International Journal of Pedagogy Innovation and New Technologies

journal homepage: http://www.ijpint.com

ISSN: 2392-0092, Vol. 7, No. 1, 2020

Social area of the internet in the context of values and personal safety threats in cyberspace

Joanna Grubicka

CONTACT: *Joanna Grubicka, Ph.D., Assistant Professor, National Security Institute, Cyber Security Department, Pomeranian Academy in Slupsk, Słupsk, Poland, E-mail:* joanna.grubicka@apsl.edu.pl

Keywords:

virtual reality, cyberspace, virtual communities, digital freedom, personal security in cyberspace

Abstract:

The subject of the article directly fits into the process of broadly understood security. The author indicates the opportunities and threats in the social space of the Internet of human functioning. The aim of the article is to analyze the basic human threats while experiencing freedom and trust in the virtual space. The author poses the question: Should the Internet be a space of unlimited freedom? Freedom seems to be not only an immanent but also a constitutive feature of the virtual space in which the Internet functions. It should be emphasized that the issues are discussed from very different perspectives and in processes as well as social relations. The article consists of three parts. In the first one the author presented the issues of cyberspace development, whose specific features favor the development of the virtual community. Next, she defined the most important areas concerning the culture of freedom and the consent of human education as a way of promoting its independence in the social space of the Internet. The last part of the publication contains the most important theses regarding threats related to human personal safety in cyberspace.

1. Introduction

Contemporary man and all the areas of his existence undergo many transformations in the present reality. This situation is compounded by certain changes that are of global nature, among which the following can be mentioned: rapid development of information and knowledge, the emergence of the phenomenon of uncertainty and axiological chaos, widening the scope of mistrust and fear of various challenges and life dilemmas in the modern world, growing difficulties in people's adaptation to the new challenges of globalization, European integration and information society, as well as rapid development of rights and obligations, increased criticism of various phenomena and trends of civilization, changes and personality degradation of the individual (Banach, 2004, p. 79).

The complexity of the world can be analyzed in the context of cultural and civilization changes, which cannot be discussed here, still the analyzes carried out by Mead (2000) describing the process of development and socialization in various cultures, both primitive and contemporary, in the consistent aspect can bring down cultural transformations of the contemporary world to reversing the traditional principles of upbringing and socialization (the elders learn from the younger – pre-figurative culture).

The complex and changing living space of man is therefore determined by socio-cultural factors influencing the development and quality of self-creation, which is especially true of the younger generation. What is often noticed is the disturbing superficiality, briefness, shallowness and fragility of relations between people, which are based on maintaining contacts on the basis of temporality and randomness, and not the closeness of meetings "face to face".

The personal ties in the family, peer and local environment as constitutive of the human community give way to material (instrumental) ties, characteristic of community and purposeful interactions, where "commodity" is not the emotions and experiences of people, but a common interest, exchange of services and goods. Instrumental ties imply cooperation only if it serves to achieve some limited and direct goal (Marshall, 2008, p. 421).

The aftermath of globalization processes is the increasing socio-cultural unification projecting the course and character of the upbringing processes in the contemporary school. The school has largely lost its educational influence by becoming a merely educative institution. This is a highly disturbing phenomenon since education not supported by shaping character can turn against the individual. The richness of the offer and the multiplicity of patterns and environments that human beings encounter may contribute to the state of internal chaos. Hence the susceptibility of young people to various ideologies, beliefs, impact of subcultures, with which the school and the family simply cannot cope. Building a certain educational alternative in the form of coming back to nature and simple life, tradition, search for universal values, return to the roots, and involvement in social and charitable activities can create important goals of school, family or environmental education.

People involved in upbringing already mention the so-called "New children" who are unable to concentrate, who are inefficient at work, introverted and unable to live in society. In many schools in the West, any discipline has completely fallen down, and normal teaching has become simply impossible. Despite the use of newer and newer teaching methods, modern laboratories, computers and IT, as well as employing better educated teachers, the knowledge of graduates of these schools is lower than before, the ability to independent, creative thinking is pitifully low, willingness very poor , and orientation towards the world and values none or only little and false (Wielgus, 2001, p. 45).

In many theoretical studies attention is paid to the situation of educational reality in the modern world, which is increasingly called global due to various processes that it has been undergoing for a long time. These processes, called globalization, have been identified with rapid intensification that it exceed the flow of capital, goods, labor, services and ideas. This phenomenon cannot be limited only to economics, because it is also the dissemination of certain processes taking place beyond capital, goods, work, services, and also concerns politics, culture or knowledge (Green, 2003).

It can be said that in Poland today we are dealing with a cultural vacuum, in which huge, opposing loads accumulate – on the one hand a sense of freedom, on the other – material degradation. The IT revolution certainly has an impact, which must have caused a deep cultural crisis, because social bonds are weakening, rules are breaking down, various taboos are being broken, we have a sense of chaos of values.

The Internet is a relatively new medium for communicating, expressing thoughts, passing on ideas and views, but the ease of disseminating information also creates a field of abuse, entering the sphere of freedom of other people. Until recently it seemed that global network is a field completely unregulated and not guaranteed by any rules. This situation is slowly changing and lawmakers and courts are beginning to set limits of behavior in the network. People posting content on the Internet must do so with a minimum of caution, so as not to breach the limits of freedom of speech, especially in the field of broadly understood public security, crime, morality, public order, personal rights of others and secret and confidential information.

As Stewart Brand, creator of The WELL™ said they wanted to create a space where they could implement their own ideas, experiment. Although they did not have any money or influence at that time they were aware of the chance that appeared before them (...). Everyone could say anything there. The most controversy was related to the philosophical approach to human freedom, traditionally associated with the concept of free will. In the considerations concerning freedom, a distinction was made between two concepts: freedom from something, i.e., from factors limiting the freedom of choice, and freedom to something, understood as an activity based on cognition and the use of natural and social necessity. In both these meanings, freedom is not an absolute concept and – like any sphere of human activity – is subject to limitations.

It seems that the great myth of the age in which they had to live was the human right to freely express one's personality, this myth often takes the form today: everyone is allowed everything, but not everyone and everything. Contemporary society faces a kind of human crisis, based on a growing distrust of one's humanity, the very meaning of being, and the affirmation of joy that is creative. One of the most important changes, being at the same time a threat, is the disappearance of the "universal man", and thus versatile education. On

the one hand, there is an easy contact with culture, thanks to the dissemination of it by the media, and on the other, reducing the mass culture, causing spiritual laziness and passivity.

