Joanna Grubicka, Ph.D
Pomeranian Academy in Slupsk
Faculty Social Cybernetics and Security Engineering

RESTRICTING FREEDOM ON THE INTERNET IN A PUBLIC SECURITY SPACE

Abstract

The Internet is basically an egalitarian tool of communication, the space of easy creation and transfer of content, for which the only limit is technology and unlimited human imagination. Freedom seems to be not only immanent but even constitutive feature of virtual space, in which the Internet functions. In the era of common access to freedom in the Internet there are more and more controversies between advocates of complete freedom and followers of the idea of limiting the usage of global network's resources. Should Internet become the space of unlimited freedom? Contrary to common belief the answer to such a question is not that obvious, although intuitively one would like to say yes.

Key words: virtual reality, cyberspace, digital revolution, digital freedom

Introduction

The Internet is a relatively new medium used to communicate, express one's thoughts, transfer ideas, views, but the easiness of dissemination of the information gives the possibility to abuse, enters the sphere of freedom of other people. Until recently it seemed that global network was the area not regulated and limited by no rules whatsoever. This situation is changing slowly and legislators as well as courts have started to draw the lines concerning behavior in the net. People uploading information in the Internet must follow minimum of security so as not to violate the freedom of speech, particularly in terms of widely understood public security, crime, morality, public order, personal property of others as well as secret and confidential information.

Freedom of global network is perceived not only in terms of unlimited possibility of using its resources or expressing oneself and one's own views (with the exception for the particular rules in regulation codes for specific services, e.g. portals or criminal law rules) but most importantly in the lack of the centre which could be a subject/institution of its supervision and control. The discussed attribute is also mentioned as one of specific qualities of cyberspace. The others are : fluency, virtuality, unpredictability, alternation (in its program and information layer), interaction, lack of possibility of drawing the limits, common accessibility or versatility. The concept of freedom has many meanings and is not understood in the same way in a number of contexts and in relation to various spheres of life.

The Internet is the first global medium whose users are not only recipients but also creators of its content. In this context it is justified to analyze the issue of freedom not only in the sense of recipient's freedom but also- if not first of all- the freedom of broadcaster's in terms of the content. If everyone has the right to exist in the network does it mean that he can freely put there whatever he feels like? We might be prone to say yes at first sight but even superficial reflection raises doubts concerning such a radical opinion. Freedom is undoubtedly a positive value, one of the most important ones, even the one constituting human existence but is it the absolute value? The practice of everyday life shows that there is no way to answer the question positively . There is a question who and on what basis should limit the freedom in the Internet? The freedom of a person living in a community is subject to many limits, resulting from norms of living together to name but a few. Although the borders of social norms are not stiff and- especially these days- are shifted in a number of ways, most often in the name of broadening the area of freedom of an individual, the very existence of the norm is not questioned. Just the contrary- they are also essential and absolutely necessary values in every community's life, so they have a global dimension. To put it more simply-we deal with the situation of co-existence and interdependence

of two essential values: freedom of individual on the one hand and norms of social life on the other. It is from this perspective that we should look at the issue of freedom in the Internet.

Technological revolution has caused that modern world has become dual and simultaneous – real and virtual at the same time. Conditions and forms of those two spaces have created the environment in which technological community is being shaped and developed. The paradox of spatial global network implicates the necessity of deeper reflections in the area of idea of digital freedom in the safe space of security. Inconsistency of the idea of freedom is expressed in its two points that define it: from and to. In the aspect of virtual network- freedom to will manifest itself in both access to existing there legal information resources as well as freedom to use it in any way and express one's convictions and views. In turn- the from parameter should be determined by both freedom of limits to access the resources as well as The greatest controversies are connected with the philosophical concept of human freedom that is traditionally connected with the concept of free will. In the considerations on freedom there are two different concepts: independence from something, which is from the factors that limit the freedom of choice and freedom to do something that is understood as an activity based on learning and using the natural and social necessities. In both those meanings freedom is not an absolute concept and- as each sphere of human activity- is subjected to limits.

The ones connected with censorship and threats. Dynamism of development implicates not only positive changes but also new challenges and threats. The threats are of both types: those are the existing negative phenomena taken to the net from the real world as well as existence of new categories of dangerous behaviors and crimes.

