AN ANALYTICAL OVERVIEW ON THE VIRTUAL ENVIRONMENTAL CRIME

Nasty Marian VLĂDOIU*
“Transilvania” University, Brașov, Romania**

Abstract

Informational society represents a new stage of human civilization, a new way of life, that involves intensive use of information in all the aspects of human existence and activities, with a significant economic and social impact.

Although the idea of cybercrime is not new, the national legislator still faces serious regulatory issues of legislative instruments, able to assist in the prevention, detection and prosecution of those who commit crimes in the ‘Virtual’ environment.

In this article, we have tried to outline the issues of criminality in the virtual environment, highlighting the need for a legislative framework in complete agreement with the extent of the criminal phenomenon on the Internet, the technological development and the social requirements concerning the protection of citizens against racism, xenophobia and anti-Semitism favored by the use of online information transmission.

Keywords: informational society, criminal offences, cybercrime, virtual environment, racist threat, xenophobic threat, anti-Semitism, data transmission, Internet, computer fraud.

1. Introduction

In the development of society, analysts known three stages: agrarian, industrial and post-industrial. The end of a type of society and the beginning of another were separated by revolutionary, important events: the Industrial Revolution marked the transition to a new way of life of individuals and communities and, the post-industrial society emerged during the Cold War led to new opportunities for the development of society. Since 1973, the american sociologist, Daniel Bell¹, theorized the informational society, with the intention to announce the end of industrial society, which followed the agrarian one.

In D. Bell’s view, post-industrial society has the following characteristics: the transition from an economic activity based on the production of material goods to a

---

* E-mail: vladoiu.nasty@gmail.com.
** Ph.D., Associate Professor, Faculty of Law.
service-oriented economy; the predominance in the active population structure of the professional and technical class; the crucial importance of theoretical knowledge as a source of innovation and management (which is a guiding principle); the orientation to the implementation of learning technology; the emergence of a new „intellectual technology“.

In contrast to industrial society, post-industrial society is based on knowledge and not on work. Knowledge, especially scientifical and practical knowledge becomes the main means of production in post-industrial society, as capital and labor were strategic resources for the development of industrial society. The main feature of any society lies in the potential of basic research and its scientific and technological resources (universities, scientific laboratories) and of the ability to scientific and technological development. In this regard, informational society becomes the basis of an intellectual technology, in which theoretical knowledge and new information technologies are decisive for the industrial development.

The information concept used here defines „data processing“: the identification, the storage and the processing of datas becomes an essential resource for the economic and social exchanges. Knowledge is used in the sense of „organized set of statements or actions of ideas, presenting a rational analysis of experimental results, which is transmitted in a systematic form through means of communication“. In terms of the indicators specific for each type of society, informational society is the one that „the most important social, economic and manufacturing advantages are linking to the information processing and communications“2. The information becomes at the same time the main means of production and the main product of such a society. Informational society is based eminently on knowledge, on the generation and comparison of ideas.

Information becomes an essential resource in modern societies, politically, economically and socially evolved. The dynamism and complexity of the new type of society, which causes an increase in the volume and diversity of processed information and, also the widespread use of information and communication technologies (ICT), have led to the concept of informational society.

Informational society represents a new stage of human civilization, a new way of life that involves intensive use of information in all the aspects of human existence and activity, with a significant economic and social impact. Informational society allows its members, wide access to information, a new way of working and knowledge, amplifies the opportunity of economic globalization and social cohesion. Informational society integrates the objectives of sustainable development, based on social justice and equality of opportunity, freedom,

---

cultural diversity and innovative development, environmental protection, industrial and bussiness environment restructuring.

The dramatic changes in the past few years – the exponential growth of mobile communications and internet users, the contribution of ICT sector to economic growth and new job creation, the restructure of companies and bussinesses in general in order to take advantage by the new technologies, the accelerated development of e-commerce – support the transition from the industrial to the post-industrial era. Digital technologies increase more and more the easy access, the storage and the transmission of information. Digital information can be transformed into new social and economic values, creating huge opportunities for the new products and services development. Information becomes the key resource for the digital economy.

The „new economy” term concerns in particular the current transformations of economic activities as a result of the use of digital technologies, which provide access, processing and storage of information in a cheaper and easier manner.