Freedom is an undeniable value in the process of human development. However, this value is mainly declared and extremely rarely implemented. True freedom is connected with people's development of their own abilities and skills in order to live the life they long for, which they aspire to, guided by their aspirations (Sen, 2002, p. 251). But freedom is also the object of the aspirations and ambitions of the collectivity, especially those who not because of their fault are conscious of the experienced limitations and their sources. Sometimes subjective efforts aimed at achieving freedom are caught up in dishonest, unethical and sometimes even oppressive behaviors towards others. Therefore, a person functioning in the space of his life, on the one hand, experiences freedom and trust, while on the other hand is exposed to numerous threats.

The article aims to attempt to show human's opportunities and threats in the social space of the Internet in the context of personal safety in cyberspace.

This goal is to illustrate how conscious and active human participation in the virtual world, including existing threats limits their freedom.

2. Virtual communities – socio-cultural changes in the information society

The Internet is the first global medium whose users are not only recipients, but also content creators. Virtual reality can be used in many areas of public and economic life: in medicine, entertainment, traffic control, as a tool in professional work or in various branches of industry. Cyberspace thus fulfills educational, service, entertainment, social, economic or culture-creating functions, as well as military ones.

In this context, it is justified to place the issue of freedom not only in the sense of the freedom of the recipient, but also – and perhaps above all – the freedom of the sender of the content posted there. If everyone has the right to appear in the network, does that mean that he can freely place everything he wants in it? At first, we might be inclined to answer yes, but even a very superficial reflection raises doubts about such a categorical statement. Freedom is undoubtedly a positive value, one of the most important, even constitutive of human existence, but is it an absolute value? The practice of everyday life indicates that it is impossible to answer this question affirmatively. Immediately, however, the question arises: who and how should limit his freedom on the Internet? Freedom of a man living in a society is subject to multiple limitations, even if only resulting from the norms of cohabitation. However, the limits of social norms are not rigid and – especially today – are shifted in various ways, most often under the slogan of expanding the area of individual freedom, the very existence of them is not questioned. On the contrary, they are also a vital and absolutely necessary value in the life of every community, and therefore have a global dimension. To some extent we can witness the situation of coexistence and interdependence of two important values: freedom of the individual on the one hand, and norms of social life on the other. And it is through such a prism that one should look at the issue of freedom in the Internet.

However, the freedom of the global network is expressed not only in the unlimited possibility of using its resources or expressing one's own views (with the exception of provisions in the regulations of particular services, e.g., portals or criminal law), but mainly in the absence of the main center, which could be an entity / institution of supervision and control over its entirety. The indicated attribute is also mentioned as one of the special features of cyberspace. The others include, among others: liquidity, virtuality, unpredictability, alternation (in the program and information layer), interactivity, no possibility to set boundaries, universal availability or versatility. The notion of freedom is an ambiguous term and unequally understood in various contexts and in relation to various areas of life. Virtual reality can be considered without taking into account its current technological implementation, and thanks to this, based on fictitious, part-existing models, create a kind of VR typology, however, separating it from the typology of the phenomenon of virtuality itself. Thanks to the Internet, virtual communities, which means communities in which people meet in cyberspace and communicate long enough to get to know each other and create lasting relationships. Virtual communities arise because cyberspace is the place where network relationships can appear most clearly. In a network society, cyberspace becomes their natural environment. No wonder, then, that more and more virtual communities appear and will appear in the course of the development of this society. Internet and cyberspace are becoming a natural area of their existence.

Globalization processes, being both the cause and the effect of the emergence of information societies, have a huge impact on the economy, politics, culture, education, and thus on a man and his relations with others. The result of these huge transformations is the relaxation, the break-up of many traditional ties and the disintegration of communities, groups considered before the advent of the information age as permanent and inseparable (see: Batorski, 2006, pp. 144–146). It seems that the cult of individualism, the pursuit of self-realization and climbing the career ladder causes that the organic communities, i.e., family, neighborhood, and professional groups, lose their previous significance. The rapid development of information and communication technologies favors such a process. Compression of time and space, easy and fast communication makes members of traditional, organic, primitive social groups enter into new social relations. It turns out, however, that family and neighbor ties do not have to disappear, because with the help of highly specialized communication tools, you can put up with all barriers, for example: overcome the distance between your home and your workplace. Although the role of organic communities understood traditionally weakens, because direct communication is lost, it does not mean that the modern man is completely stripped of contacts with other people. New media, in particular the Internet – as a round-the-clock global network (Hendrykowski, 2005, pp. 13–19), a web that wraps the entire Earth, allow for the creation of completely new, other interactions and communities that constitute a new quality in interpersonal relations (Stawiska, 2008).

Virtual communities can be created using the following tools and web applications that enable people to communicate with each other:

— E-mail (e-mail), which allows you to send messages to one or many people, which enables discussion. There are countless news groups in cyberspace that correspond with each other using e-mail lists.
— MUDs (Multiuser Dimensions), or various types of virtual text games that allow the player to communicate and make personal contacts with other players.
— Chats that enable real-time conversation by sending messages together. The largest and most popular chat system is IRC (Internet Relay Chat) consisting of a myriad of free channels.
— BBS (Bulletin Bard System), (so-called forums) that group people interested in a specific topic and allow them to discuss. Their members can post the so-called posts or comments to which all participants of the forum have access. Everyone can read them and answer them with their own post.
— WWW (World Wide Web) – is a special tool because it supports all of the above, facilitates access to them and is a great interface for their use. It often happens that a specific community is formed around a website.

Two types of virtual communities can be distinguished (Castells, 2003, pp. 145–146). The first are specific virtual communities that are an extension of the real world community. There is no process today in which virtual communities would completely replace real communities. Communities organized in real time and space, which can be described as organic communities, of course exist, but their existence depends to a large extent on technical means of communication, including the Internet. The Internet is increasingly used by people to transfer ties from the real world to the virtual world, extend these ties, shorten the distance to people they know in the real world. It also facilitates maintaining contacts with people we know from real space, but with whom for some reasons, most often spatial distance one cannot communicate. The Internet allows you to constantly refresh these contacts. M. P. Effrat has identified three types of interpersonal communities (Effrat, 1974; as cited in Szpunar, 2004, p. 107), many examples testify to the fact that today they are increasingly supported by the Internet.

The classification is as follows:

— Communities as solidarity institutions, e.g., family, ethnic group, voluntary organization. Members of these groups feel mutual solidarity, and norms, roles, the feeling of warmth and closeness play a big role in these communities. The Internet supports such communities, an example of which is the communication maintained by family members who are apart from each other, friends from other cities or immigrants who are outside their country.
— Communities as interactions, that is, those in which relationships exist that connect people beyond what is necessary. These informal relations make people cooperate. An example of such communities supported by the Internet may be a group of alter-globalists, who arrange protest actions via the Internet.
— Communities as institutionally different groups, i.e., communities connected by a common institution on the basis of belonging to a social category.

The second type of virtual communities are those existing only in cyberspace.

