DOI 10.24147/2542-1514.2020.4(4).80-93

THE FREEDOM OF SPEECH AND RIGHT OF ACCESS TO INFORMATION IN THE EMERGING SYSTEM OF INTERNATIONAL INFORMATION SECURITY**

Ksenia A. Ivanova[1,2], Madi Zh. Myltykbaev[3]
[1] *Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia*
[2] *University of Tyumen, Tyumen, Russia*
[3] *MGIMO University, Moscow, Russia*

Article info
Received –
2020 July 19
Accepted –
2020 November 16
Available online –
2020 December 30

Keywords
Freedom of speech, right to access information, information and communication technologies, international information security, information security, information technologies, information threats, cyber threats, cyber space

The subject. The article is devoted to the analysis of the freedom of speech and access to information in the context of the emerging system of international information security.
The purpose of the article is to try to predict the positive and negative consequences of changing international relations in the digital age, to determine the role of freedom of speech and access to information in the context of confrontation between Russia and the United States.
The research presented in this article was carried out by combining different disciplinary approaches, including comparative law, comparative politics and international relations, political theory and sociology. Moreover, study includes methods of dialectical logic, analysis and synthesis, as well as formal legal analysis of international legal acts of the UN.
The main results and scope of their application. The rights of freedom of speech and access to information is undoubtedly one of the main in the global digital communication context.

Degree of implementation of human and citizen rights to freedom of expression and access to information are indicators of political processes, the pace of building a civil society and legal state in current country. These rights are the foundation of modern democracy.
The authors carry out a systematic analysis of the categories "freedom of speech" and "the right to access information", identify the features of implementation of these rights in cyberspace, analyze international practice of legal regulation of these rights and assess the place and role of these rights in the emerging system of international information security. A legal analysis of international legal acts shows that the positions of the United States and the Russian Federation in the field of international information security are gradually converging, and the convergence is going in the direction of the Russian position
Conclusions. The limits on the exercise of freedom of speech and access to information do not correspond to the level of development of public relations, because there are no effective legal tools to prevent defamation in the mass media, which in turn can lead to conflict between countries. It is concluded that there is a need for active international cooperation and consistent unification of the legislation of various countries, taking into account that freedom of speech and access to information in cyberspace should have the same level of protection as in the physical world.

** The article was funded by RFBR according to the research project № 18-29-16204 мк.

1. Introduction

Rights and freedoms, including freedom of speech and the right to access information, are not a fixed category. They are a product of the historical development of society, they represent a socio-cultural phenomenon, reflect the historical identity of peoples and countries of the world, so each legal system of the world has its own legal concept of rights and freedoms.

In the context of global digital communication, the issue of freedom of speech and access to information is undoubtedly one of the main ones. So, the degree of realization of human and citizen rights to freedom of expression and access to information to judge the events in the country political processes, to assess the pace of building a civil society and legal state. These rights are the Foundation of modern democracy.

Freedom of speech and the right of access to information are of particular importance in the light of rapidly increasing challenges and threats in the information environment in the context of the formation of a bipolar system of international information security, confrontation, and the struggle for a safe and stable world. Under these conditions, these rights, which are intended to serve as the core of ideological pluralism, are transformed into an instrument of propaganda that organizes confrontation, creates a threat to international security, and cultivates an atmosphere of hostility and hatred between States and peoples.

Based on this context, we will consider the nature and role of freedom of speech and the right of access to information in the emerging system of international information security, the importance attached to them by the subjects of international relations.

2. Transformation of freedom of speech and the right to access information.

The history of civilization is inextricably linked with the history of international relations. The formation of the UN in 1945 marked the beginning of modern civilization, became the starting point of modern international law, which set the vector of development for democratic legal social States, the core of which is civil society - the most important element of the social mechanism that ensures the realization of human rights. Civil society will not function without freedom of speech and access to information, including the right to create mass media for the purpose of expressing opinions, the free search for information [1, p. 9] and its further dissemination, and the prohibition of censorship.

Given the above, the period from the adoption of the universal Declaration of human rights in 1948 to the formation of the system of international information security at the present time is relevant for the study of the transformation of freedom of speech and the right to access to information.

This period can be divided into three stages of mastering the problem of freedom of speech and access to information.

