialised personnel.

Also, in order to ensure the immediate and permanent international cooperation Sin the field of combating cybercrime, the law provides the establishment, within the Prosecutor's Office attached to the Supreme Court of Justice, the Service for the combating of cybercrime, as point of contact available 24-7, and which does not involve additional costs from the state budget.

Another special law containing provisions regarding the electronic environment is Law no. 365/2002, republished in 2006, on e-commerce, meant to transpose in Romanian law Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"). The main objectives set out by the directive were provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States. The entire directive is structured around four focal points, which the Romanian law adopts and develops: the free movement of information society services, commercial communications, contracts concluded by electronic means and liability of intermediary service providers. As regards the liability of service providers, the law regulates intermediary services as mere conduit of the information (Article 9), the intermediate and temporary storage of the information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, also known as *caching* (Article 10), the permanent storage of information provided by a recipient of the service, also known as *hosting* (Article 11).

The Romanian law on e-commerce contains an article which defines the key words of the law (Article 1), which has the merit of introducing into national legislation new basic concepts of a technical and legal language consecrated by the European Union (electronic means, "information society services", "service provider", "established service provider", "commercial communication", "opt-out register"). This language is indispensable to the law's harmonization with the rhythm of technological evolutions and, at the same time, that of the Romanian legislation with the European one.

Article 2 establishes the objective of the regulation and the scope of the law, in keeping with the provisions of Directive 2000/31/EC. Article 4 entrenches the principles of the provision of IT services in Romania: the principle excluding prior authorisation, under the limits provided by para. (2) and the principle of non-discrimination between Romanian providers and EU providers established on Romanian territory.

Article 8 contains a provision which helps eliminating an important uncertainty which put a strain on the contractual circuit in the electronic environment. The text clearly stipulates which is the moment when an electronic commercial contract is considered to have been concluded.

The sanctioning regime was elaborated having in mind the practical impossibility of exercising an efficient, and especially, thorough control over the activities developed in the electronic environment. This is the reason why the legislator opted for the sanction considered to have a real applicability in the case of electronic commercial contracts, namely the relative nullity in the situation in which the provider has breached the obligations provided by law regarding the information and protection of the potential co-contracting party. The legislator creates, thus, the presumption that such a provider has determined the emergence of the contractual relation by vitiating the will of the other party.

The law also stipulates sanctions having the nature of a civil fine for those situations in which an effective control of the activities developed by a service provider is, indeed, possible. Moreover, in the spirit of the protection of the weaker party in the contractual relation, it is expressly provided that, in the litigations regarding the provision of a service of the information society, the burden of proof of the fulfillment of the obligations to inform, to protect the co-contracting party or those related to the performance of commercial communication belongs to the provider of the services, if the other party has the quality of consumer.

At present, the main provisions of Laws no. 161/2003 and 365/2002 have been included in the new Penal Code. The decision to proceed to the drafting of a new Penal Code was not a mere manifestation of the political will, but equally represented a corollary of the economic and social evolution – and also of the doctrine and case-law – and was based on a series of shortcomings in the regulation of the 1968 Penal Code.

A very important role in the harmonization of the legislation with the constitutional provisions has been played by the Constitutional Court, both through its *a priori* and *a posteriori* judicial review, the latter taking the form of the settlement of the constitutional challenges raised before the courts.

Following a failed Penal Code, repealed before even coming into force,[24] the current Penal Code was adopted through Law no.286/2009.

Published in the Official Journal, Part I no. 510 of 24/07/2009, the new Penal Code, immediately after birth, has been submitted to modifications by means of two laws, passed within an interval of less than one month, an utter example of lack of consistency and perspective in a criminal policy which sees itself as reformatory, although the distinguished members of the Cabinet had forgotten the fact that they had committed, within 12 months from the date of the Penal Code's publication in Romania's Official Journal, to submit to the Parliament a draft law for the implementation of the Penal Code, a good opportunity to make the desired amendments.

[24] 2004 Penal Code (Law no. 301/2004, Official Journal no. 575/29.06.2004)

It took almost five years since the publication of the current Penal Code for it to enter into force on February 1st, 2014 as a result of Law no. 187/2012[25] which, in turn, has brought some changes to the original shape of the Penal Code.

The offenses in the IT field provided in the new Criminal Code, contained in Chapter VI of Title VII, were developed taking into account, mainly, the provisions of this special law, matters concerning judicial practice, the features of cyberspace and of the means of electronic communications, and also the need to provide an appropriate legal response in the context of this phenomenon which is continuously on the rise, namely the antisocial acts committed in the electronic environment.

Since it facilitates communication and the dissemination of information on a planetary scale, the Internet favours offenses and appears as the vector of a new form of crime, regarding which the application of criminal law tries to identify the perpetrators, given its international dimension. The difficulty is also related to the fact that the Internet faces the heterogeneity of legal systems on a global scale. What is criminalized in one country is not necessarily incriminated in another. In addition, a major difficulty lies also with the proving of the offenses. The proof of the connection to a particular website is extremely difficult to establish.[26]

The new Penal Code criminalizes the following acts in connection with the information field or which could be considered as relevant to the extent that the deeds are carried out in connection with a computer system or software: Article 208– Harassment, Article 230 – Theft for the purpose of use, Article 249 – Computer fraud, Article 250 – Fraudulent financial operations, Article 251 – Acceptance of fraudulent financial operations, Article 302 – Violation of the secrecy of correspondence, Article 311 – Forgery of debt securities or payment instruments, Article 313 – The circulation of counterfeited values, Article 314 – Possession of instruments for counterfeiting values, Article 324 - Falsification of technical records, Article 325 – Computer forgery, Article 374 – Child pornography, Article 388 – Electronic vote fraud, Article 391 – Falsification of electoral documents and records.

[25] Published in Official Journal of Romania, Part I, no. 757 from November 12th 2012.

[26] Boroi, A., Gorunescu, M., Barbu, A., *Dreptul penal al afacerilor*, 5th edition, C.H. Beck Publishing House, 2011, p. 488.