DOI https://doi.org/10.36059/978-966-397-182-7/106-120

FEATURES OF SECURING PERSONAL NON-PROPRIETARY RIGHTS TO LIFE AND HEALTH IN THE DIGITAL ENVIRONMENT

Manzhosova O. V.

INTRODUCTION

The process of development of a modern information society requires changes in scientific views and established doctrinal provisions in different areas of law. Public relations in the digital environment cannot be fully regulated. This requires a new comprehensive scientific exploration, analysis of new ideas and the development of legal concepts. In our opinion, the specificity of the manifestation of personal non-property rights in the digital environment, in particular the rights to personal security, deserves special attention. The right to personal security in the science of civil law is regarded as a kind of personal non-property right of an individual having the highest social value. The right to personal security is closely linked to fundamental human rights to liberty and security of person.

The current legislation of Ukraine, in particular the Civil Code, contains separate provisions on the regulation and protection of the individual's right to personal safety. The personal safety of an individual is, by its legal nature, a non-material benefit. Among the features of such a non-proprietary right, one should note the higher social value. The right to personal security is a variant of general human security and is aimed at protecting the private interest of an individual. The right to personal security is a state of protection of a particular individual from danger and is the antithesis of such legal category as risk [1] Given the significant number of threats to the rights of the individual in today's information society, it is necessary to intensify scientific research in a particular field.

1. The right to information security in the system of personal non-property rights of an individual

The analysis of the concept of personal security as a legal category should start with a general concept of security. Security is characterized as a state of protection of a person from external and internal threats. Thus, in particular, V.P. Vaskovskaya believes that the concept of "human security" in a generalized form means a degree of protection of a person, which ensures its sustainable development and is based on the activities of society,

[1] Стефанчук Р. Сучасні тенденції та перспективи розвитку права фізичної особи на особисту безпеку. *Вісник Національної академії прокуратури України*. № 4. 2008 р. С. 53–58.

guaranteed by the state, its bodies and officials to identify, prevent and eliminate the consequences of threats to human interests. On the other hand, in the narrow sense, human security is a stable state of reliable protection of vital (human life and health), legitimate and private human interests. Protection of her rights, freedoms and ideals, values against unlawful encroachments, threats and any harmful effects (physical, spiritual, property, informational, social, economic, political, environmental, military, etc.)[2].

O.A. Kolotkina notes that the concept of a person's right to security has a dual legal nature. On the one hand, it is a subjective right that characterizes the element of content of the general regulatory legal relationships that arise in connection with and about the security of each individual as a subject of law. From this perspective, the right of the individual to security as a legal category is natural and has its own meaning. On the other hand, the right of the individual to security is organically linked to such universally recognized fundamental rights and freedoms as the right to life, the right to liberty and security of person, other absolute and relative rights and freedoms. The right to security is in fact "embedded" in each of these rights. At the same time, the main focus is on the possibility of the realization of one's own rights and freedoms. Thus, there is every reason to argue that the right of the person to security is one of the basic elements of the whole modern system of human rights and freedoms, and therefore the legal system as a whole[3].

The purpose of the right to the personal safety of the individual must first and foremost guarantee the safety of the most fundamental, primary and non-renewable rights – the right to life and health[4].

Security is a system-forming category and may have a structural division depending on the area of interest it serves. By this criterion, we can distinguish such types of security as: national, political, economic, informational, legal, demographic, military, technical, environmental, nuclear, radiation, fire, sanitary-epidemiological, food, etc. Although the literature holds that all these varieties of security are included in the general concept of "personal security". However, according to R. Stefanchuk, this is a false statement and does not correspond to the content of the concept of security, where "personal security" is only one of its varieties[5].

---

[2] Васьковська В.П. Право людини на безпеку та конституційно-правовий механізм його забезпечення: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: 12.00.02. К., 2006. 20 с.

[3] Колоткин О. А. Право особистості на безпеку: поняття і механізми забезпечення в РФ: теоретико-правове дослідження: автореферат дисертації ... кандидата юридичних наук. Єкатеринбург. 2009. 21 с.