It often happens that people participate in virtual communities that arise spontaneously independently of human relationships outside the network. In cyberspace it is extremely easy to find people like themselves and make contact with them, satisfying the need to belong to a group and building their identity in this way. The community network that emerges in the society is not connected by the territorial bond, but the similarity of interests, views or values, which is why cyberspace is a perfect environment for them. Communities created only on the Internet are predominantly based on similarity. This is favored by the intentionality of virtual communities. Members participate in them voluntarily, with complete freedom and freedom of choice unheard of in any organic communities. In addition, leaving such communities is extremely easy, because Internet users do not have to stay strong in them, trapped by necessities, conventions, roles or social norms. Without being restricted, people usually choose to participate in communities consisting of people similar to them (Siuda, 2006). The intentionality of virtual communities and their increasing popularity is influenced by their spatiality and asynchrony. The point is that interactions in cyberspace are not limited either spatially or temporarily. Internet communities exist in every part of the globe, at any time. Spatial proximity does not matter, and communication does not have to take place in real time.

It coincides with the nature of the network society, which is becoming less and less dependent on the territory. Virtual communities are also astigmatic, that is, the status and physical characteristics of people are not significant. Race, nationality, age, gender, physical handicap, education do not matter. Often, community participants never get the chance to meet in reality and only the Internet allows them to establish mutual relationships. Astigmatism strengthens the role of similarity in shaping these communities. They are as homogeneous in terms of interests, values, views or attitudes of their members as heterogeneous they are in terms of age, social status and other status factors (Wellman & Gulia, 1999, p. 182). It often happens that virtual communities are continuing in real space. You can find many examples of such interweaving of real and virtual contacts. A person met in a chat or online forum may want to meet off-line. It happens that groups of people who have met on the Internet also meet live, thus creating organic communities. The fact that cyberspace initiates real relationships proves that in a network society it is the best environment for the emergence of human communities. In view of this fact, the question arises whether virtual communities can really be called full communities that can complement or completely replace the participation of people in organic communities? Many Internet critics emphasize that in cyberspace individuals are alienated, unable to build relationships with other people, enter into accidental, short-term and superficial contacts. Creating internet communities is not possible due to the anonymity of people in cyberspace, allowing them to accept any identities, which means that they live in a world of delusion and fantasy.

3. Selected threats in the social space of human development

The IT revolution caused that the modern world has become dual and simultaneous – both real and virtual at the same time. The spatial paradox of the global network implies the need for deeper considerations regarding the idea of digital freedom in a safe security space. On the other hand, the incongruence of the idea of freedom is expressed in the two points marking it: from and to. In the aspect of the virtual network – the freedom to manifest itself will be both in access to the legal resources existing in it, as well as the freedom to use them in any way and express their own beliefs or views. In turn, the parameter should be determined both by freedom from limitations in access to resources as well as those related to censorship and threats. However, the dynamism of development implies not only positive changes, but also new challenges and threats. These threats are of a twofold character: they are existing negative phenomena transferred to the real world networks, and the emergence of new categories of dangerous behaviors and crimes.

The general classification of digital threats is implied by:

— human / user activity: targeted (e.g., cybercriminals) and unintentional (e.g., unconcerned users),
— lack of direct connection with purposeful human activity (system unreliability, errors in software),
— natural environment (e.g., natural disaster causing a power failure),
— hybridity of events.

In turn, the division of threats in the information attribute functioning in the digital environment will result from the purpose function, i.e., interference, theft, interception, damage, manipulation, control takeover, modification or destruction (information and / or systems). The tools used to achieve the indicated goals

are properly prepared, malicious programs – viruses or computer worms. Among them, the following are distinguished:

— logic bombs – a dormant form of malicious software that activates when specific conditions are met (e.g., on a specific day),
— Trojan horses – software which, impersonating useful or interesting applications for the user, additionally has undesirable, hidden functionality,
— hoaxes – programs that display false information that a virus is in the computer,
— spyware – software designed to spy on users, e.g., to register visited websites or passwords typed on the keyboard without their knowledge, and then to send them to the attacker,
— phishing – it is based on insidious acquisition of logins and passwords by impersonating a trustworthy institution or person.

What the indicated forms of malware have in common is the need for user interaction and response (e.g., clicking on a link), and the essence and purpose – infection of the system (device) and achievement of the intended effect (e.g., data theft).

It should be noted that attack methods that do not require specialist knowledge in the field of programming are being used more and more often. These include digital forgery and extortion, which can be divided into the following subcategories:

— made with the help of malicious software,
— made by means of false messages (e-mails),
— hybrid (fake e-mails containing malicious programs or a link to such types of programs).

The second and third of the indicated forms is based on the preparation of an e-mail message in which the attacker impersonates a specific institution or entity (e.g., postal operator or internet service provider), inserting a link to the page or an attachment with a file suggesting e.g., an invoice. In fact, the attachment contains a malicious program that infects a user's device.

Threats of a social nature are primarily related to the appearance of harmful and illegal content on the web, users taking risky behaviors or dangerous contacts. They concern such phenomena as cyber bullying, grooming, sexting, hatred, child pornography, racist content, encouraging suicides and others. It is worth pointing here also threats called APT (Advanced Persistent Threat) attacks that combine different types of programming or social engineering tools. Preparations for such attacks can take many weeks and are usually carried out by organized groups that have substantial financial resources and the time necessary to infiltrate a specific target (organization, institution, company) and then carry out a precise action.

Open Internet resources facilitate access to various content, including illegal content, as well as content that is not illegal in the light of the law, but belongs to the harmful category. The harmful content is considered to be the one that can cause negative emotions in the recipient and that may affect his / her emotional and social sphere and behavior. Among them there are e.g., content depicting violence, physical injuries, presenting drastic scenes, cruelty to animals, calling for self-destructive activities, discriminatory and pornographic ones. Almost a quarter of Polish young Internet users have been in contact with "content potentially threatening the social development of children, created by other users", potentially threatening the social development of children, created by other Internet users (Kirwil, 2011, pp. 42–44). Not only can the harmfulness of content affect human development. Their attractiveness is also paradoxical. Interestingly enough, attractive content and applications with which users come into contact with the network may result in the loss of control over the time and intensity of the use of the Internet, computer, computer games, social networks and other virtual activities. This may affect the limitation or resignation from other activities of daily life and lead to neglect of the family, duties, schooling or hobbies and / or avoiding contact with peers. Surveys of Polish teenagers showed that they have stayed in the network longer than originally planned (83.3%), and more than half have felt irritated when the Internet stopped working or they did not have access to it (64.2%). In addition, every fifth teenager has resigned from sleep, every third from the duties in order to be able to use the Internet (29.8%) (Kamieniecki et al., 2017).