The first stage can be called declarative. This period is determined by the content, clarifies wording and concepts, and by the end of the XX century "the issue of freedom of speech thanks to the painstaking work of scientists, diplomats and officials became deeply developed concept, presented in dozens of Conventions and the UN Declarations that do not depend on state boundaries and is universal" [2]. The universal Declaration of human rights (UDHR) of 1948 was the first international document to enshrine the rights in question. Thus, article 19 of the UDHR proclaims: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and freedom to seek, receive and impart information and ideas by any means and regardless of frontiers."

The next international act in time, but not in importance, is the Convention for the protection of human rights and fundamental freedoms (hereinafter – the ECHR) of 1950. Article 10 of the ECHR follows the article 19 of the UDHR and adds that the exercise of these freedoms "may be subject to certain formalities, conditions, restrictions or penalties prescribed by law and are necessary in a democratic society in the interests of national security, territorial integrity or public order, the prevention of disorder or crime, for the protection of

ISSN 2542-1514 (Print)

health or morals, protection of reputation or rights of others, prevent the disclosure of information received confidentially, or supporting the authority and impartiality of justice". There is also a mechanism that prevents the abuse of these restrictions. Article 17 clarifies that nothing in the ECHR "may be interpreted as meaning that any state, any group of persons or any person has the right to engage in any activity or to perform any action aimed at abolishing or restricting the rights and freedoms recognized [in the ECHR] to a greater extent than is provided for [in the ECHR]".

International Covenant on civil and political rights (hereinafter – ICCPR) of 1966 is a clear example of consensus in the context of intensified ideological confrontation in the international arena. The wording is widely interpreted in the ICCPR due to the lack of a mechanism to prevent the abuse of restrictions, the human rights Committee is formed. Article 19 of the ICCPR provides as follows:

"1. Everyone has the right to hold opinions without interference.

2. Everyone has the right to freedom of expression; this right includes freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or through the press or artistic forms of expression, or by other means of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article imposes special duties and responsibilities. It may therefore be subject to certain restrictions, which, however, must be established by law and are necessary:

a) to respect the rights and reputations of others;

b) for the protection of state security, public order, public health or morals."

As highlighted in paragraphs 18 and 19 of the Human Rights Committee's General comment No. 34, freedom of expression includes the right to access information held by public authorities.

The final international act of the first stage can be considered the Charter of fundamental rights of the European Union of 2000, article 11 of which ("Freedom of expression and freedom of information") provides that everyone has the right to freedom of expression, including freedom to hold opinions, to receive and impart information and ideas without interference from state bodies and regardless of state borders. It is added that the freedom and pluralism of the media must be respected.

The second stage is characterized by the development of law enforcement practice. At this stage, the limits of the exercise of freedom of speech and the right of access to information in the practice of international and national courts are being calibrated and clarified. Despite the fact that determining the relationship between rights and freedoms, on the one hand, and other competing interests, on the other, is a daily function of national and international courts, there is no unambiguous answer to the question of freedom of speech and access to information. Defining the limits of freedom of expression under article 10 of the ECHR is particularly difficult when it comes to preventing violence.

It should be noted that the decisions of the European courts are among the most motivated. Naturally, international norms have been most developed in the practice of the European court of human rights (hereinafter – the ECHR).

Article 10 of the ECHR ("Freedom of expression") is broadly interpreted by the ECHR, in whose practice several related freedoms are enshrined: freedom of speech, freedom of access to information, freedom of dissemination of information. Here are some current examples of court cases on freedom of speech (Ali Gürbüz V. Turkey, 52497/08 et al., 12 March 2019 ; Margulev V. Russia, 15449/09, 8 October 2019), freedom of access to information (Rodionov V. Russia, 9106/09, 11 December 2018; Sedletska V. Ukraine, 42634/18), freedom of information dissemination (Szurovecz V. Hungary, 15428/16, 8 October 2019; Brisc V. Romania, 26238/10, 11 December 2018).

We also note that the issue of freedom of expression has always occupied a special place in the European legal system. Here are some examples of the ECtHR's consideration of disputes related to the exercise of this freedom in 2002 alone: Dischand and Others V. Austria, 29271/95, 26.02.2002; McVicar V. United kingdom, 46311/99, 07.05.2002; Nikula V. Finland, 31611/96, 21.03.2002 [3, pp. 841-846].

We should also note that, despite the fact that the practice of the ECHR is subsidiary to national jurisdictions, it is a "guiding star" in matters of compliance with human rights standards.

