SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2810-4188, ISSN-L 2810-4188
Nº. 1 (2021), pp. 577-585

PERSONAL SAFETY IN COMPLIANCE WITH THE REGULATIONS OF THE ROMANIAN PENAL CODE

M.G. POPESCU

Miron Gavril POPESCU
Faculty of Humanities and Social Sciences,
"Aurel Vlaicu" University of Arad
E-mail: mirongavril.popescu@yahoo.ro
ORCID: 0000-0002-3935-707X

Abstract

Guaranteeing liberty and security rights is a fundamental principle of law state and its legal regulation is a priority in the legal systems of the countries of the European Union.

The rapid development, of technology information and its applicability, in the last decades, have ensured its access in all sectors of life, from economic to social and cultural. With these premises, cybercrime has become a field of maximum and acute actuality.

By promoting and protecting the fundamental rights of citizens and the state law, the right to liberty and security of person and in the cyber environment must be guaranteed.

The Romanian legislator shows an active and constant interest in the field, by substantiating and updating the internal normative framework that regulates information systems, as well as by ratifying the legal documents issued by the Council of Europe.

Keywords: *freedom, security, computer system, computer data, cybercrime*

INTRODUCTION

The concept of personal safety, its classic sense, in historical evolution. Viewed in historical evolution, the theme of liberty subtle appears, at the beginning of the fourteenth century, in Western Europe, more precisely in France, whose kings at that time, Philip the Fair in 1311, respectively, Louis the X-th, in 1315, issued two ordinances, in order to abolish the relations of servitude, invoking the natural law, according to which every human being must be born free.

However, the first constitutional consecration of the right to liberty was made by the British, the Magna Charta Libertatum, adopted and signed in 1215 by King John Lackland, being the first document by which the English nobility restricted monarchical power, requiring the king to respect its privileges.

Art. 39 of the Magna Charta Libertatum expressly provided that *no free man shall be arrested or imprisoned, or deprived of his property, or declared outlawed, or left in any manner, and we shall not act against him, and no one will go against him without a fair trial of his judges, according to the law of the land*[1].

The concern of modern states for the legislative consecration of individual liberty was later materialized, in chronological order, in England by the Petition of Rights (1628) and the Habeas Corpus Act[2] (1679), respectively, in the United States by the Bill of Rights[3] (Virginia 1776), respectively, the US Declaration of Independence (July, 4th, 1776)[4], in France, the French Declaration of the Rights of Man and of the Citizen[5] (August, 26th, 1789) and, last but not least, the Universal Declaration of Human Rights (O.N.U December, 10th, 1948).

The term individual freedom is used in the current Constitution of Romania, the same semantics being used over time in the previous Romanian Constitutions (from 1866, 1923 and 1938).

The Romanian Constitution in force, regulates in article 23 two fundamental legal institutions, in close and mutual interdependence: individual freedom and security of the person. Thus, the Romanian legislator agrees with the current acceptance of the European Court of Human Rights, *as the right to liberty and security is unique insofar as this expression must be read in a single sentence* (Macovei, 2003, p. 95).

According to these regulations, the security of the person as a fundamental right, represents the guarantee given by the Constitution to citizens and people against any abusive forms of repression and in particular against any arbitrary measures aimed at depriving them of liberty by arrest or detention (Tudor, 1998, p. 416).

[1] *Art. 39 Nulum liber homo capiatur vel imprisometur, aut dissaisatur, aut ultrager, aut executur, aut aliquo, modo destinatur, nec super cum ibimas, nec cum mittemus, nec per legale judicium parium suorum nel per legem terrae.*

[2] *Habeas corpus* represents the guarantee given by the Constitution to every English citizen, according to which once arrested or detained, the citizen will be referred without delay to a jury, called to pronounce either the release of the accused or his detention.

[3] *The Bill of Rights* expressly states that people are by nature equally free and independent. According to the same normative act, these are granted rights inherent to human nature, namely the right to life and liberty, as well as the right to acquire and preserve property and to pursue happiness and security.