[4] Стефанчук Р. Сучасні тенденції та перспективи розвитку права фізичної особи на особисту безпеку. *Вісник Національної академії прокуратури України*. №4. 2008р. С. 53–58.

[5] Стефанчук Р.О. Особисті немайнові права фізичних осіб (поняття, зміст, система, особливості здійснення та захисту) : монографія. К. : КНТ, 2008. 626 с.

It should be noted that the personal safety of an individual is, by its legal nature, a personal non-material benefit, endowed with such characteristic features. First, it is of higher social value as a kind of general human security (Article 3 of the Constitution of Ukraine) and closest in nature to personal inalienable rights (the right to life, dignity, personal integrity). Without the right to security, it is impossible to think about the reality of the exercise of these rights. Secondly, it arises simultaneously with the appearance of personality; has an individual focus on a specific entity – an individual, and is aimed at protecting his or her private interest. This is the differentiated benefit from, for example, national security, where the subject is not a particular individual, but a collective entity – a nation. However, closely linked to these categories, with the security of the state and society, the collective rights of social communities are exercised. Third, it is a state of protection of a particular individual from danger[6]. Therefore, personal safety goes beyond personal physical security. This right is filled with the need to ensure the safety of the ecological, moral environment, social conditions of the person's realization of his biosocial nature[7].

In particular, in our opinion, it is worth talking about the right to information security of the individual, whose provision of modern conditions of development of information technologies and access to the Internet is relevant.

Today, a large number of scholars from different branch of law are investigating the problems of information security of the individual. It is possible to distinguish O. Zolotar's thorough research "Information security of the person: theory and practice" which among other things defines the right to a secure information environment is not only protection of information, but also protection from negative information influences[8].

The main features of information security are:

1) The existence of certain stable conditions in which society resides;

2) Protection of vital interests of being human, society, state;

3) Aiming to prevent harm to these interests;

4) Acknowledgment of existence of differences of interests of the person, society, the state;

5) Recognition of the mutual connection of the person, society, the state in the prevention of their harm;

[6] Ваганов П.А. Риск смерти и цена жизни. *Правоведение*. 1999. № 3. С. 67–68.; Ардашев А.І. Конституційні основи забезпечення безпеки особистості в Російській Федерації: автореферат дисер. наук. ступеня канд. юрид. наук. Москва, 2008. 21 с.

[7] Ардашев А.І. Конституційні основи забезпечення безпеки особистості в Російській Федерації: автореф. дисер. на здобуття наук. ступеня канд. юрид. наук. Москва, 2008. 21 с.

[8] Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

6) Achieving the goal on the basis of recognition of the harmony of interests of the person, society, state without giving preference to any of them;

Information security is a generic concept and covers such varieties as "cybersecurity", "real-time media security", etc.[9] [IT Law, p56]

In a certain aspect, it is not superfluous to note that significant threats to one's personal safety are those directly related to the physical and mental security of a person, which is a prerequisite for his quality of life. For example, it is a threat to the impact of low-quality information (untrue, false, misinformation) on the individual and society[10]. The realization of these threats leads to the violation of the most important absolute human rights and freedoms – for life, for health, for bodily integrity, respect for human dignity, for privacy, and so on[11].

2. Relationship between the right to information security and personal non-property rights to life and health

Some types of information threats in the digital environment can not only have a detrimental effect on the mental health of a social network user, but also cause significant tangible damage to his or her physical health or even life. These include the playback of potentially life-threatening and health-related actions taken by other Internet users (for example, dangerous flash mobs, games, chelens); self-medication based on online counseling or information posted on the Internet, etc.

Health information is increasingly available on the Internet. The number of websites with medical information is constantly growing. The number of Internet users who access such information is also increasing. There are many benefits of such a convenient and fast way to obtain health information, diagnosis and treatment. However, there are also a number of information threats to life and health that need to be identified and eliminated.

To date, there are three main ways to access medical information on the Internet: 1) search for medical information; 2) interaction with medical professionals; 3) participation in support groups (Cline and Haynes, 2001).