ISSN 2658-4050 (Online)

Thus, in April 2014, the Turkish constitutional court ruled that the blocking of access to Twitter by the Turkish government is a violation of freedom of expression in accordance with article 26 of the Turkish Constitution and the jurisprudence of the ECHR, which provides that fundamental rights and freedoms can only be restricted by law without prejudice to their essence and provided that such restrictions should not contradict the democratic structure of society and the principle of proportionality. In a subsequent decision, the Turkish constitutional court overturned the order of the Turkish authorities to block access to YouTube based on the same judgments of the ECHR [4, p. 85].

The third stage is characterized by penetration into all spheres of life of the Internet and, as a result, a rapid increase in the number of challenges and threats in the information sphere. The international community was faced with the issue of developing rules of conduct. Freedom of speech and the right to access information in the digital age are the most relevant and have an absolute priority of protection. In modern conditions, the right to access information is primary, since without information, the implementation of most other rights and freedoms is difficult. The right to access information can be considered as the right to freely receive and disseminate data and thoughts independently, that is, without state intervention. In jurisprudence, this right is often referred to as the "right to know". It is worth noting that this right should be exercised not only without the intervention of the authorities, but also without taking into account state borders.

Undoubtedly, the realization of the right to" know", designated in the middle of the last century, in practice has become fully possible only in our time. The reason for this is the rapid development of modern information and communication technologies (hereinafter – ICT), before the appearance of which these rights were only declarative in nature.

It is worth noting that the right of access to information in the ICCPR covers both the receipt and dissemination of information, as well as the search, use and dissemination of data, including orally, in writing, through print, artistic forms of expression or other methods of the person's choice.

Without the current communication technologies, means of communication and the Internet, it is difficult to imagine how a person could independently receive and distribute and, moreover, extract any information so easily and freely. Of course, only on the basis of modern ICTs can there be conditions that allow a person or society as a whole to realize the right to access information. However, one of the negative manifestations of Informatization was the use of digital space for terrorist and extremist purposes [5, p. 15].

Based on the above context, freedom of speech and the right to access information acquire a special place in the system of international information security. They are both the cornerstone of the emerging new international relations, and a bone of contention, becoming an instrument of interference in the internal Affairs of States, violations of the sovereign rights of peoples [6, p. 3].

3. Bipolar system of international information security.

For the first time in 1998, the 53rd session of the UN General Assembly (hereinafter-the UNGA) adopted a resolution calling on States to consider at the international level existing and possible threats in the field of information security. According to the Secretary Of the Security Council of the Russian Federation N. P. Patrushev, "this was the first step towards the formation of an international information security system designed to counter threats to strategic stability and promote equal strategic partnership in the global information space" [7, p.11].

The problem of ensuring international information security has brought the ideological confrontation between the countries of Western democracy and the rest of the world to a new level, and has become the impetus for the formation of a bipolar system in this area. The international community has expressed concerns about the continuing expansion of the information gap, the "arms race" in the information and communication technologies environment. It is this gap that is the main cause of instability and conflict, which can easily transform into a global confrontation. Information and communication technologies are

ISSN 2542-1514 (Print)

cross-border, global in nature, and therefore require special international regulation [8, p. 343].

Today, within the framework of the UN, there are two relevant approaches to the issue of international information security, which are proposed by Russia and the United States. These initiatives have led to the polarization of international relations.

Today, the development of a consensus between Russia and the United States in building international information security is the key to a secure world. Let's compare these approaches and determine the role of freedom of speech and the right of access to information in them.

4. Assessment of the role and importance of information and communication technologies at the present stage of historical development

Comparing the positions of the United States and the Russian Federation on the formation of an international information security system is advisable to start with an international assessment of the role and importance of information and communication technologies in the development of the world economy, science and culture. The international community is showing complete unity on this issue. Analysis of the UN General Assembly resolutions, reports of governmental experts on developments in the field of information and telecommunications in the context of international security (1st UN Committee), reports of the UN Secretary-General clearly indicate the extremely important role of information and communication technologies in shaping the current level of development of civilization.

In particular, UN resolutions 74/28 and 74/28A of 12 December 2019, after noting the fact of intensive deployment of the latest information technologies and telecommunications, confirm that this process contains significant new opportunities for accelerated progress in all areas of the economy, science and culture. At the same time, the potential for interaction between States aimed at their common good is also growing. Similar assessments of the role of information and communication technologies are present in documents not only of the UN, but also of various regional international associations: ASEAN, OECD [9].

