THE INTERNET BETWEEN PROMOTION AND INFRINGEMENT OF THE FUNDAMENTAL RIGHTS FREEDOMS vs. CYBERCRIMES

Silvia-Maria Tăbușcă (Martiș)[1]

Abstract

The Internet has become a mean by which individuals can exercise their right to freedom of opinion and expression, as well as the freedom of association, which, both play a crucial role in supporting democracy and guaranteeing human rights. But, at the same time, it also has become a mean for human rights infringement such as privacy, discrimination of specific vulnerable groups, espionage, child pornography and prostitution, as well as the democratic destabilization.

The fundamental rights are neither created, nor abrogated by any state or non-state actor, being attached to humans at their birth only by the fact of being humans. "All men are by nature equally free and independent and have certain inherent rights, of which, when they enter a state of society, they cannot, by any compact, deprive or divest their posterity." These rights, recognized as universal, inalienable and indivisible, are supported by the International Bill of Human Rights, which comprises three main legal instruments: the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights.

The promotion and protection of all human rights and of democratic principles serves as an international minimum standard widely enforced. Therefore, the framework of international human rights law remains relevant and equally applicable to new communication technologies, such as the Internet.

Keywords: Internet, human rights, freedom, cybercrime, privacy, espionage, discrimination

1. Introduction

Information and communication technologies have become a part of daily life for a significant number of people around the world. In this way, the online networks and digital communication provide indispensable information resources especially for youngsters. Used by billions of people around the globe, the Internet has been shown to be, on one side, a main promoter of fundamental freedoms, and on the other side, an illusion of anonymous and private environment.

Starting from the well-known words of Lawrence Lessing, a law professor at Stanford University - "we can build or code cyberspaces to protect values that we believe are fundamental, or we can build or code cyberspace to allow those values to disappear[i]" -the present paper analyses the promotion of some rights and freedoms related to the Internet and, at the same time, it explains the need for Internet regulation in order to protect other rights

[1] Assistant Lecturer, PhD, Romanian-American University, School of Law

like the right to privacy, the rights of the child, freedom from discrimination as main human rights and the democratic system.

During the last decade, the number of Internet users worldwide grew from 400 million in 2000 to over 5 billion users in 2010[ii]. With this increase in the number of users, the promotion of human rights has extended at the expense of the threats to some other individual rights and security. It is therefore essential that all actors, both public and private, respect and protect human rights on the Internet.

Fundamental rights are universally accepted as a set of individual rights applicable to all, in any time and space. The fundamental rights are neither created, nor abrogated by any state or non-state actor, being attached to humans at their birth only by the fact of being humans. "All men are by nature equally free and independent and have certain inherent rights, of which, when they enter a state of society, they cannot, by any compact, deprive or divest their posterity[iii]".

These rights, recognized as universal, inalienable and indivisible, are supported by the International Bill of Human Rights, which comprises three main legal instruments: the Universal Declaration of Human Rights[iv], the International Covenant on Civil and Political Rights[v], the International Covenant on Economic, Social and Cultural Rights[vi]. The promotion and protection of all human rights serves as an international minimum standard widely enforced and needed for the individual security rights. Therefore, the framework of international human rights law remains relevant and equally applicable to the new communication technologies, such as the Internet.

2. Freedoms vs. Cybercrimes

The Internet has moved society closer to ideal justice[vii]. It has become a mean by which individuals can exercise their right to freedom of opinion and expression, as well as the freedom of association, which, both play a crucial role in supporting democracy and guaranteeing human rights. But, at the same time, it also has become a mean for human rights infringement such as the right to privacy, discrimination of specific vulnerable groups, espionage, child pornography and prostitution, as well as security rights.

