IWONA FLOREK

Alcide De Gasperi University
of Euroregional Economy in Józefów

iwona@wsge.edu.pl

ORCID: 0000-0003-0194-3361

SUSRAN ERKAN EROGLU

Alcide De Gasperi University
of Euroregional Economy in Józefów

ORCID: 0000-0003-1522-9652

DOI: 10.13166/JMS/112765
JOURNAL OF MODERN
SCIENCE TOM 3/42/2019,
S. 27–36

THE NEED FOR PROTECTION OF HUMAN RIGHTS IN CYBERSPACE

ABSTRACT

Technology is an integral part of social life. The widespread use of computers and the development of information and communication technologies have made people dependent on this technology in many ways. Computer products such as Internet, mobile phone, satellite are among the indispensables of daily life. The developments in information technologies attract the attention of the international community as much as the individuals and affect this society as well. In particular, the tools and methods that are created by using computers have created cyber area life in addition to the real world, and this area has begun to provide significant benefits and facilities in the daily lives of individuals and communities. In this article the relation between cyberspace and protection of human rights in this sphere will be examined socially and legally.

KEYWORDS: *Human rights, cyberspace, individual rights, protection*

INTRODUCTION

Using an unlimited, seemingly knowledgeable resource such as the Internet, users of cyber space are exposed to many threats. Attention is drawn to, among others on the collection of data on citizens by various entities from the public and private sectors and the issue of possible use of this information in the future, as well as a kind of exploitation of consumers who are appropriately manipulated participate in increasing the profits of companies and corporations, often in an illegal manner (Czopek, 2016, 67-73). According to M. Sitek, man in this new reality (virtual reality) is treated more subjectively than objectively (Sitek, Such-Pyrgiel, 2018, 202), which entails the hypothesis that the protection of human rights in cyberspace is not as well developed as in the virtual reality. The development of teleinformatic technologies and the Internet causes coming into existence of new threats so as cybercrisises. Virtual reality is also the source of considerable risks for individual's safety (Zawisza, 2015, 403). In the context of such threats related to the development of the Internet, the issue of protecting the privacy of people using the network seems particularly important.

Countries' dependency on information technologies and especially to the Internet is increasing day by day. Today it is estimated that 168 million DVDs are produced in a day, which is sent to 294 billion e-mail messages daily on the global network. A total of 864,000 hours of video is uploaded daily to Youtube servers, while Netflix users are watching 22 million hours of TV or cinema in one day. Nearly two-thirds of the world's population has Internet connections and 20% have membership in social networks. Again, 85% of the world's population use mobile phones (Klimburg, 2012). These figures show how the dependence on information technologies has increased. Information technologies, in addition to the opportunities provided to facilitate life, also led to the development of new concerns in the security dimension. In this new world, criminal acts such as theft and fraud have become possible without the need for physical contact or being in the same place as the victim. Furthermore, information technologies have increased the communication skills of criminal groups or terrorist organizations, strengthened the possibilities of propaganda and ensured the emergence of new fields of activity. However, it has some disadvantages due to malicious and unconscious use. For example, the fact that terrorism takes place in cyber areas beyond traditional methods leaves the world facing a cyber-terrorist threat (Domański, 2013, p.83). Now the terrorists have begun to use new methods of cyber attack beyond their traditional methods. The rapid development of computer and Internet technologies makes it difficult for governments to monitor the virtual world and often leaves them inadequate and helpless. For this reason, governments prefer to avoid traditional methods, ie prohibition and access, to combat malicious practices in the virtual world by escaping into simplicity. However, with the introduction of computers as a means of attack by terrorist groups, international organizations such as NATO and the EU, as well as countries such as the USA, China and Russia, are also investigating how to protect against a possible cyber attack. In addition, the task to respond quickly to possible cyber attacks and to remove the communication and coordination of enemy forces to eliminate the information technology "cyber forces" have started to have (Billo, Chang, 2004).