The conclusion about the unanimous recognition by all countries of the extremely important role of information and communication technologies in the further development of the global community is not in doubt, but it should be noted that the international community is equally United in recognizing the existence of a number of negative consequences of the development of such technologies [10, p. 85]. We are talking, first of all, about such relatively new phenomena as cybercrime, cyberterrorism, cyber attacks and cyber threats. The us President's Executive orders recognize cyber threats to critical infrastructure as one of "the most serious national security challenges we face." The facts related to these phenomena began to attract the attention of the international community relatively recently - in the period 1990-1996, but the scale of threats grew so rapidly that in 1998 the problem first entered the UN agenda . Since 2009, the permanent "group of governmental experts on developments in the field of information and telecommunications in the context of international security"has already worked in this organization.

In the first report of the group, it is recorded that the existing and possible threats in the field of information security should be considered the most serious problems of the XXI century. The list of sources of such threats is indeterminate, and their manifestation is subversive activities against individuals and legal entities, national governments and infrastructures. In the event of threats, there is a significant damage to the security and stability of not only individual countries, but also the international community as a whole due to reactions in the global network. The spread of information and communication technologies inevitably leads to the emergence of new vulnerabilities in critical infrastructure and unexpected options for disruptive actions [11, p. 129]. Due to the specifics of modern telecommunications and the Internet, each element of information and communication technologies can be a source or object of high-tech attacks. Moreover, the specifics of these technologies are such that not only the means of storing, processing and transmitting information can have a dual purpose, but the means of protection can create threats to international peace and security both on a global and national scale [12, p.18].

ISSN 2658-4050 (Online)

The dual purpose and significant risk of threats arising from the malicious use of information and communication technologies have been clarified in each report of the group of governmental experts. In General, since 2010, no session of the UN General Assembly has completed its work without the adoption of resolutions containing paragraphs on the threats associated with the use of such technologies. If we add to this the presence of similar formulations in documents at the regional level: resolutions of the Council of Europe and the European Parliament, the European Union Agency for cybersecurity and cybersecurity certification, decisions of the NATO Warsaw summit, documents of the inter-American Committee of the OAS, as well as the responses of States cited in the report of the UN Secretary-General, then the conclusion about the international recognition of the dual nature of information and communication technologies and the significant danger of threats associated with them is fully confirmed [13, p. 127]. This conclusion, despite its apparent simplicity and obviousness, is of fundamental importance for the processes of formation of the international legal system for ensuring information security. Without the recognition of dual-use information and communication technologies, the question of the legality of their use as weapons and the qualification of such use from the standpoint of the relevant norms of international law cannot be raised.

Summing up all the above, it should be emphasized that there is no significant disagreement in the international community on the role and significance of information and communication technologies, their dual nature, the possibility of using them as weapons, and related threats. Accordingly, the positions of USA and Russia here also coincide, which explains the identical paragraphs in the draft resolutions of the UN, the US and Russia. Disagreements and contradictions appear at the level of concepts for ensuring international and national security in the context of the global application of information and communication technologies.

5. Contradictions in the definitions of information and cybersecurity.

The contradictions between Russia and the USA in security definitions related to the use of information and communication technologies are not related to contradictio in adjecto – a classic logical error which consists in the contradiction between determined and determining. On the contrary, each of the parties offers its own rather logical formulations, but, nevertheless, the difference between them is significant and leads to far-reaching consequences [14, p.8].

The United States defines the phenomenon known in the Russian Federation as "information security" in the form of security structures for storing, processing and transmitting information (data) [15]. Accordingly, in the US Federal law, the term "cybersecurity" is used to refer to this concept, which refers to the protection of information systems from unauthorized access, use, destruction, as well as the protection of information from disclosure, destruction, modification or destruction. In US Federal law, the term "information security" is also used, but has a completely different meaning. It is understood as the security of citizens, provided by a sufficient level of information about all actions of the Executive power . Control in this area is provided by a specially created Agency for this purpose – Information Security Oversight Office (ISOO), while cybersecurity is handled by the national infrastructure Advisory Council (NIAC) . Thus, in the US legal system, the terms "information security" and "cybersecurity" are not synonymous and refer to different phenomena.

This approach has an important feature. The concept of "cybersecurity" is much narrower than "information security". It covers only aspects of the health of the technical infrastructure and the integrity of the transmitted, stored and processed data. As for the data itself, it is considered that they cannot be a threat if they do not damage cyber structures and do not lead to a violation of the integrity and established procedure for processing other data. In other words, if information from global cyberspace does not cause any physical or financial damage, then its dissemination is not a malicious influence, and the source of such disclosure cannot be accused of malicious actions, which accordingly eliminates the risk of becoming a target for retaliatory measures available to the UN.