Unlike any other means of communication, such as radio, television and printed publications based on one-way transmission of information, the Internet represents an interactive medium. It "has been established as a modality for the liberalization of communication and information… The media have, in practice, monopolized most of the real opportunities for public communication. Despite of this, the Internet has made freedom of expression a practical fact and a global phenomenon for anyone with a computer and a telephone[viii]". While this medium has arguably improved the general standards of living and access to information there are also a lot of other issue raised in the same time. Virtually any internet connection transmission can be intercepted, with or without the knowledge of the rightful sender or receiver, and thus one of the best solutions for ensuring people privacy over the internet is the use of better and better encryption solutions. This issue of ensuring internet privacy by means of encrypting data can be covered from two large perspectives: use of widely spread and tested solutions (either commercial of freeware versions) or use of

localized and specialized solutions with a lower degree of usage, fact that by itself renders the protection degree to a higher level (less people use it, less people try to break it). Among the known and established protection solutions with widespread use we can mention PGP[2], BitLocker, TrueCrypt or SafeVault software suites while for the second category we can list any personal development of a software based on powerful yet quite unknown algorithms such as MSDSSA[3][ix], Misty1-10[4] or XTEA[5]. Besides the privacy breach that internet users might suffer in conjunction with different messages transmitted over the internet, there is also another very specific and concerning issue related to the same problem: the material losses one can suffer after using different forms of online payment. This special problem is very important and may be of great importance when balancing diverse freedoms versus restraints when using the internet[x].

2.1. Freedoms

The revolution of the new technologies changed our society and will continue to do so in the future. Based on what we have achieved through the information technologies, there is no doubt that the equal right to access and use a secure and open Internet is the main freedom related to this environment. Thus, the users should have access to legal content, should be able to run applications of their choice and should be permitted to attach any legal electronic information.

Furthermore, the Internet has become the key environment by which individuals may exercise their freedom of opinion and expression[xi] as it is guaranteed by the art.19 of the International Covenant on Civil and Political Rights. The protection of this freedom requires respect of the "right to hold opinions without interference". It includes not only freedom to "impart information and ideas of all kinds", but also freedom to "seek" and "receive" them "regardless of frontiers" and in whatever medium, "either orally, in writing or in print, in the form of art, or through any other media of his choice". So, the main freedoms comprised in this article are:

- *freedom to hold opinions*, which gives citizens the right to criticize the government and to form opposition. In this way any state must not indoctrinate its citizens;
- *freedom to impart information and ideas of all kind*, which give citizens the right to distribute information and ideas through all possible lawful sources, including Internet;
- *freedom to receive information*, which includes the right to gather information and to try to get information through all possible lawful sources, including Internet.

[2] PGP = Pretty Good Privacy software application
[3] MSDSSA = Multilayered Structural Data Sectors Switching Algorithm, proposed by Alex Tabusca from the Romanian-American University
[4] MISTY1-10 = encryption algorithm proposed by Mitsuru Matsui and others from Mitsubishi Electric
[5] XTEA = Extended Tiny Encryption Algorithm, proposed by David Wheeler and Roger Needham from Cambridge Computer Laboratory

Other relevant statement made by art.19 is related to the term "regardless of frontiers", which feats perfectly into the new technology of the Internet. It indicates that the information, both imparted and received, may come from beyond the frontiers of the country.

Based on these freedoms, the Internet empowers individuals to widely disseminate their opinions and, indeed, reach broad audience. Information is more and easily accessible today. Thus, the human rights news travel far and fast on the Internet without boundaries or restrictions and a violation of human rights, a massacre, a mass arrest is immediately known worldwide. For example, recordings and photos of the war crimes and crimes against humanity committed in the Darfur region of Sudan, from August 2003 to March 2004, were widely spread all over the world throughout the Internet.

Moreover, the last year death in police custody of a 28-year-old Egyptian businessman, determined the creation of the largest dissident web page called "we are all Khaled Said". He was removed from an Internet Cafe in Alexandria by two police officers who then beat him to death. A human rights activist used the Internet to spread the word about human rights violations in Egypt by posting photos of Said's battered and bloodied face contrasting with pictures of him happy and smiling. This death was considered a symbol against the oppression that any Egyptian might face because Said did not belong to any faction and was not a political opponent, but a simple citizen.

Initially, the webpage offered the Egyptians a tool to express their opinions about government abuses in a country where freedom of expression and freedom of assemble were limited. Subsequently, the forum invited people to a popular uprising that started on 25 of January 2011. Millions of protesters demanded to overthrow the regime of Egyptian President, Hosni Mubarak, and to establish a democratic system of government.

