Borders of Digital Network Freedom in Public Security Space

Tadeusz Szczurek
ORCID: 0000-0002-3433-8072
Military University of Technology in Warsaw, Poland

Joanna Grubicka
ORCID: 0000-0001-7934-6044
Pomeranian Academy in Słupsk, Poland

Dorota Zbroszczyk
ORCID: 0000-0002-5777-4934
University of Technology and Humanities in Radom, Poland

Abstract. *In the era of common access to freedom on the Internet, there are more and more controversies between advocates of complete freedom and followers of the idea of limiting the usage of the global network's resources. Should the Internet become a 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. The Internet is basically an egalitarian tool of communication, a 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 an immanent, but even a constitutive feature of the virtual space in which the Internet functions.*

DOI: 10.5604/01.3001.0014.3198
http://dx.doi.org/10.5604/01.3001.0014.3198

Keywords: virtual reality, cyberspace, digital revolution, digital freedom

Introduction

The digital revolution has brought about the fulfillment of daring visions concerning the possibility of distant communication as well as the creation of virtual reality. Tim Berners-Lee's breakthrough invention of the World Wide Web standard (1991) and the basics of HTML created a global network that is a digital concept of equality and freedom both in terms of access as well as the possibility of using the sources. The beginning of the Internet in its present form dates back to the 1970s, whereas The WELL™ is considered to be the first virtual community/social movement. It is described as 'the place which is situated a few keys away, regardless of where you are'. It is assumed that The WELL™ defined the present shape of the net, when at its beginnings, only 1% of the Earth's population had global access to it[1].

Stewart Brand, creator of the WELL™ says, 'We wanted to create the space in which we could fulfil our ideas, experiment. We had neither money nor influence but we were aware of the chance that we had just then. (…) Everyone could say whatever they wanted there.' 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

[1] Virtual resolution, BBC documentary, 2010.

concepts: independence from something, which is from the factors that limit the freedom of choice, and the freedom to do something that is understood as an activity based on learning and using the natural and social necessities. In both of those meanings, freedom is not an absolute concept and — as with each sphere of human activity— is subjected to limits[2].

The Internet is a relatively new medium used to communicate, express one's thoughts, and transfer ideas and views, but the ease of dissemination of information creates the possibility to abuse, and enters the sphere of freedom of other people. Until recently, it seemed that the global network was an area not regulated or limited by any rules whatsoever. This situation is changing slowly, and legislators as well as courts have started to draw lines concerning behaviour on the net. People uploading information on the Internet must follow a 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.

The boundaries of digital freedom and safety

Freedom on the global network is perceived not only in terms of unlimited possibilities of using its resources or expressing oneself and one's own views (with the exception for the particular rules in the Terms of Service for specific services, e.g. portals, or criminal law rules) but most importantly in the lack of a centre which could be a subject/institution of its supervision and control. The discussed attribute is also mentioned as one of the specific qualities of cyberspace. The others are; fluency, virtuality, unpredictability, alternation (in its program and information layers), interaction, limitlessness, common accessibility, and 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 consumers, but also creators of its content. In this context, it is justified to analyse the issue of freedom not only in the sense of the recipient's freedom, but also — if not first of all — the freedom of broadcasters in terms of the content. If everyone has the right to exist on the network, does it mean that they can freely put there whatever they feel 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 an absolute value? The practice of everyday life shows that there is no way to answer the question positively. There is the question of who and on what basis should they limit freedom on the Internet? The freedom of a person living in a community is subject to many limits, resulting from the 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

[2] Szczurek T, Dylematy wynikające z aktywności państwa w obszarze bezpieczeństwa, [in:] Pawłowski J (Ed.), Współczesny wymiar bezpieczeństwa. Między teorią a praktyką. Warsaw, 2011, pp. 135–145.

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 life, so they have a global dimension. To put it more simply, we are dealing with the situation of co-existence, and the interdependence of two essential values: freedom of the 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 on the Internet.

The technological revolution has made the modern world become dual and simultaneous — real and virtual at the same time. The conditions and forms of those two spaces have created an environment in which a technological community is being shaped and developed. The paradox of a spatial global network implicates the necessity of deeper reflections in the area of the idea of digital freedom in the safe space of security. The inconsistency of the idea of freedom is expressed in its two points that define it: 'from' and 'to'. With respect to a virtual network — freedom will manifest itself in both access to the legal information resources which exist there, as well as the 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 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 the existence of new categories of dangerous behaviours and crimes. The 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.