ISSN 2542-1514 (Print)

It is necessary to recognize that the same content is invested in the concept of "information security" not only by the United States, but also by a number of mainly European countries. At the same time, arguments are expressed in favor of this interpretation, which are not conditioned by allied or political considerations. In particular, France's response to the UN Secretary-General contains the following clarifications: "France does not use the term" information security", preferring the term" information system security", or "cybersecurity". This choice is due to the fact that France, as an active supporter of freedom of expression on the Internet (as evidenced by the fact that in 2018 it co-sponsored human rights Council resolution 38/7), does not believe that information itself can be a vulnerability factor from which it is necessary to protect itself, without prejudice to measures that can be taken on a proportionate and transparent basis under conditions strictly defined by the legal framework, in accordance with article 19 of the ICCPR. Briefly, the meaning of this approach can be expressed as follows: even unpopular or divisive speech should be protected by the right to freedom of speech [16, p. 294].

The term "cybersecurity" is more precise, since it refers to the ability of an information system to resist phenomena from cyberspace that compromise the availability, integrity and confidentiality of stored, processed or transmitted data and related services that are available in these systems or to which these systems provide access. Cybersecurity is based on methods of ensuring the security of information systems and is supported by the fight against cybercrime and the creation of a cyber defense system [17, p. 64].

This position is typical for the countries of North America and European countries that are members of the European Union. It is not devoid of grounds from the field of international law, but at the same time provides enough arguments for criticism also from the standpoint of international law. In particular, reference to paragraph (b) of part 3 of the same article 19 of the ICCPR shows a whole set of cases where information is harmful and dangerous in itself, and its dissemination should be restricted by law. A clear example is that the anonymity provided by THE tor (the Onion Router) system, created for the private use of the Internet, has allowed some criminal groups to create sites with illegal content that offer prohibited services and products for sale. The new software interacts with darknet sites such as Silk Road ("silk road" is an anonymous online trading platform, most of the goods sold on it are illegal. It is best known as a platform for the sale of prohibited psychotropic substances, which accounted for 70 % of the total mass of goods offered) [4, p.86].

Supporters of the US position persistently promote their point of view in the international community. An example is paragraph 1 (b) of draft resolution 74 of the UN General ASSEMBLY session. It calls on States to: "support the implementation of joint measures identified in the reports of the Group of governmental experts to address threats arising in this area and to ensure an open, interoperable, reliable and secure information and communication environment, based on the need to maintain the free flow of information."

Of course, we should not forget that the Internet was originally created for the free, cross-border exchange of information, and the right to free expression of ideas and opinions is one of the basic, fundamental and universally recognized human and civil rights. The right to freely Express one's opinion includes the right to receive and disseminate information and ideas without any interference from public authorities and regardless of state borders, as well as the opportunity to Express one's opinion and communicate it, as a set of information, to another subject, who, in turn, has the right to receive this information [18, p. 141]. On March 9, 2015, the Parliamentary Office of Science and Technology (POST), which advises the UK Parliament, published a report entitled "Darknet and online anonymity", which States that a ban on online anonymity of the network would be "technologically unworkable" and counterproductive. If the ban were imposed, an anonymous network such as Tor Hidden Services (THS) would simply add secret entry nodes or "bridges" that are "very difficult to block." The report also says that the anonymous network is used not only for criminal purposes, but also to protect public interests, such as information, journalism, law enforcement investigations and circumventing censorship on the Internet [4, p.86].

In the context of this article, it is important to note the use of the term "information and

ISSN 2658-4050 (Online)

communication environment" in the draft resolution instead of the traditional term "cyberspace" for the US position. Such a change may well be interpreted as a" drift" towards the position of the Russian Federation that is more relevant to modern reality. However, the key element of this paragraph of the draft resolution is not a change in terminology, but the requirement to preserve the free flow of information. It is this part that guarantees the protection of any content sent by a state to a sovereign part of the information and communication environment of another state. The presence of such a provision in the UN General Assembly Resolutions will allow the United States not to support measures against States that broadcast content using information and communication technologies aimed at destabilizing the situation in other States. In addition, and this seems to be extremely important, this approach saves the United States in the future not only from condemnation, but even from considering actions taken against other States in the information and communication environment. The position in which the main thing is the free flow of information, in the legal sense, "frees hands" to conduct actions in the information environment that are not compatible with the maintenance of peace and stability [19, p.191]. The only condition for the legitimacy of such actions (again, according to the United States and its allies) is the absence of damage to cyber structures. With regard to this condition, it should be noted that it is not a difficult and insurmountable obstacle. First, the damage is difficult to prove (Russia consistently demands to avoid unsubstantiated accusations), and secondly, the infliction of such damage, especially in relation to critical infrastructure, is advisable only in the case of an open conflict with the use of force. In other cases, as international experience shows, specially prepared content sent to the information environment using information and communication technologies is sufficient for destabilization [20].