Currently, there is a right to choose between the real social space and the alternative space, which is cyberspace. If the real space is as real as possible, then cyberspace is virtual. If the real space is territorially limited, meetings can take place at a certain latitude, in a specific time zone, then there is no time limit in cyberspace. In every unit of time, you can contact people around the world, and thus cyberspace becomes a new space of

interpersonal or social relations. Anonymity in cyberspace causes that without these barriers you have to deal with the low level of stressfulness of this virtual reality. If contacts through these barriers are in fact elitist, limited to a certain group of people, they are of an egalitarian (Grubicka, 2017) character in cyberspace. It determines that cyberspace is becoming an increasingly attractive social space. Cyberspace is also increasingly an opportunity to escape from problems in the real world. While avoiding uncomfortable dialogues, questions, comments or contacts in reality, Internet users are able to hide themselves in the network and create a space there corresponding to their current needs or giving anonymity and a relative sense of security (Grubicka, 2017, pp. 56–57).

Users of cyberspace, participating in various virtual communities begin to believe that it is not only a simulation of contact with another human being or group, but actually a form of interpersonal communication (Burszta, 2003, p. 175). According to Burszta (2003, p. 159), this leads to the phenomenon of social loneliness, difficulties in defining one's identity, as well as the ability to communicate with other face to face.

From the observation of the online social life that the activity of its members is the beginning of the interaction continued in reality or vice versa, this reality is transferred and continued in the virtual space. This shows that the virtual community is not a completely separate reality, but only one way to conduct an interaction that can affect other aspects of human life. Particularly, that its participants make their socio-economic statute, sex, age, cultural environment, and offline relationships. M. Smith lists five basic features that define the virtual community, and at the same time are not achievable in traditional communication (Butkiewicz, 2003, p. 200). These include: anti-spatiality, asynchrony, anti-carnation, stigmatism, anonymity. Dependence of the virtual community with assigned features in the perspective of social pathology analyzes is presented in Figure 1. However, as in any social space, and also in cyberspace, various deviations appear, that is all behaviors, which to a greater or lesser extent deviate from the applicable norms, the applicable value system.

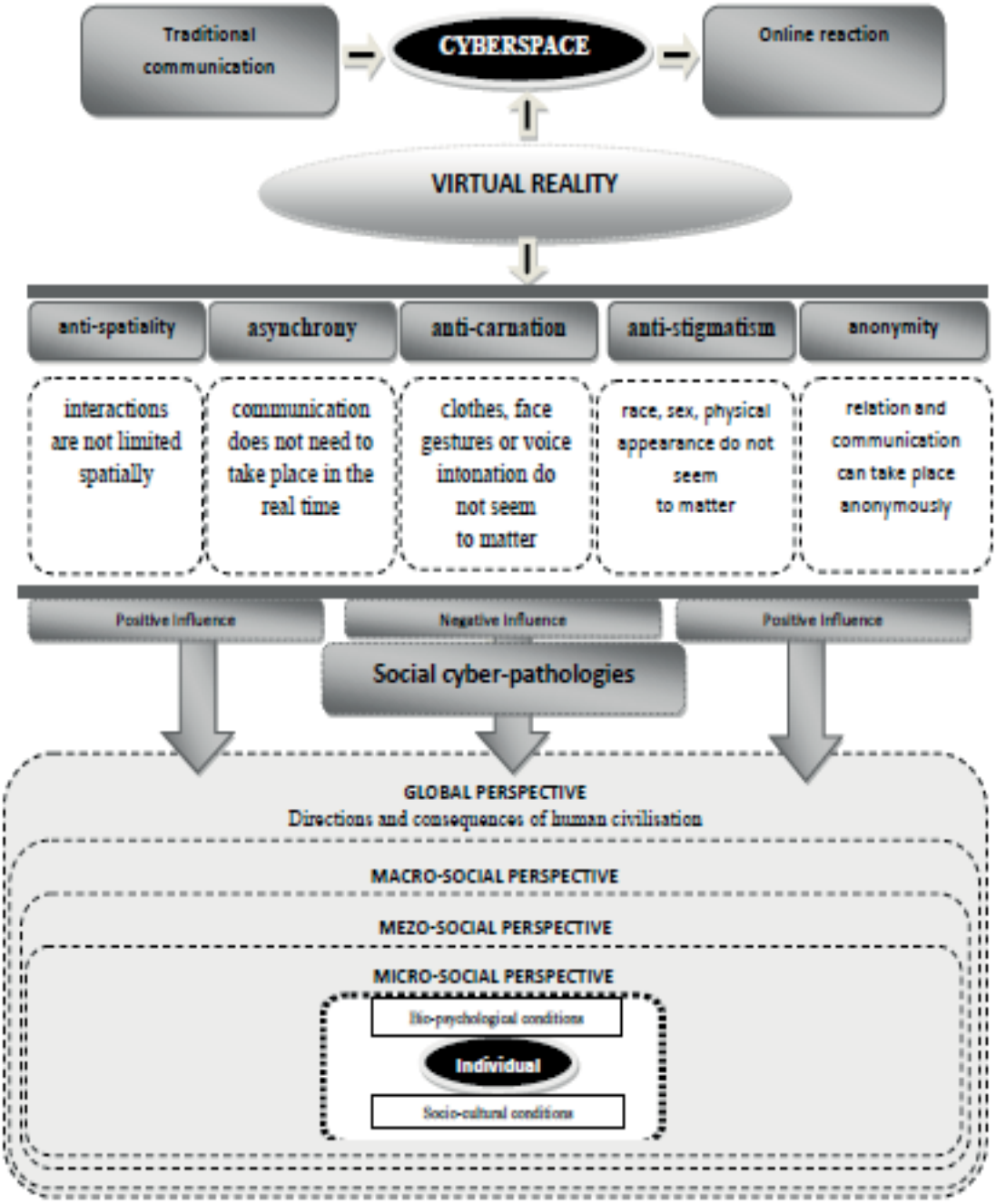
Social pathologies are one of the greatest threats to a man in the social space of security, although it is often overlooked or marginalized in the broadly understood problem of social security. And this is an important problem not only from the perspective of individuals affected by the pathology, but also of the whole society. It is not important whether we are dealing with new or old signs and whether other society is being even more disintegrated.

What is important, however, is that all these phenomena indicate a serious illness of society. Currently, in the social pathology itself, the term deviation and social pathology are often used interchangeably. However, these terms should be clearly distinguished for a simple reason, because if one talks about abnormal behavior, they must be positive and negative. Devotees on the one hand are a threat and on the other hand needed in society for social progress. New pathologies, social cyber pathologies, are characterized by an objective criterion for assessing pathological phenomena. The assigned criteria in real space, take on features in cyberspace, including: behaviors that deviate from norms, contrary to the system of values, accepting social destructive damages and behaviors that require appropriate social intervention through appointed people, institutions that counteract these types behavior.