The division of threats in terms of attributes of information functioning in the digital environment will be the result of the goal'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 achieve the mentioned goalss are appropriately prepared, malicious programs — viruses or computer worms. Here, one can mention:

- Spyware — software whose aim is to spy on its users, e.g registering the visited sites or passwords typed into 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 when certain conditions are met (e.g. on a certain day);
- Phishing — based on the insidious acquisition 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 goal 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, methods of attack that do not require specialist knowledge in the field of programming are being used, such as 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 a link to this kind of program).

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

Threats of a social character are connected first of all with harmful and illegal content on the net, and undertaking risky behaviours by users or dangerous contacts. They concern such phenomena as cyber violence, grooming, sexting, hating, child pornography, racist content, encouraging others to commit suicide, and others. It is also worth mentioning here the threats called directed attacks, or APTs (*Advanced Persistent Threats*), which connect different types of programming or socio-technical tools. Preparations for such kinds of attacks can take a number of weeks, and are usually conducted by organised groups that have at their disposal significant financial sources as well as the time necessary to infiltrate the specific target (organisation, institution, firm) and then conduct its precise action.

The open resources of the Internet make access to various information easy, including illegal content as well as content that is not illegal in the light of the law, but belongs to the category of harmful. Harmful content is that which can evoke negative emotions in a recipient, and which can influence their emotional and social sphere as well as behaviour. There is content, among others, visualising violence, physical damage, graphic images, cruelty to animals, discrimination, pornographic, and calling for auto-destructive activities. The modern information carriers and attractive form, encourage youth to spend more time online stimulating the development of content by digital natives. They are limiting themselves though an addiction to new technologies, which are becoming necessary to their normal functioning. Prevention and ensuring of suitable level of safety should be referred to as preventing digital dangers[3]. Almost one fourth of Polish young Internet users have been in touch with 'content potentially threatening the social development of children, created by other users of the Internet'[4]. It is not only the

[3] Zbroszczyk D, Grubicka J, Bezpieczeństwo adolescenta wobec zagrożeń w cyberprzestrzeni, [in:] Jarmoch E, Trzpil I.A, Świdreski A.W (Eds), Bezpieczeństwo człowieka a miłosierdzie. Opieka i ochrona. Drohiczyn, 2017, pp. 219–220.

[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. Warsaw: Szkoła Wyższa Psychologii Społecznej, 2011, pp. 42–44.

mischievousness of the content that can have an influence on the human development. It is its attractiveness as well, paradoxical as it may sound. Interestingly, the attractive content and applications with which the users cope with on the net may cause a loss of control over time and intensity of using the Internet, computer, computer games, social networking sites, and other virtual activities. It can have an impact on limiting or resignation from other activities of everyday life as well as lead to neglecting family, duties, school, or a hobby, and/or avoiding contacts with their peers. Research on Polish teenagers showed that they spent more time on the net that they initially planned (83.3%), and more than half experienced irritation when the Internet stopped working or they had no access to it (64.2%). Additionally, in order to use the Internet, every fifth teenager gave up sleep, and every third from their duties (29.8%)[5].

The Internet facilitates interpersonal contacts, but the contacts on the net are connected with some kind of risk, especially in the 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[6], and many admit to personal meetings in the real world with previously unknown people that they met on the net. This group of dangerous contacts also includes the phenomenon of grooming children based on starting the relation by the Internet between an adult and a minor (below 15) in order to induce and later abuse them. Grooming children on the Internet is the crime defined in art.200a of the Penal Code: § 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 them, at taking advantage of a mistake or incapability to truly understand the situation or by means of illegal threat to meet them shall be subject to the penalty of deprivation of liberty for up to 3 years. § 2. Whoever by means of ICT makes a proposal to a minor under 15 years of age of sexual intercourse or makes them submit to another sexual act or to perform such an act or participate in the production or recording pornographic content and aims at its realisation shall be subject to fine, the penalty of deprivation of liberty for a term up to 2 years*[7].

Dangerous contacts are also contacts aimed at involving a teenager in a number of sects, groups, communities and subcultures with e.g. radical views promoting aggressive behaviour, behaviours such as self-mutilation, a radical diet, or using psychoactive substances. Such contacts are undertaken by people interested in gaining data and other confidential information that are later used for the purpose 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 their inexperience as well as their lower competences (because of their age) concerning the right assessment of the situation, understanding and predicting the consequences of their actions, in contrast with their openness, willingness to make friends and trust, are more prone to serious consequences.