As you can see, there are several aspects to the problem of finding medical information on the Internet. First, it is of insufficient quality and reliability. In addition, medical information may be non-differentiated, incomplete, or misleading and may not have a scientific basis. Secondly, even

[9] ІТ-право:теорія та практика : навч.посіб. / авт. кол. ; заг ред Є.О. Харитонова, О.І. Харитонової. – 2-ге видан., виправлене та доповнене. – Одеса : Фенікс, 2019. – 475 с.

[10] Гуцу С. Ф. Правові основи інформаційної діяльності: навч. посібник Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін-т», 2009. 48 с.; Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL: http://www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf (дата звернення: 04.01.2020).

[11] Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

if it is correct and correct, it is not possible to control the correct interpretation and implementation of it by the Internet user. Improper self-diagnosis, self-selection of methods and treatments based on information posted on online sources can directly harm the health and even the life of a person.

The interactive nature of social media exacerbates these problems because anyone can download content to the site. In so doing, authors of medical information found on social media sites are often unknown or identified by limited information[12].

At present, it is impossible to assess the magnitude of the problem of poor quality medical information, as studies on this issue are not consistent. Although some authors believe that the quality of medical information on the Internet is poor (Doupi and Van der Lei, 1999; Latthe et al., 2000), others believe that it is of equal importance to information provided by other media (Sandvik, 1999 Hellawell et al. 2000). These controversial results are not surprising given the large number and variety of medical information sources on the Internet. Because of this problem, criteria for assessing the quality of health information on the Internet have been developed by several organizations (Eysenbach et al., 2000; Winker et al., 2000). These criteria take into account not only the content of the website (quality, reliability, accuracy, scale, etc.), but also the form (design, aesthetics, interactivity, use of the media, etc.), accessibility (fee for access, navigation, functionality, etc.), source reliability and privacy policies (Kim et al., 1999; Winker et al., 2000). So far, however, the impact of these criteria on the development and use of health information websites has been relatively weak, as they are subject to the good will of website designers and because users are unaware of them. Some research shows that using one of the most popular search engines (Google, AltaVista, Lycos, etc.) to search for information about a particular disease, only one in five links to a website with relevant information. Important information about each of the selected health issues is not available on most of the websites studied. This deficiency can adversely affect users' decisions. For example, lack of information about alternative treatments prevents users from making informed choices (Berland et al., 2001). In addition, although the information available is often valid, in many cases it is incomplete. Moreover, finding accurate health information can also be difficult, due to lack of usability and persistence (sites disappear and change without notice) (Cline and Haynes, 2001). Once the information has been found and assumed to be reliable and complete, users should understand it and bring it to life (D'Alessandro et al., 2001). Currently, most health information

[12] Lee C. Ventola Social Media and Health Care Professionals: Benefits, Risks, and Best Practices URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4103576/ (дата звернення: 06.01.2020).

websites provide technical information for people who are unfamiliar with the scientific medical literature[13].

Another problem with medical information posted on the Internet and the potential harm to the health of Internet users is the activity of pharmaceutical companies that can promote their products directly to consumers. Products can be advertised directly on company websites, in partnership with health information websites, or through banner ads on other websites. These new ways of disseminating medical information carry important risks of conflict of interest and drug overdose (Meyers, 2001). It is difficult for Internet users to distinguish between materials that promote drugs, as well as non-public information about health problems and their treatment. In addition, knowledge of different therapeutic alternatives allows patients to be more informed and make informed choices, but it may also make them insist on prescribing unnecessary or ineffective medicines. Finally, it is now possible to make more or less legal purchases online (such as Viagra), which can endanger human health through excessive consumption, dangerous products, drug interactions, etc. (deKieffer, 2000). Therefore, the danger is that the Internet can increase the use of health services and drugs without having a positive impact on the quality of care, disease prevention or health promotion[14].

Another way to access health information on the Internet is to interact with health professionals. Such information may be useful to the Internet user in certain circumstances. The dissemination of medical information on the Internet can facilitate the transfer of knowledge from healthcare professionals to the public and help people maintain and improve their health.

There are many social media tools available for healthcare professionals, including social media platforms, blogs, media sharing sites, and more. These tools can be used to improve or enhance professionalism, education, organizational assistance, patient care, patient education, and health care programs. However, they also present potential risks such as the dissemination of poor quality information, damage to professional image, breach of patient confidentiality, breach of personal and professional boundaries, and other ethical or legal issues.