Examples of behaviors of destructive social objects of both personal and structural entities in cyberspace are: cybercrime, cyber bullying, cybersex, addiction to the Internet (net-holism) and telephone (phonoholism). It is worth paying attention to the fact that an individual, small social groups or larger communities through IT tools can be a victim as well as the perpetrator of pathological behaviors. Reference subject of activities undertaken by the social environment in the scope of ensuring their safety and protection against pathological phenomena, can also become the causative agent of these activities. To do harm to yourself, self-destruction seems to be a logical activity, typical of a madman.

According to Freud, each individual carries an impulse, pushing towards life and everything, called the "drive of life", but also a completely opposite, inclining towards death and destruction, which he described as "the drive of death". It is also a factor causing the development of symptoms and self-destructive behaviors in some people. However, only in some cases these behaviors become rooted and transform into permanent personality traits. Usually this happens if there are large layers of suppressed anger. Aggressive impulses in cyberspace are directed to another person but for some reason it is impossible to express them. Sometimes this happens because they are directed to a loved one or for fear of the consequences of saying them out loud. In these cases, the aggression is directed at the person. That's when the man learns how to behave like his greatest enemy and develop self-destructive personalities.

Figure 1. *Virtual community in the perspective of analyzes of social pathologies*



Source: own study

Self-destructive thoughts include all thoughts aimed at the devaluation of a person, preventing their progress or undermining their achievements. In the mind of a self-destructive person, such thoughts appear almost automatically. People with self-destructive tendencies often behave in a hostile or even hurtful way towards others. They provoke unnecessary conflicts, behave in a mindless way, they are rude, jealous, they gossip, etc. They perceive the other person as a source of quarrel. Other people cause them to be frustrated because ties are based on comparisons in which for one reason or another they always lose. After such conflicts, they usually fall into the stage of deep self-pity. They attack, but when someone responds to their attack, they behave like victims of injustice. They offend, but when someone offends them, they feel sorry for themselves. They do not admit that it was their own fault.

The Internet is conducive to interpersonal contacts, however, online contacts carry certain risks, especially in cases of using the network to establish relationships with people unknown directly in the offline world. It is worth noting that just such an activity – contacting people online personally unknown – is declared by as many as 25 percent of young Internet users (Kirwil, 2011, pp. 42–44), and many admit to a personal meeting in the real world with previously unknown people, and met in the network. The group of dangerous contacts

should also include the phenomenon of children's seduction on the Internet based on creating a relationship via the Internet between an adult and a minor (under 15 years of age) in order to seduce and abuse them. Seduction of children on the Internet is a crime regulated in art. 200a of the Penal Code, which reads as follows:

> **Article 200a**
> *§1 Whoever establishes contact with a minor under the age of 15 in order to commit crime described in art. 197§3 p. 2 or art. 200 as well as produces and maintains pornography content via tele-information system or telecommunication system, in order to meet the person through misleading the person, using the mistake of incapability to proper comprehension of a situation or through unlawful threat, shall be subject to the penalty of deprivation of liberty for up to 3 years.*
> *§2 Whoever submits a proposal to a minor of sexual intercourse, undergoing or performing other sexual act or participating in production or recording pornography content and aims at its realization via tele-information system or telecommunication net shall be subject to the penalty of restriction of liberty or deprivation of liberty for up to 2 years* (Act of 6 June 1997. – Penal Code, 1997).

Dangerous contacts are also contacts aimed at drawing a teenager into various types of sects, groups, communities and subcultures, e.g., on radical views, propagating aggressive behavior, e.g., self-mutilation behavior, restrictive diet or the use of psychoactive substances. Such contacts are also made by people interested in obtaining personal data and other confidential information, later used for criminal purposes.

Building and maintaining potentially dangerous contacts with strangers is not only the domain of young people, but because of inexperience and often less due to age competences in the proper assessment of the situation, understanding and predicting the effects of actions taken in contrast with openness, willingness to make friends and trusting it is them who are more exposed to serious consequences.

The Internet is a place of experimentation, also with its own identity and taking risky behaviors. What are the behaviors of web users? These include: seeking information about drugs and other psychoactive substances or activities harmful to health or making dangerous contacts, including strangers who may display pedophile tendencies or individuals / groups that encourage behavior that is risky or illegal. One can include sexting (including camera sexting) into the group of risky behaviors – the phenomenon of sending content (photos, videos) of an erotic nature, mainly your naked or half-naked photos, using the Internet and a mobile phone. Sexting can also take the form of sex-communication live, through instant messaging using a video camera on the device. Research shows that every fourth Polish teenager has received intimate pictures, 7% of teenagers have sent intimate pictures (see Lange, Osiecki, Chrzanowski, & Wrońska, 2014, pp. 6–36), and about 30% of teenagers "know a person" who sends intimate pictures. In addition, teenagers abuse / dysfunction the Internet (13%) (Makaruk, Wójcik & Konsorcjum EU NET ADB, 2012, pp. 3–33) gamble online and, above all, do not protect their privacy by sharing too much information about themselves, publishing numerous photos and admitting friends to random friends. This "openness" is a contribution to other users' electronic aggression and violence. These include calling, scaring, persecuting, denigrating, humiliating someone on the Internet using new technologies. Experiences related to various forms of cyber bullying, such as altering and publishing ridiculous photos and videos, making the victims' secrets public, persistent, vulgar and malicious comments on entries, and deliberately ignoring the victim's online activity, have been confirmed by many young internet users (Pyżalski, 2012, pp. 212–219; Kamieniecki et al., 2017, pp. 49–86).

What is the future of the Internet? Modern technologies, changing at an extremely fast pace, will make technical use of the network even easier. Perhaps voice communication will be enough to work with a computer, as long as it is adequate to use such a name. Certainly, the network will become an even richer source of knowledge, information, entertainment and a communication platform. Such a perspective is quite real and perhaps quite close. One thing will not change – using the Internet is and will be a matter of responsibility, there is a need and reflection on which materials are should and should not be used.

4. Assessment of personal security in the virtual world and Internet threats in the users' awareness

We live in times when the problems of values, good and evil, are of little interest. One should get to know each other and understand others (magic of labels: "we", "they", "others"). There is a romantic myth that a child by nature is good and capable of self-development, if only we create the necessary conditions for growth. The family, school and church are rapidly losing strength to the peer group and mass media (computer games, colorful magazines, sports and music shows). The peer group becomes a dangerous educator (aggressive, hedonistic and consumption behaviors).