[5] Raport Nastolatki 3.0. Warsaw, 2016.

[6] Kirwil L, pp. 42–44.

[7] 6 June 1997 Act. — The Penal Code, Journal of Laws. Dz.U. 1997, No. 88, item 553 as amended.

The Internet is a place to experiment, including with one's own identity, and to undertake risky activities. What activities are undertaken by Internet users? Among others: searching for information on drugs and other psychoactive substances, activities harmful for one's health, making dangerous friends, including stranger adults who could have paedophilic tendencies or with individuals/groups persuading them to engage in risky or illegal activities. Risky behaviours also include sexting (including camera sexting) — the phenomenon of transferring content (images/short films) that are of an erotic character, mainly their own naked or semi-naked photos by means of the Internet or a mobile phone. Sexting can also take the form of live sex-communication, by means of using the camera in the device. 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[8]. What is more, teenagers abuse/misuse the Internet (13%)[9], 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 cause of electronic aggression and violent activities undertaken by other users. It is among others calling names, threatening, stalking, gossiping, humiliating somebody on the Internet by means of new technology. Experience connected with different forms of cyber violence, i.e. editing and uploading ridiculing photos and films, publication 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[10].

What is the future of the Internet? Modern technologies changing incredibly fast will lead to technical usage of the Internet becoming even easier. It is possible that voice will be all that is required to work with a computer, as long as one's speech is adequate. Surely, it will become an even richer source of knowledge, information, entertainment, and communication. This kind of perspective is quite realistic and may be quite close, however 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 an information society include: easy access to global information infrastructure, the right to property, reliability of information, and the right to protect privacy[11]. For modern countries, the guarantee of these rights as well as their protection is a great challenge. National legislation norms concern-

[8] Raport Ogólnopolskie badanie — Nastolatki wobec Internetu realizowane przez Pedagogium WSNS we współpracy z Rzecznikiem Praw Dziecka oraz Naukową i Akademicką Siecią Komputerową. Warsaw, 2014.

[9] Makaruk K, Wójcik S, EU NET ADB, Badanie nadużywania Internetu przez młodzież w Polsce. Warsaw, 2012.

[10] Cf. EU NET ADB Badanie nadużywania Internetu przez młodzież w Polsce. Warsaw, 2012, p. 7; Wojtasik Ł, Przemoc rówieśnicza a media elektroniczne. Dziecko Krzywdzone. *Teoria, badania, praktyka,* 2009, No. 1, Issue 26, p. 2; Pyżalski J, Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży. Cracow, 2012, pp. 215–219; Raport Nastolatki 3.0. Warsaw, 2016.

[11] Benkler Y, Bogactwo sieci, Jak produkcja społeczna zmienia rynki i wolność. Warsaw, 2008, p. 476.

ing the Internet are limited to the territory. The immanent feature of the Internet is its global access which enables any statements to be uploaded to its resources. The prevention of certain content being uploaded onto the net is becoming a 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 surveillance and control over the citizens. It gives different firms and institutions great possibilities for spying on their users, collecting information, and preparing data about potential clients. Also, national institutions are becoming more and more interested in what is happening online[12]. One can risk the statement that cyberspace increases the sphere of not only freedom but also control. Repressions towards defiant bloggers, and blocking access to undesired websites have become a notoriously used practice in some countries hostile to freedom on the net, e.g. in China. Authoritarian countries can use the function of filtering and monitoring messages. There is a conviction that appropriate access to Internet tools will guarantee greater freedom everywhere. However, the example of China proves something different. China, more than any other country, proves that common access to the Internet while maintaining control over its use is possible[13]. The fundamental issue in this area is keeping a balance between the security of the nation and communities, and the freedom of an individual and their rights to easy exchange of information. A human being, when dealing with greater and greater technological development, becomes less alert and trusts technology too much. It is particularly dangerous in the case of the information which is primarily sent through the Internet.[14] In order to provide ICT security for 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 cyberspace;
- cooperation in the area of prevention and fighting forms of computer crime;
- supporting projects defining the culprits of cyber terrorism;
- sharing essential information concerning serious ICT threats identified in government 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 on the virtual net as well as greater and greater real losses connected with their consequences, various efforts have been undertaken for over two decades aiming at normalisation of the digital world — at the state, organisation as well as the broadly understood international level. The fact that, in its present shape, there is no way to go back to the times of the beginnings of the network, is out of the question, as back then, it was a place of only concept, and it was used mainly to exchange the thoughts of the

[12] Podgórski M, Wirtualne społeczności i ich mieszkańcy. Próba etnografii, [in:] Kurczewski J (Ed.), Wielka sieć. E-seje z socjologii Internetu. Warsaw, 2006, pp. 105–106.