Today, there are some ways to solve certain problems. This could be the implementation of a mechanism for directing Internet users to peer-reviewed sites with verified and reliable information. Yes, Так, HCPs can guide patients to credible peer-reviewed websites where the information is subject to quality control. The World Health Organization is leading a request to the Internet Corporation for Assigned Names and Numbers to establish a new domain suffix that would be used solely for validated health information.

[13] Benigeri M., Pluye P. Shortcomings of health information on the Internet URL: https://academic.oup.com/heapro/article/18/4/381/631899 (дата звернення: 04.01.2020).

[14] Ibid.

The issuance of this domain suffix would be strictly regulated, and the content of websites with these addresses would be monitored to assure compliance with strict quality criteria. These domain addresses would be prioritized by search engines when providing results in response to health-related inquiries[15].

Another type of information threat to a non-proprietary right of an individual is information that encroaches on the life of an Internet user and may result in death. However, it should be noted that this problem is complex and requires thorough scientific research by representatives of various fields of science. We will carry out preliminary scientific exploration and outline the general outlines of the problem.

To date, the immense amount of information on the topic of suicide is available on the Internet and via social media. Biddle et al.10 conducted a systematic Web search of 12 suicide-associated terms (eg, suicide, suicide methods, how to kill yourself, and best suicide methods) to simulate the results of a typical search conducted by a person seeking information on suicide methods. They analyzed the top 10 sites listed for each search, for a total of 240 different sites. Approximately half were prosuicide Web sites and sites that provided factual information about suicide. Prosuicide sites and chat rooms that discussed general issues associated with suicide most often occurred within the first few hits of a search. We should note that this study focuses primarily on prosuicide search terms and thus likely excludes many suicide prevention and support resource sites. Recupero et al.11 also conducted a study that examined suicide-related sites that could be found using Internet search engines. Of the 373 Web site hits, 31% were suicide neutral, 29% were anti-suicide, and 11% were prosuicide. The remaining sites either did not load or included "suicides" in the title but were not suicidal sites (e.g. movie sites and novels with "suicides" in their title or music bands whose names included "suicides"). Together, these studies have shown that obtaining prosuicide information on the Internet, including detailed information on suicide methods, is very easy[16]. As you can see, there are several factors behind the rise in Internet-induced suicides. These can be Cyberbullying and cyber harassment.

Cyber-billing is a specific concept for a specific category of activity that is covered by the general concept of billing. Cyber-billing is defined as any form of electronic communication, text messaging, instant messaging, websites and e-mail, repeated or extended over time that intimidates, degrades,

[15] Lee C. Ventola Social Media and Health Care Professionals: Benefits, Risks, and Best Practices URL:// https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4103576/(дата звернення 10.01.2020).

[16] David D. Luxton, Jennifer D. June, Jonathan M. Fairall Social Media and Suicide: A Public Health Perspective Am J Public Health. 2012 May; 102 (Suppl 2): S 195–200. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3477910/(дата звернення 05.01.2020).

harms physical or mental health, emotional well-being, honor , the dignity or reputation of another person.

Kowalski, Robin M., Limber, Susan P., Agatston, Patricia W. The following types of cyberbullying are distinguished:

1. Fights, or flaming – the exchange of short inflammatory cues between two or more people, which is usually deployed in public places on the Web;

2. Harassment attacks are repeated offensive messages directed at the victim (for example, hundreds of sms on a mobile phone, constant calls), with overload of personal communication channels. They also occur in chats and forums and online games;

3. Denigration – the dissemination of degrading false information. Text messages, photos, songs that are often sexual in nature;

4. Impersonation, impersonation – the persecutor positions himself as a victim by using his password to access an account on social networks, blogs, mail, instant messaging, or creates his account with a similar nickname and performs on behalf of the victim negative communication. Feedback waves are organized when letters of provocation are sent to friends from the victim's address without their knowledge;

5. Fraud, confidential information hijacking and outing & trickery – receiving personal information and posting it on the Internet or sending it to unauthorized persons;