The position of the Russian Federation is also largely determined by the content invested in the concept of "information security". In accordance with the adopted Doctrine of information security of the Russian Federation, this concept is defined as "the state of protection of the individual, society and the state from internal and external information threats, which ensures the implementation of constitutional rights and freedoms of man and citizen, decent quality and standard of living of citizens, sovereignty, territorial integrity and sustainable socio-economic development" [21]. In accordance with this definition, any actions in the sovereign part of the information space that lead to the listed consequences should be considered directed against the information security of the country. This, in turn, gives the state the right to respond appropriately, since sovereignty and the international norms and principles that follow from it apply to activities related to information and communication technologies and to the corresponding infrastructure located on the territory of the state, and therefore they are subject to the jurisdiction of the state . Moreover, in such cases, it is theoretically possible to appeal to the UN security Council, since modern threats to international peace and security are not necessarily related to the use of armed forces. Under article 39 of the Charter of the United Nations, the determination of any threat to peace is within the authority of the UN Security Council. The UN security Council has already recognized that threats in the "economic, social, humanitarian and environmental fields" can be considered as threats to international peace and security [22].

Next, we will outline an important point that largely reveals the essence of the Russian position in the field of international information security. Information attacks and retaliatory measures mean that there is a conflict, and the probability of such conflicts increases. Preventing such conflicts is a major task of the international community. To solve this problem, reasonable measures are needed to prevent conflict situations in the information space. The Russian interpretation of the concept of "international information security" gives a clear answer to this question. In particular, States, using information and communication technologies, should not allow damage to the information systems of other States, interference in the internal Affairs of other States by generating and broadcasting content that carries threats, contains hostile propaganda and insults. In General, States must comply with a number of rules of responsible behavior in the information space. Such requirements and rules

ISSN 2542-1514 (Print)

have already been established and enshrined in UN General ASSEMBLY Resolution RES / 73/27 of 5 December 2018. Any state can join them on a voluntary basis. Even opponents of the Russian position agree that compliance with such rules reduces the risk of conflicts, which is confirmed by UN General ASSEMBLY Resolution RES / 74/27 of 12.12.2019.

At the moment, compliance with the rules of responsible behavior of States in the use of information and communication technologies (hereinafter referred to as the Rules) is not an international legal norm, and therefore the prospects for changing their status and the reaction of the expert community to such changes are of interest. In order to familiarize civil society with the views of the expert community, the United Nations office for disarmament Affairs (UNODA) has prepared a material "Voluntary, Non-Binding Norms for Responsible State Behavior in the Use of Information and Communications Technology A Commentary", containing comments from more than 40 experts on all thirteen points of the Rules. An analysis of the comments shows that the objections relate mainly to the unclear status of the Rules. At the moment, their provisions can serve as voluntary standards of state behavior, but with some refinement, accompanied by changes in national legislation, they can be perceived as a legal norm [22].

The positions of Russia and the United States allow the use of retaliatory measures to information threats. This immediately raises the question of the international community's attitude to such actions and responses. Of course, the international community represented by the UN should be guided in such cases by the provisions of the relevant sections of international law, so the question of the applicability of existing international law to information security remains relevant. This issue is not only of academic interest, but also of crucial practical importance. In the case of a positive answer to the conflicts in the information environment become applicable to existing conventions that are applicable to cases of use of armed force. Violation of their requirements would be a violation of international law, and in some circumstances, a war crime with all its consequences. In this regard, the question of the applicability of existing norms of international humanitarian law to actions in the information space is extremely important in General and is of interest in the context of this article. The latter is due to the fact that it is the interpretation of information security and the wording of its main provisions that will serve as the basis for the qualification of actions using information and communication technologies.