On the other hand, many children across the world face sexual violence and gender-based violence, physical punishment, war and other forms of violence. Many of them are also exposed to gang violence, armed assault, rape, harassment and sexual and gender-based violence by their peers in the schoolyard. In addition, advances such as cyberbullying, especially through mobile phones, computers, websites and social networking sites, are a new form of violence that adversely affects children's lives. Cyber bullying is typically defined as the behavior that individuals or groups perform in digital environments to cause discomfort or harm to others. The higher the chances of staying anonymous and the lack of oversight, the higher the number of victims, the higher the rate of thinking about bullying and the maximization of the distress that will arise, the cyber bullying that a potentially larger audience is witnessing to bullying is separated from the traditional bullying by the before mentioned features (Boulton, Hardcastle, Down, Fowles, Simmonds, 2014, 145–155).

For centuries, states have tried to justify armed interventions on humanistic grounds, such as defending human rights and protecting minorities. In the past, interventions that have been brought to the agenda due to justified war have turned into humanitarian interventions. The common point of all interventions is the idea of imposing respect for the principles of humanity (Bouchet-Saulnier, 2002). Just being human is enough reason to help others. It is not humane to be interested in the problems of others (Grotius, 2011). Although there is no definition of humanitarian intervention supported by a large number of people, it can be expressed as a military operation in order to prevent harm to the people under threat. The concept of humanitarian intervention envisages to appeal to and encourage participation in international power under the auspices of the United Nations (UN) for the protection of the threatened peoples within their own country. Although humanitarian intervention appears to be a good-willed, noble, and must be done, it has the potential to cause dangerous consequences when considering international policies and interests. The desire to do humanitarian intervention for humanitarian purposes, when the use of force is legitimate, may force some states to consider this as an opportunity. In general, the United Nations Security Council has the authority to grant military intervention in international law for humanitarian purposes (UNSC). One of the main challenges of humanitarian intervention is the use of force without self-defense or the decision of the Security Council in the article 2/4 of the UN Treaty. Although there is no clearly defined agreement with legal binding that justifies human intervention, it has become an international convention (Himes, Kenneth, 1994, 82-105). It considers it legitimate for a state to apply to power to protect its citizens from the ruthless and intense behavior of its own citizens. Despite all the criticism, it is accepted that the humanitarian intervention would be better rather than doing anything against the violations. Although the main objective of the participating states is not humanitarian concerns, the results of the masses may be of benefit. However, the existence of a systematic systematic discrimination. In humanitarian intervention practices reduces the attraction of the intervention. It is difficult to find intervention on humanitarian grounds in history (Chomsky, 2001). The phenomenon of humanitarian intervention has been used as an excuse to invade the weak countries in the past and nowadays. At the end of the interventions, the emergence of human consequences is not enough to hide the main purpose. In this context humanitarian actions in cyberspace arise or at least should arise from maintaining ethical standards of network users. Building ethical standards for cyberspace is an important task that requires reflection. Nevertheless, it can be said that they do not differ significantly from the ethical norms used in the real world. (Sitek B., 2018, 83).

Since 2009 the UN Internet Governance Forum (IGF) committed to making human rights and principles work for the online environment and to outline how human rights standards should be interpreted to apply to the Internet environment, and the Internet policy principles which must be upheld in order to create an environment which supports human rights to the maximum extent possible. They have developed a system of rules in force in the network and relating to human rights (internetrightsandprinciple).

1. The principle of universality and equality: Everyone comes to the world as a free being. The dignity that he possesses entitles him to equal access to rights that must be respected, protected and carried out on the web.
2. Principle of the rule of law and social justice: The Internet is a space where people's rights are propagated, protected and implemented. Social justice also applies online. Every Internet user is obliged to respect the rights of other users.
3. The principle of availability: Everyone has equal access to a safe and uncensored Internet.
4. The principle of freedom of speech and association: Each user has the right to search, download and publish information. This information may not be subject to censoring or other similar restrictions. In addition, everyone has the right to associate and identify via Internet with specific groups of a political, social or cultural nature.
5. The right to privacy and data protection: Every Internet user has the right to privacy on the Internet. Firstly, this means that no one has the right to monitor his activity on the Internet, secondly, it means the right to encrypt information and thirdly – the right to remain anonymous on the web.
6. The right to life, freedom and security: The right to life, freedom and security must be respected, protected and carried out on the Internet. No one has the right to violate these laws or use them to violate other human rights on the Internet.
7. The principle of diversity: The network should promote linguistic and cultural diversity as well as new technical and strategic solutions. The Internet should be a development environment for various ideas and views.
8. The principle of access to information: Each user has equal access to information that can not be filtered, data flow control systems, or discrimination for political, economic or other reasons.
9. The principle of standardization and regulation: Internet infrastructure, communication systems as well as data format should be based on standards that ensure interoperability of networks and services, and equal publishing and access to information.