6. Isolation. Any person has a desire to be a member of a group. Exclusion from the group is perceived as social death. The more a person is excluded from interaction, the worse he / she feels and the more his / her self-esteem falls. In a virtual environment, this can lead to complete emotional destruction of the child. Online alienation is possible in any type of environment where password protection is used, a spam list or friends list is formed. Cyber isolation is also manifested by the lack of response to instant messages or emails;

7. Cyber-harassment – the hidden tracking of a victim for the purpose of organizing an attack, beating, rape, etc.;

8. Hapisling (slap slap) – the name comes from cases in the London subway where bullies beat random passersby for laughing and raising their own status by recording it on a cellphone camera. Now so called any videos with recordings of actual scenes of violence that are subsequently posted on the Internet without the victim's consent[17].

Most often cyberbullying occurs in the environment of minors and minors, this phenomenon is quite typical for adults. Typically, cyberbullying is repeatedly caused by a person or group of individuals who have certain benefits (physical, psychological or administrative.) And is committed for the

[17] Kowalski, Robin M., Limber, Susan P., Agatston, Patricia W. Cyber bulling: bulling in the digital age. Oxford: Blackwell Publishing Ltd, 2008. 218 p.

purpose of intimidating or punishing something. From a psychological point of view, billing is a deliberately cruel, degrading treatment of a person or a long-term rejection of a person from a collective.

Cyberbullying, when directly or indirectly linked to suicide, has been referred to as cyberbullicide.

Suicide videos, suicide descriptions, and suicide practices can all be posted on the Internet in the public domain.

A recent study by Dunlop et al.specifically examined possible contagion effects on suicidal behavior via the Internet and social media. Of 719 individuals aged 14 to 24 years, 79% reported being exposed to suicide-related content through family, friends, and traditional news media such as newspapers, and 59% found such content through Internet sources[18].

Therefore, it can be noted that accessibility and speed of information dissemination on the Internet, lack of control over such information is a negative factor. This can encourage vulnerable people to commit suicide. Foreign experience can be used to solve the problem, including we also found examples of features on Web and social media sites that allowed for proactive prevention capabilities. For example, Google's Internet search engine has a feature that displays a link and a message about the National Suicide Prevention Lifeline at the top of the search page when keyword searches suggest suicidal ideation or intent (eg, "I want to die")[19].

When developing approaches to addressing the situation, the legal issues involved in monitoring and filtering the content of the Internet must be taken into account. Today, there are opposite approaches. There are supporters of the need to intervene and control the content of information. Their opponents believe that t content of information on the Internet will violate the freedom of speech and expression.

3. The problem is balancing the right to freedom of information and the right to life and health

One of the most difficult problems is securing the right to receive "secure" information from the Internet that does not endanger the life, physical and mental health of the individual. This right often conflicts with the right to freedom of expression and expression. Including through digital sources. Of course, it's easiest to talk about removing certain information from the Internet.

[18] Dunlop SM, More E, Romer D. Where do youth learn about suicides on the Internet, and what influence does this have on suicidal ideation? J Child Psychol Psychiatry. 2011;52(10):1073–1080. URL: https://psycnet.apa.org/record/2011-20427-008 (дата звернення 6.01.2020).

[19] David D. Luxton, Jennifer D. June, Jonathan M. Fairall Social Media and Suicide: A Public Health Perspective Am J Public Health. 2012 May; 102 (Suppl 2): S195–S200. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3477910/(дата звернення 10.01.2020).

In 2007, the Committee of Ministers of the Council of Europe adopted a Recommendation on promoting freedom of expression and information in a new information and communication environment, which emphasized the need to empower individual users with access to a new information and communication environment. At the same time, it was stated that "a fair balance must be struck between the right to express views freely and to share information in a new environment and respect for human dignity and the rights of others" (Committee of Ministers (26 September 2007), Recommendation CM / Rec (2007) 11 on promoting freedom of expression and information in new information and communication environments)[20].