General classification of digital threats is implicated by :

- human/user activity: purposeful (e.g. cyber criminals) as well as inexpedient (e.g. easygoing users),

- lack of direct connection with purposeful human activity (fallibility of systems, flaws in programming),
- natural environment (e.g. natural disaster that causes power failure),
- hybridity of events.

Division of threats in terms of attributes of information functioning in the digital environment will be the result of the aim's function, i.e. interference, theft, interception, damage, manipulation, taking over control, modification or destruction (of information and/or systems). The tools that are used to reach the mentioned aims are appropriately prepared, malicious programs- viruses or computer worms. Here one can mention:

- spyware- software whose aim is to spy its users, e.g registering the visited sites or passwords typed in the keyboard without their knowledge and then sending the information to the attacker;
- Trojan horses - software that misleads its user as pretending to be a useful or interesting application and at the same time possessing undesired, hidden functionality;
- Hoaxes - programs that display untrue information that there is a virus in the computer;
- logical bombs - dormant form of malicious software activated at the moment of meeting certain conditions (e.g. on a certain day);
- phishing - based on insidious gain of logins and passwords by pretending to be a trustworthy institution or person.

What the most mentioned forms of malicious software have in common is the necessity to interact and react on the side of the user (e.g. clicking the link), whereas their point and aim are infection of the system (device) and achieving its desired effect (e.g. theft of data).

It is important to notice that more and more often one uses the methods of attack that do not require specialist knowledge in the field of programming. Those

are digital forgeries and extortions that could be divided into the following subcategories:

- committed with the help of malicious programming,
- committed with the help of false announcements (e-mails),
- hybrid (false mails containing malicious programs or link to this kind of program).

The second and the third of the mentioned forms are based on preparing the e-mail in which the attacker pretends to be a certain institution or subject (e.g. post office operator or the Internet services provider) putting in its content the link to the website or an attachment with a file suggesting e.g. an invoice. In reality the attachment contains malicious program which infects user's device.

Threats of social character are connected first of all with harmful and illegal contents in the net and undertaking risky behaviors by users or dangerous contacts. They concern such phenomena as cyber violence, grooming, sexting, hating, child pornography, racist contents, encouraging to suicide and others.

The Internet facilitates interpersonal contacts, but the contacts in the net are connected with some kind of risk, especially in case of using it to make friends with people they do not know offline. It is worth mentioning that it is this kind of activity – online contact with people not known personally- that is declared by as many as 25% of young Internet users[1] and many admit personal meeting in the real world with previously unknown people that they met in the net. This group of dangerous contacts includes as well the phenomenon of inducing children based on starting the relation by the Internet between an adult and a minor (below 15) in order to induce and later abuse him/her. Inducing children in the Internet is the crime defined in art.200 of the Penal Code:

Art. 200a

[1] L. Kirwil, *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo-część 2. Częściowy raport z badań EU Kids online przeprowadzonych wśród dzieci 9-16 i ich rodziców*. Warszawa: Szkoła Wyższa Psychologii Społecznej., Warszawa, 2011, p.42 -44.

§ 1.*Whoever, in order to commit a crime defined in art. 197 § 3 p. 2 or art.200, as well as produce or record pornographic content by means of ICT makes contact with a minor under 15 aiming, by misleading him, at taking advantage of a mistake or incapability to truly understand the situation or by means of illegal threat to meet him shall be subject to the penalty of deprivation of liberty for up to 3 years.*

§ 2. Whoever by means of ICT makes o proposal to a minor under 15 years of age to sexual intercourse or makes him/her submit to another sexual act or to perform such an act or participation in production or recording pornographic content and aims at its realization shall be subject to fine ,the penalty of the deprivation of liberty for a term up to 2 years[2].

Dangerous contacts are also contacts aiming at involving a teenager into a number of sects, groups, communities and subcultures with e.g. radical views promoting aggressive behavior , behaviors e.g. self-mutilation, radical diet or using psycho-active substances. Such contacts are undertaken by people interested in gaining data and other confidential information that are later used for the sake of crime.