[4] *The U.S. Declaration of Independence* settles down equality of all people as a bith consequence. At the same time, the Declaration provides inalienable rights to life, liberty and the pursuit of happiness, being regulated the establishment of governments that seek to respect these rights. Since the authority of these governments emanates from the consent of the governed, if the form of government becomes destructive, the people have the right to remove it. The same Declaration states the independence of the judiciary, the right to be tried by a jury court, the subordination of the military to civilian power

[5] *The French Declaration* settles down, as a cardinal principle, the equality of all people in front of s law, the right to property, security, freedom of thought, expression and expression, deriving from this fundamental right.

I. THE CYBER SPECE – NEW REALITIES, NEW PERSPECTIVES ON PERSONAL SAFETY

The rapid development of information technology and technique, in recent decades has made virtual communication tools / means a vital resource of daily activity, in all reference sectors of life, from the economic sector to the professional sector, the educational, social and cultural sectors.

Consequently, the values, principles and rules that the states of the European Community promote and regulate must also be respected and implemented in the on-line environment, so that cyberspace remains free and open.

The obligation to comply with these regulations has been laid down under the constitutions of the Member States, under general organic laws, special laws and last but not least, international legal documents, initiated by the Council of Europe.

The use of virtual space in everyday life, in order to facilitate social, economic, political relations, by ensuring a rapid exchange of information and other resources between states, citizens and ethnic groups, has been speculated by individuals and antisocial groups, which granted the extremely high dynamics to the development and diversification of information technology negative connotation.

The novelty, the complexity, the high speed of development, as well as the faulty and insufficient regulation of the protection in this field, including in terms of specific forensic tactics, have created a significant gap between resources alocated to protect and combat cybercrime and its evolution. Thus, today, the states of the European Union through individual and conjugated methods and tactics allocate legislative, human resources not just to ensure that the evolution of the cybercrime phenomenon has a proportional correspondent in the activity of prevention, detection and prosecution of criminals.

If, crime or delinquency *lato sensu* is a particular form of social deviance, this phenomenon affecting human relations with a negative effect on public order and communities of people, violating the social values characteristic of a society and not only, given the danger of the phenomenon[6], cybercrime is considered as the set of crimes committed, through or in connection with the use of computer systems or communication networks, in a given time and space, computer systems and communication networks can be both the instrument, target or location of these crimes (Ioniță, 2010 , pp. 395-398).

The legislation of the member states of the European Union and implicitly the Romanian legal norm, doctrine and criminal judicial practice, settle four areas of action of cybercrime[7], currently delimited, as follows:

a) activities that harm privacy: collection, storage, modification and disclosure of personal data;
b) dissemination activities of obscene and/or xenophobic content: pornographic material, racist material and inciting violence;
c) economic crime, unauthorized access and sabotage; activities aimed at distributing viruses, espionage and computer fraud, destruction of data and

[6] http://www.criminalitatea-informatica.ro
[7] www.eur-lex.europa.eu

programs or other crimes; programming a computer to "destroy" another computer;

d) inobservance of the intellectual property right.

Whereas today the phenomenon of cybercrime is one of the major threats of the 21st century, which is progressing at an extremely fast pace and in a surprisingly versatile manner, both in itself and as a *modus operandi* for other types of crime, the Council Europe has initiated numerous steps to regulate virtual activity, in order to protect the security of the person, in the virtual space.

Thus, the Council of Europe issued a series of recommendations, among which we mention: Recommendation R (85) 10[8], Recommendation R (95) 13[9], Recommendation no. R (89) 9[10].

Pursuant to R (89) 9, the main criminal offenses belonging to virtual space are inventoried, under the generic name of minimum list. This minimum[11] *list is completed with the facultative*[12]*list.* The Council specificates that this list is not limitative, moreover, the Council's recommendation is to pro-update and pro-adaptability, so that the above-mentioned lists are supplemented by other facts likely to incriminate: the creation and dissemination of computer viruses, trafficking with illegally obtained passwords, etc. intended to facilitate the penetration of a computer system, disturbing the proper functioning of it or of stored computer programs, etc. (Vasiu, 1998, p.98).