[13] Benkler Y, p. 159.

[14] Grubicka J, Konwergencja technologiczna a system bezpieczeństwa informacji, [in:] Filipkowski W (Ed.), Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use. Gdynia, 2015, pp. 86–99.

users, making the dream of global communication come true. Today, it is a structure that functions in every area and sphere — both state and private. The point is about the challenge of finding a balance between maintaining the freedom of the net and its security — at each of the levels and in each area mentioned above. The best examples of activities undertaken in this area are particularly: the 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, and — in the international space — the American International Strategy for Cyberspace. What the undertaken activities have in common is their clearly defined goal: maintaining and developing security of the while providing the freedom of the Internet — understood generally as the development of society based on the protection of its basic rights and freedom (particularly the freedom of speech) and simultaneously effective protection of data and privacy, and securing the easy flow of information, and the prevention of censorship. Paraphrasing the words of A. de Tocqueville, one can state that the freedom of the Internet ends where its security starts. It is not possible to provide security without interfering with 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 the case of the digital world, because of its peculiar character (also from a *strict* technical point of view) would lead in consequence either to anarchy, or to the strongest actors taking control.

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 highly essential: these days, most such trivial things as bills are dealt with by the means of the network (information on 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 on the net will manifest itself there. At the information level, it will concern: open, equal and unlimited access to its resources for all of its users. This issue is also vital in the context of so-called free software, whose idea as well as its realisation assume the possibility of activating, copying, disseminating, analysing as well as its change and correction by its users. According to the definition of free software published by the Free Software Foundation[15], the user is granted the following freedoms, which at the same time constitute the basic assumptions of free software:

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

[15] What is free software? *Elecronic source*: http://www.fsf.org/, *accessed:* 9.11.2019.

Freedoms 1 and 3 are possible only when the source code is accessible[16].

These assumptions lead to a better understanding of the context of using network services such as *Software as a Service* (Saas), whose point is to offer certain services or programs by a provider operating on their devices. In practice, it means that the user uses the tools/programs offered by a provider by means of a browser, so there is no need to install separate software on one's own device, e.g. the set of Google applications, in order to use their functionality fully. Despite the comfort of using this kind of service, as was directly stated by Richard M. Stallman, *We have no control. When using this service on the net, we deprive ourselves of freedom. And it is both in terms of the data we provide their providers with as well as the freedom which truly free software gives to its users*[17]. Apart from lack of control over data, it is also the provider who decides about the method and scope of using it by users of the accessible software since, *de facto* what is used is the provider's computer.

There is no way to discuss the freedom of the network only in its commonly known form since it has another layer called the Deep Web. Other names connected with this definition are Dark Net and Dark Web. The Dark Web is a set of websites that hide the IP addresses of the servers they use, which for example results in it being impossible to find such websites by means of standard search engines. The most often used coding tool that allows the identity (of addresses as well as end users) to be hidden is the Onion Router (TOR)[18]. Despite controversies which such types of tools raise, especially in terms of illegal content or criminal activity, solutions providing 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. A classic example of the possibility to follow the activity of its users are so-called cookies, which in theory 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 the classical, wider meaning, security is defined as the condition of being free of threats. In the context of ICT security, it is the state of being free of threats such as: sabotage, spying, diversion as well as transferring information to unauthorised subjects.

The definition also includes 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, data), and particularly systems of methods of security. The security of resources — in the technical meaning — is defined by two models of management: restrictive (what is not allowed is forbidden) and liberal (what is not forbidden is allowed).

The abovementioned documents of a strategic and normative character assume establishing certain spheres of responsibility for the security of the network itself, and also the data that functions there, which is on the Internet, intranets, extranets etc., as well as for specific elements and areas. As an example, we can take certain

[16] Wolne oprogramowanie. Wikipedia. *Electronic source:* https://pl.wikipedia.org/wiki/Wolne_oprogramowanie, *accessed:* 9.11.2019.

[17] Richard M Stallman odwiedził Polskę. Król hakerów twierdzi, że w Sieci pozbawiamy się wolności. *Electronic source:* http://gadzetomania.pl/3758,richard-m-stallman-odwiedzil-polske-krol-hakerow-twierdzi-ze-w-sieci-pozbawiamy-sie-wolnosci, *accessed:* 11.09.2019.