However, the restriction rules remain the same according to the principle that "what is used offline should be equally applied online". In July 2012, this principle was endorsed by the Human Rights Council in its innovative Resolution on the Protection, Promotion and Promotion of Human Rights on the Internet (UN Human Rights Council (5 July 2012), Resolution A / HRC / 20/8 on the promotion , protection and enjoyment of human rights on the Internet) affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights; recognizes the global and open nature of the Internet as a driving force in accelerating progress toward development in its various forms; calls upon all States to promote and promote access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries; encourages special procedures to take these issues into account within their existing mandates, as applicable; decisions to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, the Internet and other technologies, as well as how the Internet can be an important tool for the development and exercise of human rights, in accordance with its program of work[21].

Guided by the commitments provided for in Article 19 of the International Covenant on Economic, Social and Cultural Rights, Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, stated in his important report for 2011 that how to impose any restriction on online content as an exclusive measure, such restriction by analogy to offline content must pass a three-stage, cumulative test:

[20] Бенедек В., Кеттеман М. Свобода вираження поглядів та Інтернет URL: https://rm.coe.int/168059936a. (дата звернення 6.01.2020).

[21] UN Human Rights Council (5 July 2012), Resolution A / HRC / 20/8 on the promotion, protection and enjoyment of human rights on the Internet URL : https://www.right-docs.org/doc/a-hrc-res-20-8/?path=doc/a-hrc-res-20-8 (дата звернення 6.01.2020).

1) it must be prescribed by law, comply with the principles of predictability and transparency. growth;

2) it must pursue one of the objectives set out in Article 19 of the International Covenant on Economic, Social and Cultural Rights, namely: the protection of the rights or reputation of others, the protection of national security or public interest, the protection of health or morals;

3) it must be both necessary and least restrictive in order to achieve the relevant objective (the principle of proportionality). In addition, legislation that establishes appropriate restrictions should be applied by an independent body reasonably and in a non-discriminatory manner, and there should be adequate safeguards against abuse when applying such legislation[22].

Therefore, a person has the right to seek, receive and impart information and ideas of his choice without any interference and regardless of national boundaries. This means that: 1. a person can speak freely on the Internet and have access to other people's information, views and opinions. These include political statements, religious beliefs, attitudes, and expressions that are favorably or offensively considered, and that may offend, shock, or drive others out of balance. In doing so, the individual must give due consideration to the reputation and rights of others, including their right to privacy; 2. Restrictions may be imposed on such statements that call for discrimination, hatred or violence. Such restrictions should be lawful, purposeful and enforceable; 3. A person should be aware that content he or she creates on the Internet, or content about the person created by other Internet users, can be made accessible in any corner of the world and harm your dignity, safety, privacy or otherwise. harm you and your rights at this time or in the next stages of your life. At the request of the individual, such content must be removed or removed within a reasonably short period of time; 4. You can expect to have clear information about what online content and behavior is illegal (eg, harassment on the Internet), and be able to report potentially illegal content. Such information should be tailored to the age of the person and circumstances, and should be provided with advice and support with due respect for confidentiality and anonymity; 5. a person should be given special protection against interference with physical, mental and moral well-being, in particular protection against sexual exploitation and violence on the Internet and other forms of cybercrime[23]

The rules of national law duplicate international provisions. The current Constitution of Ukraine enshrines the right to freedom of information and

[22] La Rue F. Report of the Special Rapporteur on freedom of opinion and expression, § 69. URL : https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session26/Documents/A-HRC-26-30-Add2_en.doc (дата звернення 9.01.2020).

[23] Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів та пояснювальний меморандум) URL : https://rm.coe.int/16802e3e96 (дата звернення 09.01.2020).

details it in the Law of Ukraine "On Information". Thus, Article 2 of this Law establishes the following principles of information relations: guarantee of the right to information; openness, accessibility of information, freedom of information exchange; accuracy and completeness of information; freedom of expression and beliefs; the lawfulness of obtaining, using, disseminating, storing and protecting information; protection of a person from interference with his or her personal and family life. On the same principles, the state information policy is built, the main directions of which are: ensuring access of everyone to information; ensuring equal opportunities for creating, collecting, receiving, storing, using, distributing, protecting, protecting information; creating conditions for the formation of an information society in Ukraine; ensuring the openness and transparency of the activities of the authorities; creation of information systems and networks of information, development of e-government; continuous updating, enrichment and storage of national information resources; ensuring information security of Ukraine; promoting international cooperation in the information field and Ukraine's entry into the world information space (Article 3).