Making and maintaining potentially dangerous contacts with strangers is not the domain of only young people, but it is them who because of inexperience as well as lower competences (because of age) concerning the right assessment of the situation, understanding and predicting consequences of undertaken actions in contrast with openness, willingness to make friends and trust are more prone to serious consequences.

The Internet is the place to experiment, also with one's own identity and undertaking risky activities. What activities are undertaken by the Internet users? Those are among others: searching for information on drugs and other psychoactive substances or activities harmful for one's health or making

[2] 6 June 1997 Act. – The Penal Code, Journal of Laws. 1997 nr 88 poz. 553 with later changes

dangerous friends, including stranger adults who could have pedophiles tendencies or with individuals /groups persuading to risky activities or ones against the law. Risky behaviors are also: sexting (including camera sexting) – so the phenomenon of transferring contents (images/short films) that are of erotic character, mainly their own naked or half-naked photos by the means of the Internet or a mobile phone. Sexting can also take the form of sex-communication live, by the means of communicators using the camera in the device. The research shows that every fourth Polish teenager has received intimate photos, 7% of teenagers have sent such photos and about 30% of teenagers " know a person" who sends intimate photos.[3] What is more, teenagers abuse/misuse the Internet (13%)[4], gamble online and first of all do not protect their privacy since they share too much information about themselves and upload numerous photos with a wide group of recipients as well as accept random people to their group of friends. This " openness" can be the reason of electronic aggression and violent activities undertaken by other users. It is among others calling names, threatening, stalking, gossiping, humiliating somebody in the Internet by means of new technology. Experience connected with different forms of cyber violence i. e. editing and uploading ridiculing photos and films, publicity of victims' secrets, persistent, rude and malicious comments as well as purposeful ignoring of online activity of the victims have been confirmed by many young Internet users[5].

What is the future of the Internet? Modern technologies changing incredibly fast will cause that technical usage of the Internet will become even easier. It is possible that to work with a computer, as long as this expression will be adequate, it will be enough to communicate by voice. Surely, it will become

[3] Report *Ogólnopolskie badanie Nastolatki wobec Internetu realizowane przez Pedagogium WSNS we współpracy z Rzecznikiem Praw Dziecka oraz Naukową i Akademicką Siecią Komputerową, Warszawa, 2014*

[4] K. Makaruk, S. Wójcik, *EU NET ADB, Badanie nadużywania internetu przez młodzież w Polsce*, FDN, Warszawa, 2012

[5] Cf. *EU NET ADB Badanie nadużywania Internetu przez młodzież w Polsce*, Fundacja Dzieci Niczyje, Warszawa 2012 p. 7 , Ł. Wojtasik, *Przemoc rówieśnicza a media elektroniczne.* Dziecko Krzywdzone. Teoria, badania, praktyka, Nr 1 (26) 2009 p.2. J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży.* Kraków: Impuls, 2012, s.215 -219, *Raport Nastolatki 3.0.*, NASK, Warszawa 2016

even richer source of knowledge, information, entertainment and communication platform. This kind of perspective is quite realistic and can be quite close. One thing will not change – using the Internet is and will be the matter of responsibility, so the reflection on which materials are or are not worth using is and will be necessary.

The fundamental rights of information society include: easy access to global information infrastructure, the right to property, reliability of information and the right to protect privacy[6]. For modern countries the guarantee of those rights as well as their protection is a great challenge. National legislation norms concerning the Internet are limited to the territory. The immanent feature of the Internet is its global access that enables uploading in its resources any statements. Prevention of uploading in the net certain contents is becoming the problem of modern countries. One often draws attention to the fact that the Internet – although generally associated with the freedom of speech- can also become a tool of invigilation and control over the citizens. It gives different firms and institutions great possibilities of spying on their users, collecting information and preparing data about potential clients. Also, national institutions are more and more interested in what is happening in the net[7]. One can risk the statement that cyberspace increases the sphere of not only freedom but also control. Repressions towards defiant bloggers or blocking the access to undesired websites have become the practice notoriously used in some countries hostile to freedom in the net e.g. in China. Authoritarian countries can use the function of filtrating and monitoring the messages. There is a conviction that appropriate access to the Internet tools will guarantee greater freedom everywhere. However, the example of Chine proves something different. China, more than any other country, proves that common access to the Internet and at the same time maintaining the control