We live in the world of different values. Human life is about making choices all the time. Today, great attention is paid to the need for "axiological education", leading to the conscious selection of values by people and determining their hierarchy as the basis for constructing their own philosophy of life, professional aspirations and preferred lifestyles. Axiological concepts influence educational goals because:

— axiology gives an overall view of the world of values;
— it is a determinant of education goals in large and small social groups;
— more and more attention is paid to individual systems and hierarchies of values.

The overriding value in terms of contemporary axiology is a man, his life, mental and physical development, self-realization, freedom, identity, subjectivity (Lewowicki, 1997, p. 19).

There is a crisis in the norms of social life and quality of life (fast life, immediate satisfaction, lightness of life). Schools still leave a large group of functional illiterates (misunderstanding commands, reading without understanding). This is because the school primarily provides memory-alphabetical knowledge, fragmentary information that cannot be merged into operational knowledge.

It may not be an exaggeration when one can accept the position that nowadays fewer and fewer people are going to pursue happiness, and more and more are looking for ways to save themselves from the misfortunes of the threatening and the upcoming. The range of such conflicts seems huge nowadays. People cannot cope alone with each other, and in their mutual relations there is a wave of reluctance and unfriendliness, jealousy and aggressive actions.

The fundamental rights of the information society include: free access to the global information infrastructure, ownership, credibility of information and the right to privacy protection (Benkler, 2008, p. 476). The guarantee of these rights and their protection is a great challenge for modern countries. National legislation on the Internet is territorially limited. The immanent feature of the Internet is its global reach, allowing any messages to be included in its resources. Therefore, the problem of contemporary states is to counteract the publication of certain contents on the web. It is often pointed out that the Internet – however generally associated with the freedom of expression – can also become a tool for surveillance and surveillance of citizens. It gives various companies and institutions great opportunities to track users, collect messages and create databases of potential clients. Also, state institutions are increasingly interested in what is happening in the network (Podgórski, 2006, pp. 105–106) (Podgórski, 2006 p. 105-106.) One can therefore risk saying that cyberspace is expanding the sphere of not only freedom, but also control. Repressions against defiant bloggers or blocking access to undesirable websites have become a practice commonly used in some countries hostile to freedom on the Internet, e.g., in China. Authoritarian states can use the filtering and monitoring functions of the message. There is a belief that adequate access to online tools will ensure greater freedom everywhere. The example of China indicates something else. China, more than any other country, proves that universal access to the Internet is possible while maintaining control over its use (Benkler, 2008, p. 159). The fundamental issue in this respect is balancing the rationale between the security of states and societies, and the freedom of the individual and their right to freely exchange information. When dealing with ever-increasing technological progress, a man loses his guard and overly trusts in technology. This is especially dangerous in the case of information protection, where the vast majority of it is transmitted via the Internet (Grubicka, 2015). In order to ensure the ICT security of the country, areas of responsibility as well as ways and forms of cooperation should be defined, in particular:

— protection of the critical ICT infrastructure of the state against the dangers of cyberspace;
— cooperation in the field of preventing and combating forms of computer crime;
— supporting projects establishing the perpetrators of cyber-terrorism;

— sharing relevant information about serious IT threats identified in own systems and ICT networks and other important facts for the protection of the country's critical ICT infrastructure;
— undertaking actions to increase public awareness in the cyberspace security category.

Considering the fact of real threats to the virtual network and the increasing, real losses related to their effects, for over two decades efforts have been undertaken in order to standardize the digital world – both at the level of states, organizations and in the broad international space. It is not disputable that in the present form, there is no longer the possibility of returning to the origins of the network, which was just a place of ideas and served mainly to exchange ideas of users, making the dream of global communication a reality. Today it is the basis for the functioning of every area and sphere – both state and private. The challenge is to find a balance between maintaining the freedom of the network and its security – at each of the levels mentioned above and in each area. The best example of actions undertaken in this area are in particular: European Union Cyber Security Strategy: an Open, Secure and Protected cyberspace, Directive on Measures to Ensure a Common High Level of Network and Information Security within the Union or – in international space – American International Strategy for Cyberspace. What the undertaken activities have in common is a clearly defined goal: maintaining and developing network security with ensuring Internet freedom – understood in general as the development of a society based on the protection of fundamental rights and freedoms (in particular freedom of speech) with simultaneous effective data and privacy protection and ensuring free flow of information , (among others prevention of censorship). Paraphrasing the words of A. de Tocqueville, one can state that the freedom of the network ends where its security begins. For it is impossible to ensure security without interfering with the internal structure and functioning of a given sphere. At the same time, it is impossible to ensure freedom without protection, which in the case of the digital world, due to its special specificity (also from the strictly technical side), would lead either to anarchy or to stronger control.

Threat to such understood freedom, however, becomes a different type of action that would allow Internet service providers to set different conditions for access to users, with the right to introduce additional charges including for the so-called special services. On the other hand, the challenge is *post-mortem* regulations, because it is only on the knowledge and previous activity of users that their heirs will be able to not only inherit digital assets, but also be able to terminate matters in the digital world, such as using services, servers or account deletion. Issues of this kind, although sensitive, remain extremely important: nowadays, most prosaic matters such as bills are carried out via the network (e-mail notification, payment via electronic banking, etc.). It can be concluded from the previous considerations that just as cyberspace has certain layers, the paradigm of network freedom in these layers will be manifested. At the information level, it will concern: open, equal and unrestricted access to their resources for all users. This issue is also relevant in the context of the so-called free software, whose idea and implementation assumes the ability to be run, copied, distributed, analyzed, changed and improved by users. According to the free software definition published by the Free Software Foundation, the user is entitled to the following freedoms, which are at the same time basic assumptions for the software to be defined as free:

— freedom 0: running the program for any purpose,
— freedom 1: analyze the program and adapt it to your needs,
— freedom 2: distribution of a copy of the program,
— freedom 3: improve the program and publicize your own improvements, so that the whole community can benefit from them (see Free Software Foundation, 2019).

Freedoms 1 and 3 can only be met if software source code is available The indicated assumptions allow for better understanding of the context of using network services such as Software as a Service (SaaS), the point of which is to offer certain services or programs by the service provider, run on its devices. In practice, this means that the user uses the tools / programs offered by the service provider via a web browser, so there is no need to install separate software on his own device, e.g., Google application suite, to fully use their functionality. Despite the convenience of using this type of services, as stated explicitly by Richard M. Stallman: *That people have no control, as using the service on the Internet we at the same time deprive ourselves of freedom, both in terms of data entrusted to service providers, but also in this freedom, which gives users truly free software* (Miąsik, 2013). In addition to the lack of control over the data, it is also the responsibility of the service provider to the manner and scope of use by the users of the provided software, because the service provider's computer is in fact used.