The online social media played a major role with regards to the recent acts of disorder committed in London. It encouraged the population to take part, in a larger number, in the 2011 public unrest in several cities from UK. Therefore, a 16-year-boy and an 18-year-man, who posted on Facebook messages inciting others to riots, were detained as result of a police operation in south side of Glasgow, being charged with breach of peace.

2.2. Cybercrimes

If, within the previous part of the present paper, I have presented the main advantages of using Internet in order to promote human rights and democracy, now it is the time to talk about the danger of the enormous amount of personal information that people reveal when they use Internet and about the infringement of democratic principles. At the present time, technological advancements and digital infrastructure bind the world population in a complex and intertwined system. Most of the public facilities, such as electricity supplies, transportation systems, military services, depend on the use of new technologies and the stability of the cyberspace. The last decades' attacks against information infrastructure and Internet services have shown our vulnerability to the new crimes.

The 2005 – 2007 power outages, which left more than half of the Brazilian population in the dark, was caused by cyber-attacks, even if the government put it on the weather. It is known

that most electric grids are so interconnected to the Internet that an attacker can easily penetrate these networks from anywhere. They said that cybercrimes presents a major threat to Brazil, the world's second-largest power producer, and to other countries where critical infrastructure such as health system, defense, emergency response, banking, telecom, are connected to the Internet. Furthermore, in June 2008 hackers broke into a Brazilian governmental website, comprising valuable data for which they demand 350 million dollars ransom. This amount was not paid, there being a backup of the information, but it took over a week to regain control from the hackers[xii].

In May 2007, Estonia, which is a member of NATO and the European Union, was under attack by a rogue computer network - "the attacks were aimed at the essential electronic infrastructure of the Republic". The national security of the entire country was affected and all commercial banks, telecom, media outlets felt the impact of the hackers actions. Estonia was slammed with traffic coming in from more than 4 million packets per second; nearly 1 million computers suddenly navigated to a multitude of Estonian site, from foreign ministry to the major banks. The identified cause was botnets comprising hijacked computers in the US[xiii]. It was said that the attacks were virtual, psychological and real.

In July 2009, there were 27 American and South Korean government agencies and commercial websites temporally jammed, among which the American Treasury Department, Secret Service, Federal Trade Commission and Transportation Department, New York Stock Exchange, Nasdaq, as well as the South Korean's Defense Ministry, the National Assembly, Presidential Blue House, Shin Han Bank[xiv].

The results of spy agencies have shown that the attacks appeared to be carried by a specific organization or a government, rather than an individual hacker. Therefore, the development of information society has given rice to new type of crimes and to the commission of traditional crimes using Internet, which can be easily spread because they are not restricted by the national boundaries. At the same time, the new technologies permit the criminals to be located in other places than the one where their acts produce the effects. Based on these specific aspects related to the commission of new crimes, the solutions to this problem must be addressed through the norms of international law.

The term "cybercrime" refers to any crime that involves a computer or a network, which is used for the commission of a crime. In order to commit a crime, a user has to take criminal offences against the confidentiality, integrity and availability of computer data and systems through illegal access, illegal interception, data interference or system interference.

Illegal access may give to a user control over the confidential data and secrets or encourage him to commit more dangerous offences, like computer related fraud or forgery. The access is defined as being the fact of entrance into another computer system or to a computer system on the same network, such as LAN or Intranet, without the right to do so.

Illegal interception represents the act of procuring the content of data directly, by accessing and using the computer system, or indirectly, by using electronic eavesdropping or tapping devices, through devices which collect and record wireless communications. This offence

applies also to non-public transmission of data, which may be publicly available information, communicated confidential or may be kept secret for specific purposes.

The term "system interference" is legally referred to as computer sabotage and it criminalizes the intentional hindering of the lawful use of computer systems by using or by influencing computer data. All these aspects of cybercrimes may have as a result the infringement of individual rights, especially the right to privacy. In this context, there is an illusion that the Internet is a unanimous and private environment, but it is absolutely not.

3. Conclusions

By the end of 2011, eighty-two countries[xv] around the world had adopted a national broadband strategy in order to provide larger access to the Internet, developing public services online such as e-health, e-education and e-government. In this way, most of the counties promote and respect fundamental freedoms and democratic principles. It has been proven that the Internet, as a whole, but especially the Facebook and YouTube, have already started to play a major role in promoting fundamental rights and widely showing their violations when they occur.