The construction of the new society model raises major socio-political issues – both nationally and internationally – the mitigation of „digital divide” phenomenon (the exclusion of some categories and regions or geographical areas from the benefits of new technologies), the social cohesion, the conservation and promotion of the specific culture of each nation and local communities, the protection of citizens and consumer.

The only way that these problems could be solved is through a broad dialogue between the governmental authorities, the representatives of bussiness environment, of the academia and also of the civil society.

The Government and its institutions are designed to stimulate, conduct and control the transition process to the informational society, by initiating a specific regulatory framework and action programs.

In turn, the bussiness community in the field of information and communications technologies should provide high-tech products and services, at the most affodable prices and rates.

By the complexity of the phenomena involved in the development of informational society, phenomena that must be understood and managed by the necessity of a new culture of knowledge and learning in terms of using new technologies, and also by the necessity of research, development and technological innovation, the active participation of the academic community is also essential.

The civil society also has such an active role in formulating requirements and priorities regarding the use of new technologies to the benefit of the whole society, as well as an responsive role to the policies and governmental regulations. These roles can be exerted both at group level (non-guvernmental organizations, professional associations etc.) and individual level.
2. Romanian legislative guidelines in respect of offenses committed in the virtual environment

Given the current conditions that allow easy access to information in the virtual environment, regardless geographical or national boundaries, taking into account the virtually limitless possibilities of the exchange and dissemination of information, the evolution at technological level was practically inevitable. This evolution, however, has led to a significant increase of crime, being recorded the emergence of new crimes or the enhance of traditional crimes through the new technologies.

While criminality has increased with the technological development, the legal instruments of protection of citizens against abuses and harm, committed in the virtual environment, are jumping through hoops, and it feels at normative level, the stringent need for the legislator to devise ways that the access and carrying out activities through computer systems be made safe for public order, and those who exceed the limits to be held liable, particularly criminally liable.

A definition of cybercrime was formulated by the group of experts of the OECD in 1983, related to any misconduct, unethical or unauthorized, concerning automatic treatment of data and/or data transmission.

According to UNAFEI\(^3\) by cybercrime in a broad sense we understand: any crime in which a computer or a computer network is the subject of an offense, or a computer or a network is the instrument of carrying out a crime. While, in a narrow sense by cybercrime we understand: any offense in which the perpetrator interferes without authorization, with the processes of automatic data processing.

In the study „The legal aspects of cybercrime in the informational society” (the COMCRIM study)\(^4\) are presented categories and sub-categories of cybercrimes, such as violations of privacy, economic offenses, the penetration of computer systems in order to overcome technical difficulties of security („hacking”), computer espionage, the piracy of computer programs, computer sabotage, computer fraud, distribution of illegal or harmful information (racist propaganda, dissemination or child pornography etc.), crimes against life, crimes related to organized crime; electronic warfare.

Internally, there are now several legal provisions, included in special laws, that regulate various acts in connection with the virtual environment or informational society as whole. Are punishable as follows: crimes against the confidentiality and integrity of data and systems; computer crimes; child pornography through a computer system\(^5\); The offense of illegal access to a

---

\(^3\) The United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) that has the aim of promoting the sound development of criminal justice systems and mutual cooperation in Asia and the Pacific Region.

\(^4\) Realized for the European Commission by Ph.D. Professor Ulrich Sieber from University of Wurzburg, Germany

\(^5\) Law no. 161/2003 on certain measures to ensure transparency in the exercise of public dignities, public functions and in the business environment, the prevention and punishment of corruption, published in the Official Gazette no. 279 of 21/04/2003
computer system and The offense of unauthorized access to an electronic system; The offense of altering the integrity of computer data and, also destruction and theft offenses provided in article 217, respectively 208 of the Romanian Criminal Code; computer forgery and the offense of forgery provided in Title VII of the Criminal Code; Offenses involving computer fraud or deception set in article 215; Offenses of forgery and deception in connection with electronic payment instruments; The offense of making available to the public, including by Internet or other computer networks, without the consent of the holders of rights, their works or products bearing rights related to copyright or sui generis rights; The offense of public communication of works or products bearing rights related to copyright; The offense of promoting pirated goods by any means and in any manner, including by public notices or electronic means of communication.

Therefore, we observe a tendency of the national legislator to criminalize in principle, facts of an economic nature, committed in the informational environment, but also intellectual property offenses.