The law guarantees the protection of the right to information by ensuring equal access to information for all subjects of information relations. No one may restrict the rights of a person in the choice of forms and sources of information, except as provided by law. The subject of information relations may require the elimination of any violation of his right to information. At the same time, abuse of the right to information is assumed to be inadmissible. The information cannot be used to call for the overthrow of the constitutional order, violation of the territorial integrity of Ukraine, propaganda of war, violence, cruelty, incitement of interethnic, racial, religious hatred, acts of terrorism, violation of human rights and freedoms[24].

So, how is the balance between a person's right to free access to the Internet and the right to eliminate information threats to his or her life and health? The protection of a person's right to life can be ensured by a series of measures. As you can see, it is impossible to do it by technical means alone.

On the other hand, the formation of a conscious perception of information posted on the Internet is promising for the individual and for society as a whole. This will allow her to be critical of such information. In view of this, it is worth noting that in the scientific literature, for today, the concept of "information hygiene" of a person is being formed as a prevention of information threats.

Information hygiene studies the regularities of the influence of information on the mental, physical and social well-being of a person, his work capacity, life expectancy, public health of society, develops standards

[24] Про інформацію : Закон України від 02.10.1992. *Відомості Верховної Ради України* . 1992. № 48. Ст. 65.

and measures for improving the information environment and optimization of intellectual activity. The main tasks of information hygiene: 1) study the characteristics and patterns of information media, processes and flows, perception, processing, storage and production of new information, the dependence of individual and public health on information; 2) definition of hygienic standards of information, information environment, information networks and processes, scientific substantiation of hygienic information behavior; 3) development of sanitary measures for the organization of information networks and processes, hygienically sound production, distribution, consumption, storage, reproduction of information; 4) development of measures for optimization of information and intellectual activity[25] Adherence to the principles of personal information hygiene can help effectively address the issue of protecting one's personal non-property rights to life and health from information threats.

CONCLUSIONS

Creating a secure information environment and protecting a person from information threats requires a sound approach. It is necessary to develop a comprehensive national strategy on this issue, which will cover all spheres of public life. A separate direction could be an inclusive education company that would increase the level of awareness of individuals about their rights and freedoms in the information society, the possibility of protection against information threats. It is also necessary to formulate in society an understanding of the need to "self-censor" information that a person places openly.

SUMMARY

The article deals with the specifics of securing personal non-property rights in the digital environment, including the right to personal security. The right to personal security is regarded as a kind of personal non-property right of the individual having the highest social value.

The right to information security of the individual is analyzed. The concepts and features of information security are considered. Particular attention is paid to the threats to personal security that encroach on the absolute rights and freedoms of man – life, health, bodily integrity, respect for human dignity, privacy, etc.

The article explores some types of information threats that can have adverse effects on the mental health of an Internet user and cause permanent damage to their physical health and life. These include reproduction of potentially life-threatening and health-related activities by other Internet users (such as dangerous flash mobs, games, challenges); self-medication based on online counseling or information posted on the Internet, etc.

[25] Молодцова И. А., Максимова Е.А., Сливина Л.П. Информационная гигиена: общетеоретическая оценка проблемы инновации в информатике. *НБИ технологии.* Волгоград, 2018. Т. 12. № 2. С. 25–29.

The advantages and disadvantages of free access of the internet users to medical information are outlined. Increasing effectiveness of interaction with skilled healthcare professionals on the Internet was noted.

The problems of balance between the right of a person to free access to the Internet and the right to eliminate information threats to his life and health are analyzed. The necessity of realization of a set of measures for formation in the society of conscious perception of information placed on the Internet is noted.