At the same time, the Internet became an ungoverned territory that is marked by anonymity and easy to commit crimes, being a less protective place. The cyberspace has created the "crime of choice" because its attribution is difficult to be done and criminals are rarely caught and prosecuted. Moreover, the Internet may become the "weapon of choice" giving easy access to a nation's most sensitive data and national infrastructure. Usually, ministers of defense develop strategies to combat the threats of missile attacks, naval bombardment and tank advances, but not digital invasion.

Nowadays, cyber-attacks are becoming more popular and can cause significant damage to both countries and companies by stilling large amounts of classified data and crippling economies. The last decades' attacks against information infrastructure and Internet services have shown our vulnerability to the new type of crimes related to the information technology and communication.

Bibliography

[i] Lawrence, Lessig. 2006. „*Code: And Other Laws of Cyberspace*". Basic Books.

[ii] International Telecommunication Union, StatShot No. 5, January 2011, available from: http://www.itu.int/net/pressoffice/stats/2011/01/index.aspx

[iii] Virginia Declaration of Rights was adopted unanimously by the Fifth Virginia Convention, on 12th of June 1776.

[iv] UDHR was adopted by the UN General Assembly on 10th of December 1948 at Paris, France.

[v] There are two Optional Protocols to the ICCPR. The First Optional Protocol establishes an individual complaints mechanism, allowing individuals to complain to the Human Rights Committee about violations of the Covenant, while the Second Optional Protocol abolishes the death penalty.

[vi] The Optional Protocol to the ICESCR is a side-agreement to the Covenant which establishes complaint and inquiry mechanisms and allows its parties to recognize the competence of the Committee on Economic, Social and Cultural Rights to consider complains from individuals. It was adopted by the UN General Assembly on 10th of December 2008 and opened for signature on 24th of September 2009.

[vii] Bell, Bernard. 2001. „*Filth, Filtering and the First Amendment: Ruminations on Public Libraries' Use of Internet Filtering Sofwere*". Federal Communication Law Journal 53: 191.
[viii] Steven Hick, Eduard Halpin, and Eric Hoskins. 2000. „*Human Rights and the Internet*". New York, Palgrave Macmillan: 276.
[ix] Tabusca Alexandru, 2010. „A new security solution implemented by the use of Multilayered Structural Data Sectors Switching Algorithm (MSDSSA)", published in „Journal of Information Systems & Operations Management – Vol.4, No.2 – December 2010" – ISSN 1843-4711, Universitary Publishing House, pages 164-168
[x] Pîrjan Alexandru, Petroşanu D. 2008. „A Comparison of the Most Popular Electronic Micropayment Systems", published in „Romanian Economic and Business Review", Volume 3, Number 4/2008, pp. 97-110, Pro Universitaria Publishing House, Bucharest, ISSN 1842 – 2497.
[xi] In its very first session in 1946, the UN General Assembly stated, "Freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated" (A/RES/59(1): Para.1).
[xii] Michael Mylrea. 2009. „*Brazil's Next Battlefield: Cyberspace*". Foreign Policy Journal:15.
[xiii] Joshua Davis. 2007. „*Hackers Take Down the Most Wired Country in Europe*", Wired: 21.
[xiv] Choe Sang-Hun and John Markoff. 2009. „*Cyber attacks Jam Government and Commercial Web Sites in U.S. and South Korea*". The New York Times: 8.
[xv] Among which Albania, Andorra, Argentina, Azerbaijan, Bahrain, Brazil, Burkina Faso, China, Colombia, Dominica, Dominican Republic, Egypt, Finland, Ghana, Grenada, Guinea, Haiti, India, Kazakhstan, Liechtenstein, Malawi, Malaysia, Mongolia, Morocco, Nepal, Nicaragua, Nigeria, Oman, Pakistan, Peru, Samoa, Saudi Arabia, Sierra Leone, Sri Lanka, Spain, Sudan, Suriname, Switzerland, Trinidad & Tobago, Uganda, United States.
Hamadoun Toure. 2011. „*The Quest for Cyber Peace*". ITU.
Convention on Cybercrime, Council of Europe, Budapest, 23 November 2011.