It is true that in terms of criminal groups activity, prevails the committing of financial offenses, by which are targeted payments systems, credit and payment products offered by financial institutions, hence the orientation of the legislator to criminalize as many offenses designed to protect individuals’ data.

The specialization of offenders by type of crime and destination countries, depending on the specific area, their permanent concern for the identification of new operating methods and techniques, of new products that can be defrauded, as well as computer systems that can be compromised, has led, in the past years, to increase annual criminality in the virtual environment.

Using juveniles with skills in the use of new technologies, organized and coordinated by leaders of specialized criminal groups, makes the judicial authorities approach difficult, in identifying the perpetrators of the virtual environment and instituting criminal proceedings against them. However, the ubiquity of the virtual environment, configure an extended character of gender crimes, taking into account that the victims are targeted everywhere.

The criminal groups are using systems and equipment in different countries of the world, so the judiciary's mission is carried out with difficulty. Computer fraud, cyber attacks, electronic payment fraud and child pornography in the online environment are criminal categories that require complex investigation, specialized training of those called upon to enforce the law and involve high cost equipment.

---

6 Law no. 297/2004 on the capital market, published in the Official Gazette no. 571 of 29/06/2004


8 Law no. 8/1996 on copyright and related rights, published in Official Gazette, part I, no. 60, of 26/03/1996, with subsequent amendments.
In this excurse we will stop to analyze an interesting problem and of dimension – phenomenon, regarding violations of the right to life protected in the virtual environment through the promotion of antisemitic, negationistic, racist and xenophobic attitudes.

protected in the virtual environment by We can thus speak of cyber-Semitism, cyber-negationism, cyber-racism and cyber-xenophobia, phenomenon adapted to the virtual environment, perfecting its techniques of promotion and dissemination of ideas, finding new adepts among youth.

Romania is one of the few European countries which has adopted a legislation in this area, however, we can see that the romanian legislator must adjust the speed of response depending on the conquests of technology and science, as the malevolent do.

3. The criminal protection of privacy against cybercrimes. Negationism, anti-Semitism, racism and xenophobia in the virtual environment

In order to find ways of combating racism, anti-Semitism and xenophobia, both at international and national level, there were concerns, particularly in the legal environment, to be created legal instruments able to provide protection of citizens injured in their rights and to facilitate the bringing to justice of those responsible for such manifestations.

Thus, the legislation of states tends to impede the racist, negationist, anti-Semitic and xenophobic attitudes, the threats and instigation of violence against groups of individuals, having as theme, the discrimination based on race, religion, nationality or ethnic origin.

The emergence and development of technologies, especially the expansion of the use of digital technologies, which provide access, processing and storage of information in a cheaper and easier manner, has led to the formation of an attractive and easy accessible perimeter of manifestation, of racist and xenophobic propaganda, and also allowed hiding the identity of individuals, thus hindering the approach of authorities in finding the offenders and holding them accountable.

Based on these realities, and the need to strenghthen the mechanisms for human rights protection, on January 28, 2003, there was signed in Strasbourg, an Additional Protocol\(^9\) concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems\(^{10}\), protocol ratified by Law no. 105/2009 of the romanian legislature.

Internally, since 2002 existed Emergency Ordinance no. 31/2002 prohibiting organizations and symbols of fascist, racist or xenophobic character and

---


\(^{10}\) To be seen at http://conventions.coe.int/treaty/en/Treaties/Html/189.htm.
promoting the cult of persons guilty of crimes against peace and humanity\textsuperscript{11}, subsequently approved by Law no. 107/2006\textsuperscript{12} – which gave it the character of an organic law.

Going through the provisions of this ordinance, we notice however, that it is „in legal damage”, the direct consequence is that of an objective and practical impossibility to hold accountable those who violate the criminal provisions in the field.

Thus, after the adoption of Law no. 107/2006, came into force Law no. 278/2006\textsuperscript{13} amending and supplementing the Romanian Criminal Code, which brings as novelty, the criminal liability of legal entities institution, an institution that began to produce full legal effects within 90 days of its occurrence in the Official Gazette.