One cannot consider the freedom of the network, only in the widely known form, because it has a parallel layer called Deep Web (hidden network / deep network). The term also refers to: Dark Net / Dark Web. Dark Web means websites that hide the IP addresses of the servers they use, which can make it impossible to find such sites through standard search engines. The most commonly used encryption tool used to hide addresses, but also end users is The Onion Router (TOR). Despite the controversy aroused by such tools, in particular in the field of illegal content or criminal activity, solutions that allow for anonymous activity also serve legal (ordinary) users who do not want to be tracked by tools used by digital service providers, e.g., browsers. The classic example of the ability to track user activity are so-called cookies, which in principle should only support the operation of the application itself. Tracking of searched content, websites visited, downloaded files or purchased items allow for the so-called user profiling (interests, habits or even residence).

In a classic, broader sense, safety is defined as a condition free of threats. In the context of information security, it is a condition free from threats such as: sabotage, espionage, diversion, but also transfer of information to unauthorized entities.

The scope of this definition also includes all activities serving to secure information resources – produced, collected, processed, stored and transferred in communication networks and information carriers (computers, servers, databases), and in particular security systems and methods. Resource security – in the technical sense – is determined by two management models: restrictive (what is not allowed, is prohibited) and liberal (what is not prohibited is allowed).

Previously indicated documents of a strategic and normative nature assume the creation of specific zones of responsibility for the security of the network itself and thus the data functioning in it, i.e., the Internet, intranet, extranet, etc., as well as for individual elements and areas. An example of this may be the imposition of specific obligations in the area of security on the key NIS Directive operators (2016), i.e., critical sectors such as private or public: finance, energy, transport, health care and digital service providers (search engines, trading platforms, cloud computing services). The first set contains entities that are compatible with art. 5 of the Directive and meet the following conditions:

— they provide a service that is critical to maintaining critical social or business activities;
— providing this service depends on network and information systems – the incident would have a significant disruptive effect on the provision of this service.

In addition, each of the Member States of the European Union is required to adopt a national strategy on the security of network and information systems, defining strategic objectives and appropriate measures and regulations to achieve and maintain a high level of security of network and information systems and cover the minimum sectors and services indicated in the Directive. In addition, issues which must absolutely take into account national strategies in the field of network and information systems security have been identified, namely:

— priorities and goals of network and information systems security,
— a management framework to achieve the objectives – including roles and ranges,
— duties of government bodies and institutions and other relevant entities (each country was obliged to designate a body or bodies to protect cyber security),
— measures in terms of readiness, response and restoration of normal functioning, including in the area of cooperation between public and private sectors,
— within the scope of adopted national strategies: guidelines for educational, information and training programs, and guidelines for research and development plans,
— risk assessment plans for their determination,
— list of entities involved in the implementation of the strategy.

In the area of international cooperation, the NIS Directive in art. 13 provides for the possibility of concluding international agreements "*in accordance with Article 218 TFEU, with third countries or international organizations, allowing and organizing their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data*" (The European Parliament and of the Council, 2016). In relation to the global coverage of the network, the entry of art. 18 paragraph 2 Jurisdiction and territoriality is particularly significant, which states that: a digital service provider that does not have an organizational unit in the Union, but offers services in the area of an online trading platform, internet search engine and cloud computing is obliged to appoint a representative in the Union who must have an organizational unit in one of the Member States where the services are offered.

In terms of jurisdiction, this means that the digital service provider falls under the jurisdiction of the Member State in which the representative has an organizational unit.

The issue of the existence of the network understood as a global medium and the functioning environment of the information society also needs to be raised here: its axis, focal point and reference point is and will be the user, but despite the key role, little space and attention is devoted to documents that seem to put emphasis on all of the previously mentioned layers of cyberspace. Responsibility, but above all awareness of the mechanisms and digital threats of users would undoubtedly contribute to faster and more complete achievement of the goals set in this area.

5. Summary

Freedom of the other is the most general and rather universally accepted boundary of one's freedom. Taking advantage of the freedom of speech, the right to have our own views and goods, the right to respect for personal dignity, one cannot forget that the same rights are enjoyed by others, and therefore all actions of the individual cannot limit and violate the rights of other people. There is no reason why these standards of behavior in real life should not apply to the virtual space on the Internet to the same extent. After all, it is only a tool, and although it has undoubtedly influenced social life, nevertheless, man is its creator, not material.

Virtual communities can therefore be considered as full human communities that can complement or replace participation in organic communities. The emergence of online communities is due to the features of the modern network society. Human community, participation of people in communities, is based on entangling networks of relations. The Internet – one of the catalysts of the emergence of a network society – is now the most perfect reflection of these networks. Therefore, it is an ideal environment for the emergence of human communities, which are more and more often formed in it and through it. It is a kind of change in the character of human communities based on their existence in cyberspace in the form of virtual communities. They enable people to maintain ties with others in the new social conditions in which they live – in a network society. Therefore, they are becoming more and more important today, because they enable the flourishing of human community.

Dissemination of legally banned content on the Internet (pedophilia, incitement to crime, propaganda of fascism or communism, preparation of terrorist activities) is and should be punished. Portal administrators on which such content is posted must have an absolute right and even the obligation to remove it. Another extremely important issue is the lack of responsibility for the word commonly found on the Internet, especially in anonymous vulgar "posts" deliberately aimed at the dignity of the person, good name of the social group or organization they concern. It seems that practical implementation of the principle that entries and comments on the Internet cannot function anonymously, that the technical condition for displaying content on the Internet is to register and provide your personal data (in the form hidden for the general public) would not violate the right. The applied rule should be – as much freedom as responsibility. Limitations, however, should always be individualized, referring to a specific person or group of people who are contradictory to social norms of action. In no case, however, can these restrictions be imposed by the administrative decisions of the authorities and concerning society. Such forms of action are a manifestation of totalitarianism and cannot be justified in any way.

Summing up, it should be said that there is an attempt to show human's opportunities and threats in the social space in the context of personal security in cyberspace concerning several important elements of its functioning. The first issue is the specific level of consciousness of a human being, especially his predispositions, moral and axiological attitude, and reflexivity. The second issue is the appropriate potential of freedom of culture, which is manifested in the fields of human functioning, that is education and upbringing. In each of these fields there are specific conditions for shaping and updating emancipating competences. An important issue of proper assessment of opportunities and threats in space is an appropriate educational system, which should provide education and the dominant participation of people in social life. It should shape intellectual independence, criticism and creativity, professional flexibility, the ability to participate in the scientific cognition and transformation of reality, and responsibility for the social environment, that is, the eco-humanistic attitude to this environment, including empathy.