II. NATIONAL REGULATIONS FOR THE PROTECTION OF PERSONAL SECURITY RIGHT IN THE CYBER SPACE

In this context, the Romanian legislator has proved an active and constant interest in the field of information technology, by regularizing and updating the internal regulatory framework governing information systems, various facts related to information systems or the information society as a whole, and by ratification legal documents issued by the Council of Europe.

Thus, the following laws were enacted: Law no. 365/2002 on the regulation of electronic commerce amended by Law no. 121 of May 4th, 2006, Law no. 64/2004 for the ratification of the Council of Europe Convention on cybercrime, Convention

[8] Its object, the rules for the application of the European Convention on Mutual Assistance in Criminal Matters, the letters rogatory on the interception of telecommunications.

[9] The object of this recommendation is to regulate the aspects of criminal procedure related to information technology.

[10] According to this recommendation, illegal acts related to computer systems are defined and classified for the first time, respectively, the rules to be applied by Member States to combat cybercrime are enacted.

[11] The minimum list includes: computer fraud, computer forgery, damage to data or computer programs, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of computer protected programs; unauthorized reproduction of a protected topography, while the optional list includes alteration of data and computer programs, computer espionage, unauthorized use of a computer, unauthorized use of a protected computer program.

[12] www.coe.int.ro

of November, 23th, 2001 on cybercrime, Law no. 196/2003 on preventing and combating pornography republished in M. Of. no. 198 of March 20th, 2014, Law no. 161/2003[13] on some measures to ensure transparency and exercise of public dignity, public office and business environment, prevention and sanctioning of corruption and last but not least the Criminal Code (Law 286/2009), which entered into force on February 1st, 2014.

The General Part of the Penal Code, *Title X* - The meaning of some terms or expressions in the criminal law, the chapter allocated to explain the meaning of some terms or notions includes the definition of the *computer system, computer data, electronic payment instrument*.

Thus, according to art. 180 of the Penal Code- General Part, *the electronic payment instrument is an instrument that allows the holder to make cash withdrawals, upload and download an electronic money instrument, as well as transfers of funds other than those ordered and executed by financial institutions.*

The provisions of Penal Code – General Part, art. 181 regulates, in the first paragraph, the notion of *computer system as any device or set of devices interconnected or in a functional relationship, one or more of which ensures the automatic processing of data by means of a computer program, and in the second paragraph, the notion of computer data as any representation of facts, information or concepts in a form that can be processed by a computer system.*

Regarding the Special Part of the Penal Code, unlike the other categories of crimes, *grouped as a rule, in a single title or chapter,* according to their legal object, we find cybercrimes regulated among other category of crimes: against property, false, offenses against public safety.

Therefore, we will analyze, in the following lines, cybercrimes *that generate quantifiable material damages,* crimes regulated in Title II of the Special Part of the Criminal Code, *Crimes against property,* more precisely Chapter IV, *Frauds committed through computer systems and electronic means of payment.*

Thus, the Penal Code art. 249, incriminates the computer fraud, taking over the whole regulation provided by art. 49 of Law no. 161/2003 (recalled with the entry into force of the Penal Code) and establishes its sanctioning regime. Cyberfraud means *the introduction, modification or deletion of computer data, restriction of access to such data or impeding in any way the operation of a computer system, in order to obtain a material benefit for oneself or for another, if a person has been harmed,* which is sanctioned by imprisonment from 2 to 7 years.

Art. 250 of the Penal Code, partially taking over the provisions of art. 27 and art. 28 of Law no. 365/2002[14], impleads and establishes the sanctioning regime of

[13] According to Law no. 161/2003, seven crimes are incriminated, which correspond to the classifications and definitions given by the Convention on Cybercrime.