Given that Law no. 278/2006 is also an organic law, it stands to reason that, if there is any inconsistency between the provisions of the two organic laws, they must be brought without delay in harmony and legality. The shortcoming in terms of legality consists in that in Law no. 107/2006, facts are considered offenses when the holder is an individual and are punishable as offenses, while when they are committed by a legal person are punishable as misdemeanors.

The law also penalizes only the establishment of organizations with fascist, racist and xenophobic nature, and the adherence to such organizations, while individuals who promote ideas, concepts, doctrines of the same character, can not be held liable, because their actions are not provided by the criminal law, which is an essential feature for the existence of the crime, along with social danger and guilt. For example, given the law in its current form, the individual can freely commit such acts, having in consideration that the legislator criminalizes only the organization and adherance, and also the supporting in any way of organizations with this character, which is, according to us, a great escape of the legislator.

From a different perspective, besides the fact that for six years we have had two organic laws with contrary legal provisions, regulating the same object, the authorities with law enforcement officials were notified repeatedly, and the given solutions were, in our opinion, legally unacceptable.

De lege ferenda, we believe therefore, that the immediately remedy for this „legal damage” would be, that Law no. 107/2006 approving the Emergency Ordinance no. 31/2002 prohibiting organizations and symbols of fascist, racist or xenophobic character and promoting the cult of persons guilty of crimes against peace and humanity, align to the provisions of the law that currently exist in the Criminal Code and Criminal Procedure Code through an emergency ordinance.

On the other hand, taking into account the fact that by Law no. 105/2009 was ratified the Additional Protocol concerning the criminalisation of acts of a racist

\textsuperscript{11} Published in Official Gazette, Part I, no. 214 of 28 March 2002.
\textsuperscript{12} Published in Official Gazette, Part I, no. 377 of 3 May 2006.
\textsuperscript{13} Published in the Official Gazette no. 601 of July 12, 2006.
An analytical overview on the virtual environmental crime

and xenophobic nature committed through computer systems, and that Chapter II of the protocol, called even „Measures to be taken at national level” states that „each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, acts of a racist and xenophobic nature committed through computer systems”, we consider even more necessary the coverage of this legislative gap, being required a well established legislative framework in the prevention, detection and punishment of such offenses. Romania is obliged under international instruments to which it is part of to develop a specific legal system that regulates this type of crimes.

Through the domestically adoption of Law no. 161/2003, the Romanian legislator has regulated this matter in the spirit of

The Convention on Cybercrime of the Council of Europe, in Title II of Book I, entitled „Preventing and combating cybercrime”, Articles 34-67, but these provisions cover just basically regulations and can not cover the criminal diversity which run today by a simple mouse clicking and using a keyboard.

4. Conclusions

Currently, in Romania there are several effective legal provisions, included in special laws on the criminal phenomenon and are being incriminated illegal acts in connection with computer systems or the informational society as a whole.

On the one hand, the rapid exchange of information, the exponential growth of Internet users, the development of technologies, the emergence of new digital systems and, on the other hand, the anonymity offered by computer systems, the messages encryption methods used through them, the establishment of organized groups, the structure and specialization of their members, the permanent concern to find new operating modes, products that can be easily compromised, the possibility to transmit or access illegally information without boundaries - represents reasonable grounds why the national legislator should be preoccupied in creating a legislative framework that meets the current social requirements, adapted to the new informational society, in order that the level of legal protection in the online environment could not be different from that of the „real environment”.

To note that cooperation between government, the business community, academia and civil society is particularly important for the outcome of legal regulations to correspond to a high-tech level, for the proper development of cybercrime to be proportionate to the prevention, detection and liability of offenders, which is currently overtaken by the acumen of perpetrators and the transboundary predominant character of their actions.

De lege ferenda, as the economic cybercrimes are the most numerous, should be adopted an International Code of conduct on electronic commerce, in order to have an uniform rule of the way that law should be applied in the virtual environment.
Internally, in fulfilling the obligations assumed as party to international instruments, it is more than necessary, the creation of a legal system regarding the protection of citizens against acts of racist, xenophobic and anti-Semitic nature, committed through computer systems.

Since, for the reasons shown above, the Emergency Ordinance no. 31/2002 is in „legal damage”, and therefore, we deal with an inefficient law in this area, an addition that has as subject the provisions stated in the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, would create and harmonize a legislation which can provide legal protection, both in real and virtual environment.

References