REFERENCES

1. Стефанчук Р. Сучасні тенденції та перспективи розвитку права фізичної особи на особисту безпеку. Вісник Національної академії прокуратури України. №4. 2008р. С. 53–58.
2. Васьковська В.П. Право людини на безпеку та конституційно-правовий механізм його забезпечення: автореф. дис. на здобуття наук, ступеня канд. юрид. наук: 12.00.02. К., 2006. 20 с.
3. Колоткин О. А. Право особистості на безпеку: поняття і механізми забезпечення в РФ: теоретико-правове дослідження: автореферат дисертації ... кандидата юридичних наук. Єкатеринбург. 2009. 21 с.
4. Стефанчук Р.О. Особисті немайнові права фізичних осіб (поняття, зміст, система, особливості здійснення та захисту) : монографія. К. : КНТ, 2008. 626 с.
5. Ваганов П.А. Риск смерти и цена жизни. Правоведение. 1999. № 3. С. 67-68.; Ардашев А.І. Конституційні основи забезпечення безпеки особистості в Російській Федерації: автореферат дисер. наук. ступеня канд. юрид. наук. Москва, 2008. 21 с.
6. Ардашев А.І. Конституційні основи забезпечення безпеки особистості в Російській Федерації: автореф. дисер. на здобуття наук. ступеня канд. юрид. наук. Москва, 2008. 21 с.
7. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
8. ІТ-право:теорія та практика : навч.посіб. / авт. кол. ; заг ред Є.О. Харитонова, О.І. Харитонової. – 2-ге видан., виправлене та доповнене. – Одеса : Фенікс, 2019. – 475 с.
9. Гуцу С. Ф. Правові основи інформаційної діяльності: навч. посібник Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін.-т», 2009. 48 с.; Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL: http://www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf (дата звернення: 04.01.2020).
10. Lee C. Ventola Social Media and Health Care Professionals: Benefits, Risks, and Best Practices URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4103576/.

11. Benigeri M., Pluye P. Shortcomings of health information on the Internet URL: https://academic.oup.com/heapro/article/18/4/381/631899.

12. David D. Luxton, Jennifer D. June, Jonathan M. Fairall Social Media and Suicide: A Public Health Perspective Am J Public Health. 2012 May; 102 (Suppl 2): S 195–200. URL:https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3477910/(дата звернення 05.01.2020).

13. Kowalski, Robin M., Limber, Susan P., Agatston, Patricia W. Cyber bulling: bulling in the digital age. Oxford: Blackwell Publishing Ltd, 2008. 218 p.

14. Dunlop SM, More E, Romer D. Where do youth learn about suicides on the Internet, and what influence does this have on suicidal ideation? J Child Psychol Psychiatry. 2011;52 (10):1073–1080. URL: https://psycnet.apa.org/record/2011-20427-008 (дата звернення 6.01.2020).

15. Бенедек В., Кеттеман М. Свобода вираження поглядів та Інтернет URL: https://rm.coe.int/168059936a .(дата зверення 6.01.2020).

16. UN Human Rights Council (5 July 2012), Resolution A / HRC / 20/8 on the promotion, protection and enjoyment of human rights on the Internet URL : https://www.right-docs.org/doc/a-hrc-res-20-8/?path=doc/a-hrc-res-20-8 (дата звернення 6.01.2020).

17. La Rue F. Report of the Special Rapporteur on freedom of opinion and expression, § 69. URL : https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session26/Documents/A-HRC-26-30-Add2_en.doc (дата звернення 9.01.2020)

18. Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів та пояснювальний меморандум) URL : https://rm.coe.int/16802e3e96 (дата звернення 09.01.2020).

19. Про інформацію : Закон України від 02.10.1992. Відомості Верховної Ради України. 1992. № 48. Ст. 65.

20. Молодцова И. А., Максимова Е.А., Сливина Л.П. Информационная гигиена: общетеоретическая оценка проблемы инновации в информатике. НБИ технологии. Волгоград, 2018. Т. 12. № 2. С. 25–29.

Information about the author:
Manzhosova O. V.,
Candidate of Law, Associate Professor,
Head of the Department of Civil Law Disciplines,
Chernivtsi Law Institute of the National University
"Odessa Law Academy"
7, Skovorody str., Chernivtsi, 58000, Ukraine
ORCID ID https://orcid.org/0000-0002-8873-4783