6. Applicability of existing international law to information security

After a long period of discussion, following the recommendations of the group of governmental experts, the international community recognized the applicability of existing international law to international information security. However, its practical application is still far away, as it requires the revision of existing norms and the creation of a number of new provisions. The system of international legal support for information security in the context of global cross-border information space (cyberspace) should be based on the basic principles laid down in the UN Charter. This can be implemented in a variety of ways, so the scientific literature on this issue suggests different approaches. Thus, the largest expert in the field of Internet development, the head and Creator of "DiploFoundation" Jovan Kurbaliya, describing a special case of interaction of individual citizens in cyberspace, speaks about the "real" law, in which the "Internet" should be considered a technical phenomenon, the development of previous communication technologies. Of course, the Internet is faster and larger, but it is still one of the ways to communicate between people. Therefore, any existing legal norms can also be applied to the Internet.

The Internet has a huge potential for development. It provides an unprecedented amount of resources for information and knowledge sharing, which opens up new opportunities for citizens to Express their opinions and participate in the management of public Affairs [23, p.471]. In this case, the following contradiction arises. On the one hand, the principle of freedom of expression in the context of human rights development should be applied to the development of democracy, including through the Internet environment. On the other hand, the free flow of information leads to the threat

ISSN 2658-4050 (Online)

of free circulation of potentially dangerous information, including extremist information, as well as to the possibility of influencing public opinion by introducing propaganda into the network [24].

7. Conclusion.

A study of UN documents shows that the positions of the United States and the Russian Federation in the field of international information security are gradually converging, and the convergence is in the direction of the Russian position. At the moment, the UN General ASSEMBLY resolutions initiated by the United States conceptually coincide on many points with the resolutions introduced by Russia. However, there are still fundamental differences arising from different interpretations of the concepts of "information security", "information threat", therefore, there are different approaches to the semantic content of freedom of speech and access to information. The United States and a number of other countries at the level of international documents do not recognize the fact that information itself can pose a threat to States and international peace, even without causing physical damage to cyber structures and data integrity. As a result, the United States criticizes or approves security measures, depending on their impact on the freedom of information flows. Nevertheless, the adoption of the UN General ASSEMBLY resolution RES / 73/27 with a clause against the dissemination of false or distorted messages shows that the Russian position is becoming more and more supported.

Thus, the Internet has a significant impact on the public sphere, therefore, freedom of speech and access to information in cyberspace should have the same level of protection as in the physical world. The limits of freedom of speech and the right of access to information, in our opinion, do not correspond to the level of development of public relations, since there is a possibility of unleashing a war in the information field under the pretext of protecting freedom of speech and free access to information. It is also impossible to administer prohibited information, for example, Google admitted that "it is impossible to filter out all content related to terrorism, since approximately every minute about 300 hours of video material is uploaded to YouTube." The question remains, who should give a legal assessment of the disputed materials? If this is done by the competent authorities, it will automatically lead to an unjustified increase in bureaucratic barriers, which in any society causes irritation and misunderstanding.

The lack of effective legal instruments to prevent defamation in the mass media is a serious indicator of the problems in ensuring the full exercise by citizens of freedom of speech and the right to access information, building a stable and equitable system of international information security.

ISSN 2542-1514 (Print)

REFERENCES

1. Litvak N.V. Information processes in the modern diplomatic service: the experience of France. Moscow, MGIMO-University Publ., 2016. 486 p. (In Russ.).

2. Dzyaloshinsky I.M. Features of communicative behavior in cyberspace, in: Problems of interaction of language and thinking. Moscow, Intellect Center Publ., 2010. Available at: http://www.dzyalosh.ru/02-01-Auditoriya-Media/Kiberprostranstvo.pdf (accessed on 10.07.2020). (In Russ.).

3. Berestnev Yu. Yu. Guide to the case law of the European Court of Human Rights. 2002-2016. Moscow, Razvitie pravovykh system Publ., 2016. 1288 p. (In Russ.).

4. Kittichaisaree K. Public International Law of Cyberspace. Springer International Publishing, 2017. 376 p. DOI: 10.1007/978-3-319-54657-5.

5. Sudiev I. Yu., Smirnov A. A., Kundetov A. I., Fedotov V. P. Theory and practice of information counteraction to extremist and terrorist activities. Moscow, Polygraph-Book Publ., 2014. 240 p. (In Russ.).

6. Kolosov Yu.M. Mass information and international law. Moscow, Statut Publ., 2014. 160 p. (In Russ.).

7. Krutskikh A.V. (ed.). International information security: Theory and practice. Volume 1. Moscow, Aspect Press, 2019. 384 p. (In Russ.).