Education still has to undergo transformations and changes. It must give a man much more opportunities to experience life, discover opportunities, the best prospects for his own development. Greater emphasis should be placed on individualizing, getting to know oneself and managing oneself. Certainly, it will take a long time to develop a consensual, shared vision of a safe and at the same time free digital space. The Internet makes it more difficult for authoritarian regimes to control the population, and the unprecedented openness and freedom of the networked environment requires new ways to protect societies that are open to individuals and groups that are destructive. International cooperation is a prerequisite for effective enforcement of restrictions.

References

Act of 6 June 1997. – Penal Code., Journal of Laws 1997. No. 88, item 553 § (1997).

Banach, C. (2004). *Edukacja wobec problemów współczesnego świata i człowieka.* In K. Denek, T. Koszczyc, & M. Lewandowski (Eds.), *Edukacja jutra: X Tatrzańskie Seminarium Naukowe = Education of tomorrow*. Wrocław: Wydaw. WTN.

Batorski, D. (2006). *Korzystanie z Internetu – przemiany i konsekwencje dla użytkowników.* In Ł. Jonak (Ed.), *Re: Internet—Społeczne aspekty medium: Polskie konteksty i interpretacje* (pp. 119–152). Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Benkler, Y. (2008). *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność*. Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Burszta, W. J. (2003). *Internetowa Polis w trzech krótkich odsłonach*. In W. J. Burszta (Ed.), *Ekran, mit, rzeczywistość: Po co nam rzeczywistość.* (pp. 157–175). Warszawa: Wydawn. Książkowe Twój Styl.

Butkiewicz, K. (2003). *Tożsamość. Halloween przez 365 dni w roku.* In W. J. Burszta (Ed.), *Ekran, mit, rzeczywistość: Po co nam rzeczywistość.* (pp. 191–201). Warszawa: Wydawn. Książkowe Twój Styl.

Castells, M. (2003). *Galaktyka internetu: Refleksje nad Internetem, biznesem i społeczeństwem*. Poznań: Dom Wydawniczy Rebis.

Effrat, M. P. (1974). *The community: Approaches and applications*. New York: Free Press.

Free Software Foundation. (2019). *What is free software?* Retrieved November 4, 2019, from GNU Operating System website: https://www.gnu.org/philosophy/free-sw.en.html

Green, A. (2003). Education, Globalisation and the Role of Comparative Research. *London Review of Education*, *1*(2), 84–97.

Grubicka, J. (2015). *Konwergencja technologiczna a system bezpieczeństwa informacji.* In W. Filipkowski (Ed.), *Nowoczesne technologie na rzecz bezpieczeństwa: Praca zbiorowa* (pp. 86–99). Gdynia: Wydawnictwo BP: Akademia Marynarki Wojennej. Wydział Dowodzenia i Operacji Morskich.

Grubicka, J. (2017). Restricting freedom on the internet in a public security space. *East Journal of Security Studies*, *2*(2), 56–71.

Hendrykowski, M. (2005). *Metafory Internetu*. Poznań: Wydawnictwo Naukowe UAM.

Kamieniecki, W., Bochenek, M., Tanaś, M., Wrońska, A., Lange, R., Fila, M., … Konopczyński, F. (2017). *Nastolatki 3.0: Raport z badania*. Warszawa: NASK – Instytut Badawczy.

Kirwil, L. (2011). *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: SWPS – EU Kids Online – PL.

Lange, R., Osiecki, J., Chrzanowski, M., & Wrońska, A. (2014). *Ogólnopolskie badanie: Nastolatki wobec Internetu*. Retrieved from Rzecznik Praw Dziecka – NASK – Pedagogium WSNS website: https://akademia.nask.pl/badania/raport_z_badan_nastolatki_wobec_internetu.pdf

Lewowicki, T. (1997). *Przemiany oświaty: Szkice o ideach i praktyce edukacyjnej*. Warszawa: Wydawnictwo Żak.

Makaruk, K., Wójcik, S., & Konsorcjum EU NET ADB. (2012). *EU NET ADB Badanie nadużywania internetu przez młodzież w Polsce* (No. SI-2010-KEP-4101007; pp. 3–34). Warszawa: Fundacja Dzieci Niczyje.

Marshall, G. (2008). *Słownik socjologii i nauk społecznych* (M. Tabin, A. Kapciak, & H. Banaszak, Trans.). Warszawa: Wydawnictwo Naukowe PWN.

Mead, M. (2000). *Kultura i tożsamość: Studium dystansu międzypokoleniowego* (J. Hołówka, Trans.). Warszawa: Wydawnictwo Naukowe PWN.

Miąsik, M. (2013, March 18). Richard M. Stallman odwiedził Polskę. Król hakerów twierdzi, że w Sieci pozbawiamy się wolności. Retrieved November 4, 2019, from Gadżetomania.pl website: http://gadzetomania.pl/3758,richard-m-stallman-odwiedzil-polske-krol-hakerow-twierdzi-ze-w-sieci-pozbawiamy-sie-wolnosci

Podgórski, M. (2006). *Wirtualne społeczności i ich mieszkańcy. Próba etnografii*. In J. Kurczewski (Ed.), *Wielka sieć: E-seje z socjologii internetu* (pp. 76–209). Warszawa: Trio.

Pyżalski, J. Ł. (2012). *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*. Kraków: Oficyna Wydawnicza "Impuls."

Sen, A. K. (2002). *Rozwój i wolność* (J. Łoziński, Trans.). Poznań: Wydaw. Zysk i Spółka.

Siuda, P. (2006). Społeczności wirtualne. O wspólnotowości w społeczeństwie sieciowym. In M. Sokołowski (Ed.), *Oblicza Internetu: Internet w przestrzeni komunikacyjnej XXI wieku* (pp. 179–186). Elbląg: Wydawnictwo Państwowej Wyższej Szkoły Zawodowej.

Stawiska, N. (2008). Rzeczywista nierzeczywistość. Czaty, blogi, fora internetowe – nowa przestrzeń komunikacji społecznej. In B. Płonka-Syroka & M. Staszczak (Eds.), *E-kultura, e-nauka, e-społeczeństwo* (pp. 239–250). Wrocław: Oficyna Wydawnicza Arboretum.

Szpunar, M. (2004). Społeczności wirtualne jako nowy typ społeczności—Eksplikacja socjologiczna. *Studia Socjologiczne*, *2004*(2), 95–135.

The European Parliament and of the Council. (2016). DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, (194), L 194/1-30. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Wellman, B., & Gulia, M. (1999). Virtual Communities as Communities: Net surfers don't ride alone. In M. A. Smith & P. Kollock (Eds.), *Communities in cyberspace* (pp. 167–194). London: Routledge.

Wielgus, S. (2001). Odrodzenie wychowania. In T. Frąckowiak (Ed.), *Arytmia egzystencji społecznej a wychowanie* (pp. 43–60). Warszawa: Fundacja Innowacja : Wyższa Szkoła Społeczno-Ekonomiczna.