[6] Y. Benkler, , *Bogactwo sieci, Jak produkcja społeczna zmienia rynki i wolność*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, p. 476.
[7] M. Podgórski, *Wirtualne społeczności i ich mieszkańcy. Próba etnografii*, in: Kurczewski J. (ed), *Wielka sieć. E-seje z socjologii Internetu*, Warszawa, 2006 p. 105-106.

over its usage is possible.[8] The fundamental issue in this area is keeping the balance between security of the nation and communities, and the freedom of an individual and their rights to easy exchange of information. Human being when dealing with greater and greater technological development loses its alertness and trusts technology too much. It is particularly dangerous in case of protecting the information where its significant part is sent through the Internet.[9] In order to provide ICT security of the country one must define the areas of responsibility and the ways and forms of its interaction and particularly:

- protection of critical ICT infrastructure of the state against the dangers coming from the cyberspace;
- cooperation in the area of prevention and fighting forms of computer crime;
- supporting the projects defining culprits of cyber terrorism;
- sharing essential information concerning serious ICT threats identified in own systems and ICT networks and other important facts to the protection of critical ICT infrastructure of the country;
- undertaking activities that increase social awareness in the category of cyberspace security.

Taking into consideration the fact of real threats of virtual net as well as greater and greater real losses connected with their consequences for over two decades various efforts have been undertaken aiming at normalization of the digital world- at the state, organization as well as widely understood international level. The fact that in its present shape there is no way to come back to the times of the beginnings of the network is out of the question as back then it was the place of only a concept and it was used mainly to exchange the thoughts of the users, making the dream about global communication come true. Today it is the

[8] Benkler, Y., *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność*, Warszawa, 2008, p. 159.
[9] J. Grubicka, *Konwergencja technologiczna a system bezpieczeństwa informacji*, W. Filipkowski (ed.) *Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use*. EIBW, Gdynia 2015, p. 86-99.

structure functioning in every area and sphere- both state one and a private one. The point is the challenge of finding the balance between maintaining the freedom of the net and its security- at each of mentioned above levels and in each area. The best example of undertaken activities in this area are particularly: Cyber Security Strategy of the EU: an Open, Safe and Secure Cyberspace, Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union or- in the international space- American International Strategy for Cyberspace. What the undertaken activities have in common is its clearly defined aim: maintaining and development of security of the net along with providing the freedom of the Internet- understood generally as development of the society based on the protection of its basic rights and freedom (particularly freedom of speech) and simultaneously effective protection of data and privacy and securing easy flow of information, among others prevention of censorship. Paraphrasing the words of A. de Tocqueville one can state that the freedom of the net finishes where its security starts. It is not possible to provide security without interference into its internal structure and the way of functioning of a given sphere. At the same time it is not possible to provide its freedom without its protection, which in case of digital world, because of its peculiar character (also from *stricte* technical point of view) would lead in consequence either to anarchy or to overtaking the control by the stronger ones.

Freedom understood in that way is becoming threatened by activities of different kinds which would let the providers of the Internet services establish various conditions of access for its users with the right to introduce additional fees for so called special services included. The challenge now are regulations from the area *post mortem*, because it depends only on the knowledge and previous usage of users whether their descendants will be able not only to inherit digital assets but also whether they will have the possibility to finish issues in the digital world such as: using the services ,deleting accounts. The issues of this kind,

although sensitive, remain significantly essential: these days most of such trivial things as bills are dealt with by the means of the network (information on the e-mail, using on-line banking etc.). So far we have been able to draw the conclusion that since cyberspace possesses its certain layers the paradigm of freedom in the net will manifest itself there. At the information level it will concern: open, equal and unlimited access to its resources to all its users. This issue is also vital in the context of so called free software, whose idea as well as its realization assume the possibility of activating, copying, disseminating, analyzing as well as its change and correction by its users. According to the definition of free software published by Free Software Foundation[10] the user is granted the following freedoms, which at the same time constitute basic assumptions of free software :

- Freedom 0: activating the program for any reason,
- Freedom 1: analyzing the program and adjusting it to one's needs;
- Freedom 2: disseminating of program's copies;
- Freedom 3: improving the program and public dissemination of one's own improvements, thanks to which the whole community can use it.