[18] Apart from TOR, one can also use, e.g. a web proxy to hide their IP address.

obligations in the area of security imposed by the NIS Directive[19] on operators of key services, i.e. critical sectors such as private and public finances, power engineering, transport, healthcare, and providers of digital services (online search engines, online marketplaces, cloud computing services). In the first area, there are subjects which — according to art. 5 of the Directive — meet together the following premises:

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

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

- priorities and aims of network and ICT system security;
- frameworks of management used to realise the accepted goals — including roles and range;
- obligations of organs and governmental institutions as well as other appropriate subjects (each of the countries was obliged to appoint an organ or organs to protect cyber security);
- measures in terms of readiness, reacting and returning its functioning back to a 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 and development plans;
- plans of risk assessment used to define it;
- list of subjects involved in implementation of the strategy[20].

In the area of international cooperation, the NIS Directive in art. 13 describes the possibility of forming 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.'[21] In reference to network regulations for global access 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 the field of:

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

[19] 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.

[20] *Ibid.*

[21] *Ibid.*

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, this means that a digital service provider is subjected to the jurisdiction of the member country, in which the representative has its organisational unit.

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 axis, or central point as well as the reference point is and will be a user, yet in spite of their key role, not much attention is paid to them in the documents, which seem to emphasise all the abovementioned layers in cyberspace. The said responsibility, but first of all awareness of the mechanisms and digital threats of the user, would undoubtedly contribute to faster and more complete achievement of goals set in this area.

Conclusions

The most general and rather commonly accepted limit of one person's freedom is the freedom of another. While taking advantage of the benefits of freedom of speech, the right to possess one's own views and properties, and 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 or violate the rights of other people. There are no reasons why the norms of behaviour in reality should not be applied to the same extent to virtual reality on the Internet. After all, it is only a tool, and although it has undoubtedly influenced our social life, it is a human being who is its creator, not a creation. Disseminating content on the Internet that is legally forbidden (paedophilia, persuasions to commit crime, promoting fascism or communism, planning actions of a terroristic character) is and should be penalised. The administrators of portals on which such content is uploaded must have an absolute right and even obligation to delete it. A separate but incredibly essential issue is the common lack of responsibility for the written word, especially in anonymous rude 'posts' purposefully addressed at a person's dignity, the good name of a social group, or the organisation 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 on the Internet cannot function anonymously, that a technical condition of uploading content on 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 — freedom and responsibility in equal measure. The limits should always be individualised, 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 a consensual common vision of a secure and free digital space. The Internet makes it hard for authoritarian regimes to control the population. In the same way, unseen as yet openness and freedom of the networked environment calls for new methods of protection of open societies from individuals and groups working destructively. It is international cooperation that is the condition of efficient execution of limits.

References

1. Benkler Y, Bogactwo sieci, Jak produkcja społeczna zmienia rynki i wolność. Warsaw, 2008.
2. Grubicka J, Motyka R, Człowiek jako ważne ogniwo zapewnienia bezpieczeństwa informatycznego jednostce administracyjnej. Bezpieczeństwo w administracji i biznesie we współczesnym świecie. Część 2. Gdynia, 2011.
3. Grubicka J, Konwergencja technologiczna a system bezpieczeństwa informacji, [in:] Filipkowski W (Ed.), Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use. 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. Warsaw, 2011.
5. Kulesza J, Ius internet. Między prawem a etyką. Warsaw, 2012.
6. Makaruk K, Wójcik S, EU NET ADB, Badanie nadużywania Internetu przez młodzież w Polsce. Warsaw, 2012.
7. Pyżalski J, Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży. Cracow, 2012.
8. Podgórski M, Wirtualne społeczności i ich mieszkańcy. Próba etnografii, [in:] Kurczewski J (Ed.), Wielka sieć. E-seje z socjologii Internetu. Warsaw, 2006.
9. Szczurek T, Dylematy wynikające z aktywności państwa w obszarze bezpieczeństwa, [in:] Pawłowski J (Ed.), Współczesny wymiar bezpieczeństwa. Między teorią a praktyką. Warsaw, 2011.
10. Zbroszczyk D, Grubicka J, Bezpieczeństwo adolescenta wobec zagrożeń w cyberprzestrzeni, [in:] Jarmoch E, Trzpil I.A, Świdreski A.W (Eds), Bezpieczeństwo człowieka a miłosierdzie. Opieka i ochrona. Drohiczyn, 2017.