10. The principle of managing network resources: Human rights and social justice must constitute a legal and normative basis for the functioning of the Internet and the management of its resources. The network, in a transparent way, should be managed by many different entities – respecting the principles of openness, pluralism and responsibility.

So far, not all of these principles have been codified and included in the generally applicable laws, and not only to the *soft law*.

It is worth mentioning here the activities of the United Nations in the extremely sensitive area mentioned earlier, namely the protection of children against violence in cyberspace. It is important to protect children from their birth untill they become adolescent (fort he definition of a child see: Rzewuski, 2007, 186-191). UN is engaged in building standards through appropriate legal regulations; on the other hand, for the abused child or potential juvenile cyber victim, it is important for the relevant services to implement the set standards. Therefore, the work "at the base" and education of individual social groups should be appreciated – both children, their parents and judges adjudicating in cases of cybercrime, police officers, teachers, etc. In addition to all penalizing, prosecuting and sanctioning activities, intensive educational campaigns are necessary. A proper campaign can really contribute to the greater safety of the children. Only a child who is aware of the threat will be able to defend himself against threat and the responsible parent will support his child and go to the appropriate services that will respond quickly and effectively to the actual threat (Pawlak, 2017, 102). As the Author suggests, protection at the universal level is important, but not sufficient, because the instruments used are non-binding.

The right to privacy in cyberprace

The right to privacy can be both negatively and positively defined. The negative right to privacy entails that individuals are protected from unwanted intrusion by both the state and private actors into their private life, especially features that define their personal identity such as sexuality, religion, and political affiliation, ie. the inner core of a person's private life. The positive right to privacy entails an obligation of states to remove obstacles for an autonomous shaping of individual identities (Jonsson, Cornell). Both definitions are important for understanding the right to privacy in cyberspace.

Progress in the field of dataveillance, technical means of controlling personal data, identifying and organizing knowledge about individuals has resulted in transferring the subject of anonymity to the political sphere, on the one hand, through the management of data bases on the other, through the formulation of postulates such as "the right to anonymity" or "protection of privacy" through political actions (Mazurek, 2006, 1-8).

Legal framework

The first mention of the right to privacy is contained in the Universal Declaration of Human Rights (1948) in the article 12:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

Similar provisions are embedded in other international legal acts. The right is enshrined in Articles 14 and 17 of the International Covenant on Civil and Political Rights. (1966) It is contained in Articles 16 and 40 in the Convention on the Rights of the Child (1989), article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (2004) and The Convention on the Rights of Persons with Disabilities (2006) in Article 22.

The problem of right to privacy in cyberspace, however, was legally recognized much later.

In December 2013, the United Nations General Assembly adopted resolution 68/167 "The right to privacy in the digital age", which communicated profound concern at the negative effect that surveillance and interception of communications may have on human rights.

The General Assembly affirmed that the rights held by people offline should be likewise ensured on the web, and it called upon all States to regard and secure the directly to protection in computerized correspondence. The

General Assembly called on all States to review their systems, practices and legislation related to communications surveillance, interception and gathering of individual information and stressed the requirement for States to ensure the full and effective implementation of their obligations under international human rights law.

In the European legislation there are two acts that the importance in the area of right to privacy in cyberspace. The first one was approved and announced in 2009: Directive 2009/136/ec of the European Parliament and of the council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ L 337, 18.12.2009) . The second one that has major effects from May 2018 in Europe is: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016).

The preamble of this act states:

> *"(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.*
>
> *(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data."*

The protection of rights is crucial as our life goes more to cyberspace in XXI century, but the level of protection is not sufficient. It can be seen that the protection of human rights in cyberspace, just like in the case of real reality, is more effectively implemented in the European system than at the universal level, due to the binding nature of legal acts. As Such-Pyrgiel points out, “The challenge for Europe is to create a technology that complies with the laws and principles of ethics.”