Freedoms 1 and 3 are possible only when the source code of programming is accessible[11].

The mentioned assumptions let for better understanding of the context of using the network services such as *Software as a Service* (Saas), whose point is to offer certain services or programs by a provider operating on his devices. In practice it means that the user uses the tools/ programs offered by a provider by means of a search engine so there is no need to install separate software on one's own device, e.g. set of Google application in order to use their functionality fully. Despite the comfort of using this kind of services, as it was directly stated by Richard M. Stallman : *We have no control, when using this service in the net we deprive ourselves of freedom. And it is both in terms of data we provide their*

[10] *What is free software?*, http://www.fsf.org/ [access: 9.11.2017].
[11] *Wolne oprogramowanie, Wikipedia*, https://pl.wikipedia.org/wiki/Wolne_oprogramowanie [access: 9.11.2017]

providers with as well as its freedom which is given the truly free software given to its users[12]. Apart from lack of control over data it is also the provider who decides about the way and scope of using it by users of the accessible software since *de facto* what is used is provider's computer.

There is no way to discuss freedom of network only in its commonly known form since it has its linear layer called Deep Web. Other names connected with this definition are Dark Net/Dark Web. Dark Web means websites that hide IP addresses of servers they use, which for example causes that it is not possible to find such websites by means of standard search engines. The most often used coding tool that allows to hide identity (of addresses as well as end users) is the Onion Router (TOR)[13]. Despite controversies which such type of tools raise, especially in terms of illegal content or criminal activity, solutions giving the opportunity of anonymisation of activity are used also by legal (ordinary) users who do not want to be followed by the tools used by providers of digital services, e.g. search engines. The classic example of possibility to follow the activity of its users are so called cookies, which basically should only support the activities of the application itself. Following the searched content, visited websites, downloaded files or bought products allow for so called profiling of the users (interests, habits or even place of living).

In classical, wider meaning security is defined as the condition free of threats. In the context of ICT security it is the state free of threats such as: sabotage, spying, diversion as well as transferring information to unauthorized subjects.

The definition includes also any activity that is used to secure ICT resources – generated, collected, processed, stored and transferred in communication networks as well as information carriers (computers, servers,

[12] *Richard M. Stallman odwiedził Polskę. Król hakerów twierdzi, że w Sieci pozbawiamy się wolności*, http://gadzetomania.pl/3758,richard-m-stallman-odwiedzil-polske-krol-hakerow-twierdzi-ze-w-sieci-pozbawiamy-sie-wolnosci [access: 11.09.2017].

[13] Apart from TOR one can also use e.g. *web proxy* to hide IP address

data), and particularly systems of methods of security. Security of resources - in the technical meaning- are defined by two models of management: restrictive (what is not allowed is forbidden) and liberal (what is not forbidden is allowed). Mentioned before documents of strategic and normative character assume establishing certain spheres of responsibility for security of the network itself and at the same time data that functions there, which is the Internet, intranet, extranet etc. as well as for specific elements and areas. As an example we can take imposed by NIS Directive [14] certain obligations in the area of security on operators of key services i.e. critical sectors such as private or public finances, power engineering, transport, healthcare and providers of digital services (online search engine, online marketplace, cloud computing service). In the first area there are subjects which- according to art. 5 of the Directive- meet together the following premises:

- provide service that is of key importance to maintain critical social or economic activity;
- providing the service depends on the network and ICT systems - the incident would have an important consequence disturbing provision of the service.

Additionally, each of the EU member countries is obliged to accept national strategy in terms of network and ICT systems security that would define strategic goals as well as suitable measures and regulations aiming at achieving and maintaining high level of network and ICT systems security as well as embracing the minimum defined in the Directive sectors and services. Besides, they have defined the issues which national strategies necessarily must take into consideration in terms of network and ICT systems security, namely:

- priorities and aims of network and ICT systems security ;
- frameworks of management used to realization of the accepted goals - including roles and range;

[14] Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, *op.cit.*

- obligations of organs and governmental institutions as well as other appropriate subjects (each of the countries was obliged to appoint organ or organs to protect cyber security);
- measures in terms of readiness, reacting and returning its functioning in back to normal condition, also in terms of cooperation between public and private sectors;
- in terms of accepted national strategies guidelines for educational, informative and workshop programs as well as guidelines for research-development plans;
- plans of risk assessment used to define it;
- list of subjects involved in implementation of the strategy[15].