About the Authors

Tadeusz Szczurek*, Brigadier General, a doctor habilitated in the scientific discipline of 'Security Science'. He graduated from the Military University of Technology. He received his doctoral degree at the Maria Curie-Skłodowska University and a doctoral degree at the Faculty of National Security of the National Defense Academy. He is the author or editor of more than a dozen monographs and over sixty other publications in which he addresses issues related to crisis management, environmental protection and the use of technology in the implementation of security tasks. His special attention is focused on non-military and paramilitary threats. Currently, he is the Rector-Commander of the Military University of Technology in Warsaw. E-mail: tadeusz.szczurek@wat.edu.pl.*

Joanna Grubicka*, PhD, currently holding the position of the Head of Social Cybernetics in the Department of Social Cybernetics and Safety Engineering of Pomeranian University in Slupsk; a member of the Drohiczyn Scientific Society, Academic Education Society at Pomeranian University in Slupsk, Society of Security Studies in Siedlce, and Polish Information Processing Society. The author of scientific and popular science publications concerning the development of information society, online security and services, contemporary culture advancing on the foundation of digital technologies: the theory of media, communication, Internet and social media, cyberspace threats. The executive editor of the international periodical 'East Journal of Security Studies'. E-mail: joanna.grubicka@apsl.edu.pl.*

***Dorota Zbroszczyk**, PhD, court mediator, assistant professor in the Department of Pedagogy and Psychology of Kazimierz Pulaski University of Technology and Humanities in Radom, the author of several articles dealing with social pathologies, public and health security; the organiser of nationwide and international conferences, a member of Drohiczyn Scientific Society, European Association for Security, K. Bogdanski Transdisciplinary Research Centre for Security Problems of Siedlce University of Natural Sciences and Humanities, Polish Society of Security Studies, a member of international periodical 'East Journal of Security Studies', a secretary of the Polish Society of Social Policy in Radom. E-mail: d.zbroszczyk@wp.pl.*

***Streszczenie.** W dobie powszechnego dostępu wolności w Internecie narastają kontrowersje pomiędzy zwolennikami pełnej swobody, a stronnikami prawnego ograniczania korzystania z zasobów globalnej sieci. Czy zatem Internet powinien być przestrzenią nieograniczonej niczym wolności? Odpowiedź na tak postawione pytanie, wbrew pozorom, nie jest oczywista, choć intuicyjnie chciałoby się odpowiedzieć twierdząco. Internet jest bowiem z założenia egalitarnym narzędziem komunikacji, przestrzenią swobodnego tworzenia i przepływu treści, dla których ograniczeniem jest tylko technologia oraz ludzka wyobraźnia, której granic wyznaczyć nie sposób. Wolność zatem zdaje się być nie tylko immanentną, ale wręcz konstytutywną cechą tej wirtualnej przestrzeni, w której funkcjonuje Internet.*

***Zusammenfassung.** Im Zeitalter des universellen Zugangs zur Freiheit im Internet wächst die Kontroverse zwischen Befürwortern der vollen Freiheit und Parteien, die die Nutzung der globalen Netzwerkressourcen gesetzlich einschränken. Sollte das Internet ein Raum der unbegrenzten Freiheit sein? Entgegen dem Anschein ist die Antwort auf eine solche Frage nicht offensichtlich, obwohl man intuitiv gerne mit „Ja' antworten würde. Das Internet ist per Definition ein egalitäres Kommunikationsmittel, ein Raum der freien Schaffung und des freien Flusses von Inhalten, der nur durch die Technologie und die menschliche Vorstellungskraft begrenzt ist, deren Grenzen nicht definiert werden können. Daher scheint die Freiheit nicht nur ein immanentes, sondern sogar ein konstitutives Merkmal dieses virtuellen Raums zu sein, in dem das Internet funktioniert.*

***Резюме.** В эпоху всеобщего доступа к свободе в Интернете все чаще возникают разногласия между сторонниками полной свободы и теми, кто законодательно хочет ограничить использование глобальных сетевых ресурсов. Должен ли Интернет быть пространством безграничной свободы? Ответ на такой вопрос, на первый взгляд, не является очевидным, хотя интуитивно хотелось бы ответить «да». Сам Интернет по своей сути является эгалитарным инструментом коммуникации, пространством свободного творчества и потока информации, для который ограничением является только технология и человеческое мышление, границы которого не поддаются никакому установлению. Поэтому свобода кажется не только имманентной, но даже составной частью этого виртуального пространства, в котором существует Интернет.*