8. Rogovskiy E.A. Cyber-Washington: global ambitions. Moscow: Mezhdunarodnye otnosheniya Publ., 2014. 848 p. (In Russ.).

9. Bolgov R. UN Activities in the field of information and international aspects of information security in Russia. *Sravnitel'naya politika = Comparative politics*, 2018, vol. 10, no. 1, pp. 59-69. (In Russ.).

10. Smirnov A.I. Modern information technologies in international relations. Moscow, MGIMO-University Publ., 2017. 334 p. (In Russ.).

11. Floridi L. The 4-th revolution: how the infosphere is reshaping human reality. New York, Oxford University Press, 2014. 248 p.

12. Salikov M.S., Nesmeyanova S.E., Molchanov A.N., Kolobaeva N.E., Ivanova K.A. Human Rights in the Internet. Yekaterinburg: UPI Publishing house, 2019. 148 p. (In Russ.).

13. Salnikova L.S. (ed.). The communication strategy in the digital age. New technologies. Moscow, Scientific library Publ., 2019. 300 p. (In Russ.).

14. Groshikov K.K. Socially significant information and its criminal-legal protection. Moscow, Yurlitinform Publ., 2011. 144 p. (In Russ.).

15. Karasev P. Strategy of information (cyber) security of the USA in the XXI century. *Vestnik Moskovskogo universiteta. Seriya 12. Politicheskie nauki = Moscow University Bulletin. Series 12. Political Science,* 2013, no. 3, pp. 89-102. (In Russ.).

16. Burkov A.L. (ed.). How to bring human rights home: human protection in national and international institutions. Moscow, Izvestiya Publ., 2018. 400 p. (In Russ.).

17. Menshikov P.V. (ed.). Information and communication technologies of the third Millennium. Moscow, MGIMO-University Publ., 2020. 460 p. (In Russ.).

18. Mounk Y. The people vs. democracy. Why our freedom is in danger and how to save it. Harvard University Press, 2018. 393 p.

19. Petric B. (ed.). Democracy at Large - NGOs, Political Foundations, Think Tanks, and International Organizations. New York, Palgrave Macmillan, 2012. 280 p.

20. Lebedeva M. "Soft power": the concept and approaches. *Vestnik MGIMO-Universiteta = MGIMO Review of International Relations,* 2017, vol. 3, pp. 212-223. (In Russ.).

21. Molchanov N.A., Matevosova E.K. Information Security Doctrine of the Russian Federation (new legislation). *Aktual'nye problemy rossiiskogo prava = Actual problems of the Russian law,* 2017, pp. 159-165. DOI: 10.17803/1994-1471.2017.75.2.159-165. (In Russ.).

22. Tikk E. (ed.). Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary. New York, United Nations Publication, 2017. 280 p.

23. Kaldor M., Randelov I. The handbook of Global Security Policy. Chichester, Wiley Blackwell, 2014. 541 p.

24. Hoffman B. Inside terrorism. New York, Columbia University Press, 2017. 494 p.

ISSN 2658-4050 (Online)

INFORMATION ABOUT AUTHORS

Ksenia A. Ivanova – PhD in Law; [1] Director of the Center of Local Authorities of the Institute of Management and Regional Development; [2] Associate Professor, Department of Constitutional and Municipal Law
[1] *Russian Presidential Academy of National Economy and Public Administration (RANEPA)*
[2] *University of Tyumen*
[1] 84, Vernadskogo pr., Moscow, 119571, Russia
[2] 6, Volodarskogo ul., Tyumen, 625003, Russia E-mail: ivanova-ka@ranepa.ru
RSCI SPIN-code: 6610-9218; AuthorID: 695216

Madi Zh. Myltykbaev – post-graduate student, International Law Department
MGIMO University
76, Vernadskogo pr., Mioscow, 119454, Russia E-mail: myltykbaev@my.mgimo.ru
ORCID: 0000-0003-3261-9927
ResearcherID: AAA-3864-2019
RSCI SPIN-code: 6952-1510; AuthorID: 1028441

BIBLIOGRAPHIC DESCRIPTION

Ivanova K.A., Myltykbaev M.Zh. The freedom of speech and right of access to information in the emerging system of international information security. *Pravoprimenenie = Law Enforcement Review*, 2020, vol. 4, no. 4, pp. 80–93. DOI: 10.24147/2542-1514.2020.4(4).80-93. (In Russ.).

Правоприменение
2020. Т. 4, № 4. С. 80–93
ISSN 2542-1514 (Print)