In the area of international cooperation NIS Directive in art. 13 describes possibility of making international agreements "in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data."[16] In reference to global access of network regulation in article 18 p.2 Jurisdiction and territoriality is of great importance as well. It states that a digital service provider that is not established in the Union, but offers services within:

- Online marketplace;
- Online search engine;
- Cloud computing service

Shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered.

In terms of jurisdiction it means that a digital service provider is subjected to the jurisdiction of the member country, in which the representative has its organizational unit.

[15] Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, op.cit.
[16] Ibidem.

We should also mention the issue of the network existence understood here as a global medium and the environment of functioning of digital society: its axe, central point as well as the reference point is and will be a user, yet in spite of his key role not much place and attention is paid to him in documents which seem to emphasize all the mentioned before layers in cyberspace. The said responsibility, but first of all awareness of mechanisms and digital threats of the user would undoubtedly contribute to faster and more complete achievement of goals set in this area.

Summary. While taking advantage of benefits of freedom of speech, the right to possess own views and properties, the right to respect personal dignity one must not forget that the same rights are granted to others as well and so any activities of an individual cannot limit and violate rights of other people. There are no reasons why the norms of behavior in reality would not be applied to the same extent to virtual reality in the Internet. After all it is only a tool and although undoubtedly it has influenced our social life it is a human being who is its creator, not a creation. Disseminating in the Internet contents that are legally forbidden (pedophilia, persuading to crime, promoting fascism or communism, preparing actions of terroristic character) is and should be penalized. Portals' administrators on which such contents are uploaded must have an absolute right and even obligation to delete it. Separate but incredibly essential issue is common lack of responsibility for word, especially in anonymous rude "posts" purposefully addressed at a person's dignity, good name of a social group or the organization it refers to. It seems that it would not be a violation of freedom of speech if one could successfully implement the rule that posts and comments in the Internet cannot function anonymously, that a technical condition of uploading the content in the Internet is registration and giving one's personal data (in a form hidden to an ordinary recipient). Generally speaking there should be one rule- as much freedom as responsibility. The limits should always be individualized, referring to a specific person or a group of people undertaking actions that are in conflict

with the social norms. Under no circumstances can those limits be implemented by means of administrative decisions of authorities and referring to the society. Such forms of actions are symptoms of totalitarianism and can never be justified. Surely, it will take a long time before we work out consensual common vision of secure and at the same time free digital space.

Literature

1. Benkler, Y., *Bogactwo sieci, Jak produkcja społeczna zmienia rynki i wolność*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.
2. Grubicka J., Motyka R., *Człowiek jako ważne ogniwo zapewnienia bezpieczeństwa informatycznego jednostce administracyjnej*, Bezpieczeństwo w administracji i biznesie we współczesnym świecie part. II, Gdynia 2011.
3. Grubicka J., *Konwergencja technologiczna a system bezpieczeństwa informacji*, W. Filipkowski (ed.) *Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use*. EIBW, Gdynia 2015.
4. Kirwil L., *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo-część 2. Częściowy raport z badań EU Kids online przeprowadzonych wśród dzieci 9-16 i ich rodziców*, Warszawa: Szkoła Wyższa Psychologii Społecznej, Warszawa, 2011.
5. Kulesza J., , *Ius internet. Między prawem a etyką*, Warszawa 2012.
6. Makaruk K., Wójcik S., *EU NET ADB, Badanie nadużywania internetu przez młodzież w Polsce*, FDN, Warszawa 2012.
7. Pyżalski J., *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży.* Kraków: Impuls, 2012.
8. Podgórski M., *Wirtualne społeczności i ich mieszkańcy. Próba etnografii*, w: Kurczewski J. (ed), *Wielka sieć. E-seje z socjologii Internetu*, Warszawa, 2006.