[14] Law no. 187/2012 for the implementation of Law no. 286/2009 on the Criminal Code, states that on the date of entry into force of the provisions of the Criminal Code, art. 24-29 of Law no. 365/2002 on electronic commerce, art. 42 - 47, art. 48 - 50 and art. 51 of Law no. 161/2003 on some measures

fraudulent cash *financial operations* or by using an electronic payment instrument or accepting the realization of such illicit transactions, as follows: *carrying out a cash withdrawal operation, loading or unloading of an instrument electronic money or funds transfer using, without the consent of the holder, an electronic payment instrument or identification data that allows its use, shall be punished by imprisonment from 2 to 7 years.*

The second and third paragraphs of the same article regulate alternative modalities regarding the material element of the objective side of the crime, namely: *the unauthorized use of any identifying data or through the use of fictitious identifying data,* for which the legislator establishes the same sanctioning regime, while the manner provided for in the third paragraph *the unauthorized transmission to another person of any identification data, in order to carry out one of the operations provided in par. (1),* has a milder sanctioning regime, imprisonment from one to five years.

Article 251 of the Penal Code impleads *the acceptance of fraudulent financial transactions*, committed by accepting a cash withdrawal operation, loading or unloading of an electronic money instrument or transfer of funds, knowing the operation is carried out using an electronic payment instrument falsified or used without the consent of its holder, either knowing that it is carried out through the unauthorized use of any identification data or through the use of fictitious identification data and establishes the sanctioning regime: imprisonment from one to 5 years.

Art. 252, which ends the chapter *Frauds committed through computer systems and electronic means of payment,* incriminates the attempt for each of the infractions regulated by this chapter provisions.

Title VI of the Special Part of the Penal Code, using the marginal term of Forgery Offenses, incriminates in Chapter III, false in documents, at art. 325 *the crime of computer forgery*, the new legal provision representing the taking over in full of art. 48 of Law no. 161/2003 which it repealed.

Thus, according to Romania legislator: *to enter, modify or delete, without right, computer data or to restrict, without right, access to these data, resulting in data untrue, in order to be used to produce a legal consequences*, represents *crime of computer forgery,* an act whose commission is punished by imprisonment from one to 5 years.

Infractions against the security and integrity of computer systems and data are set in the regulation of the Special Part of the Penal Code, in Chapter VI of Title VII - Offenses against public security.

Any *illegal access to a computer system, illegal interception of a computer data transmission, alteration of computer data integrity, disruption of computer systems operation, unauthorized transfer of computer data, and illegal operations with*

to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption.

computer devices or programs are incriminated and sanctioned as offenses. Even any attempt to such offenses are being sanctioned.

Thus, based on the three paragraphs of art. 360 of the Penal Code, *illegal access to a computer system,* is sanctioned differently. *If the purpose of illegal access to the computer system is* to obtain computer data, the deed is punished by imprisonment from 6 months to 5 years. The sanctioning regime is harsher (the punishment being imprisonment from 2 to 7 years) if the illegal access concerns a computer system to which, through specialized procedures, devices or programs, access is restricted or prohibited for certain categories of users.

Pursuant to art. 361 the legislator regulates two alternative contents for the infraction of *illegal interception of a computer data transmission,* as the interception, without right, of a computer data transmission that is not public and which is intended for a computer system, comes from such a system or is performs within a computer system or the interception, without right, of an electromagnetic emission from a computer system, which contains computer data. The sanctioning regime is the same, imprisonment from one to 5 years in the case of committing the crime, for any of the alternative contents.

Within the same chapter, at art. 362 of the Penal Code, *the alteration of the integrity of computer data* shall be punished by imprisonment from one to 5 years and consists in the act of modifying, deleting or damaging computer data or restricting access to such data, without right.

The infraction of *disrupting the operation of information systems* is regulated by the provisions of art. 363 of the Penal Code, while *the unauthorized transfer of computer* data from a computer system or from a means of storing computer data is incriminated in art. 364 Penal Code.