However, there are still groups more sensitive that need both: special protection and education. In addition to controlling or monitoring content posted in cyberspace, a wide-ranging educational campaign is needed. It cannot be only a one-time action, but it must be complex both in terms of content and form. Freedom offered by the Internet, must give rise to reflection that this freedom should not be abused in various areas. Normative or technical measures are not enough. Therefore, permanent education on the use of cyberspace will be a necessary as a complementary element. Its preparation will take a lot of time and effort. However, it seems that without this education it will not be possible to ensure security in cyberspace (Sitek, Such-Pyrgiel, 2018, 212).

References

Billo, C., ve Chang, W. (2004). Cyber Warfare Analysis of the Means and Motivations of Selected Nation States, Hanover: Institute for Security Technology Studies at Dartmouth College, Kasım.

Bouchet-Saulnier, F. (2002). İnsancıl Hukuk Sözlüğü.(Çeviren: Selahattin Bağdatlı). İstanbul: İletişim Yayınları. ISBN 9789750500978.

Boulton, M. J., Hardcastle K., Down J., Fowles J. & Simmonds J. A. (2014). A comparison of preservice teachers’ responses to cyber versus traditional bullying scenarios: Similarities and differences and ımplications for practice. Journal of Teacher Education, 65 (2), 145 – 155. ISSN 0022-4871.

Chomsky, Noam (2001). Amerikan Müdahaleciliği. (Çevirenler: Taylan Doğan Barış Zeren). İstanbul: Aram Yayıncılık

Grotius, Hugo (2011). Savaş ve Barış Hukuku. (Çeviren: Seha L. Meray). İstanbul: Say Yayınları. ISBN 9786050200607.

Domański Z. (2013) Zagrożenia w cyberprzestrzeni [in:] Such-Pyrgiel M. (ed.) Bezpieczeństwo społeczne w XXI wieku w ujęciu socjologicznym, pedagogicznym, prawnym i nauk o zarządzaniu, Józefów, 83. ISBN 9788362753376.

Himes, Kenneth R. (1994). The Morality of Humanitarian Intervention, Theological Studies, Vol.55, No.1, s.82-105. ISSN 0040-5639.

http://internetrightsandprinciples.org/site/[access:10.02.2019].

Jonsson R., Cornell A., Right to Privacy [in:} Oxford Constitutional Law, available: http://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156 [access:10.02.2019].

Klimburg, A. (2012). National cyber security framework manual. NATO CCD COE.

Mazurek P. (2006) Anatomia internetowej anonimowości [in:] w: D. Batorski, M. Marody, A. Nowak (red.) Społeczna przestrzeń internetu, Warszawa, SWPS, 1-8. 8389281244.

Pawlak A. (2017) Ochrona dzieci przed cyberprzestępczością w systemie Organizacji Narodów Zjednoczonych [in:] Ura E., Sitek B., Graca T. (red.) Potrzeby jako współczesny determinant treści praw człowieka, Józefów, WSGE, 89-103. ISBN 9788362753864.

Rzewuski M (2007) Definicja dziecka w Polsce. Uwagi de lege lata i de lege ferenda" Rejent 2007, nr 4, ISSN: 1230-669X, s. 186-191.

Sitek B. (2018) Zasady etyczne stosowane w cyberprzestrzeni [in:] Sitek B., Knap P., Sagan S., Roman Ł. (red.) Nowoczesne narzędzia informatyczne w przeciwdziałaniu zagrożeniom bezpieczeństwa, WSGE, 71-84. ISBN 9788362753789.

Sitek M., Such-Pyrgiel M. (2018). Wpływ cyberkultury na prawa człowieka. Journal of Modern Science, 39(4), 201-215. https://doi.org/10.13166/jms/101510. ISSN 1734-2031.

Such-Pyrgiel M. (2019) Człowiek w dobie cyfrowej transformacji, Toruń, 196. ISBN 9788366220966.

Zawisza J. (2015) Cyberprzestrzeń jako zagrożenie bezpieczeństwa państwa, Journal of Modern Science, 2015/4/27, 403-416. ISSN 1734-2031.