The last criminal offense incriminated in this chapter has as object *illegal operations with devices or computer programs* (art. 365).

Any attempt to commit any of the offenses regulated by the provisions of this chapter shall be punished.

In the content of *Title VIII of the Special Part, Offenses that affect relations regarding social cohabitation*, in Chapter I *Offenses against public order and peace*, at art. 374 the legislator summarizes the similar provisions stipulated by three special laws, more precisely: Law no. 678/2001 on preventing and combating trafficking in human beings, Law no. 161/2003 on some measures to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption and Law no. 196/2003 on preventing and combating pornography[15].

Paragraphs two and three of the same article incriminates alternative modalities of the content of the infraction, which places it in the sphere of cybercrime, as well as their sanctioning regime: *production, possession for display or distribution, acquisition, storage, display, promotion, distribution, and the provision of child*

[15] Republished in M.Of. no. 198 of March 20th, 2014.

pornography, if it has been committed through a computer system or other means of storing computer data, shall be punished by imprisonment from 2 to 7 years, as well as *unauthorized access to child pornography. Minors, through computer systems or other electronic means of communication, shall be punished by imprisonment from 3 months to 3 years or by a fine.*

CONCLUSIONS

Through the brief reviw of the main legislative regulations on cybercrime, we wanted to emphasize the urgent need for the fundamental right to security to be rethought, reformulated and updated according to the increasing use of informatic means.

In this context, the security of the person in the cyber environment must be the priority of each state of law, in order to ensure real and effective protection of the fundamental rights of citizens, because the citizen's freedom and security can only be analyzed and enacted as an inseparable binomial.

In terms of substantive law, the states of the European Union impleads as crimes the facts directed against the confidentiality, integrity and security of data and information systems, illegal access to a computer system, alteration of data integrity, etc. Given the high dynamics of the evolution of cyberspace, permanent updates of the regulations of substantive law are required, so that they reflect, in a real and accurate way.

At the same time, the high dynamics of the evolution of cyberspace and the infinity of utilisations given to it, have made the Internet the main actor and tool of cybercrime, giving the opportunity to diversify the manifestations of the phenomenon, as well as outlining a strong cross-border character, specific to this type of crime.

In this context, we consider that it becomes urgent to substantiate cross-border procedural and legal provisions, in order to prevent, detect and prosecute criminals acting in virtual space, as well as ensuring a high specialization of structures to combat and investigate cybercrime.

BIBLIOGRAPHY

Drăganu, Tudor, *Constitutional law and political institutions: Elementary treaty*. Bucharest, Lumina Lex Publishing House, vol. 1, 1998.

Ioniţa, Gheorghe-Iulian, *Cybercrime and digital forensic investigation - terminological and content controversies*, in *Forensic Magazine*, June 2010, vol. XI, no. 3, Ed. Of the Romanian Association of Criminalists, Bucharest, 2010.

Macovei, Monica, *Freedom and security of the person: Guide to the implementation of Article 5 of the European Convention on Human Rights*. Manual no. 5. Chisinau, Directorate-General for Human Rights, Council of Europe, 2003.

Vasiu, Ioana, *Computer crime*, Nemira Publishing House, Bucharest, 1998.

Penal Code (Law no. 286/2009 published in the Official Gazette).

Law no. 365/2002 on the regulation of electronic commerce amended by Law no. 121 of May 4, 2006.
Law no. 64/2004 for the ratification of the Council of Europe Convention on Cybercrime.
Convention of November, 23th, 2001 on Cybercrime.
Law no. 678/2001 on preventing and combating trafficking in human beings.
Law no. 196/2003 on preventing and combating pornography republished in M. Of. no. 198 of March 20, 2014.
Law no. 161/2003 on some measures to ensure transparency and exercise of public dignity, public office and business environment, prevention and sanctioning of corruption.
http://www.criminalitatea-informatica.ro
www.eur-lex.europa.eu
http://cj.md
www.coe.int.ro