

Communication Policy of the Russian Federation in the global information society and Information Law

Svetlana Petrova
*Doctor of Political Science,
Professor, Dean of the faculty of law
Sochi State University
Sochi, Russia*

Natalya Vorobeva
*Candidate of Law Science, Associate
Professor, Department of Civil and
Criminal Law and Procedure
Sochi State University
Sochi, Russia*

Guram Darakchyan
*Candidate of Political Sciences,
Associate Professor, Department of
Administrative
Sochi State University
Sochi, Russia*

Aibulat Yanguzin
*Doctor of Philosophy, Professor,
Scientific Secretary of the Scientific
Council on Philosophy and
Sociology¹, Professor²
¹Academy of Sciences of the Republic
of Bashkortostan
²Bashkir State University
Ufa, Russia
nbret@yandex.ru*

Svetlana Pozdyayeva
*Doctor of Philosophy, Professor of
Philosophy and Political sciences,
sub-faculty of the Faculty of
Philosophy and Sociology
Bashkir State University
Ufa, Russia*

Zhibek Issayeva
*Candidate of Philology, leading
researcher
National Academy of Education
named after Y. Altynsarin of the
Ministry of Education and Science of
the Republic of Kazakhstan
Astana, Kazakhstan*

Abstract-In the modern world, the possibility of forming meanings is expanding due to the communicative capabilities of the Internet. The network information space becomes an important tool of complex representation of dynamic information about the subject (including political jacks) in the media form. The Central problem for communicants is not only the processing, structuring, presentation of retrospective and current information, but also the search for forms of effective communication. The main motive for building communication strategies of the government is both the preservation of its own legitimacy and the legitimization of its individual initiatives and decisions aimed at society as a whole and individual social groups.

Throughout the existence of society and the state, revolutionary changes in communication technologies have been followed by significant changes in the political process. At the present stage in the world is faster mass internetization. From the local invention of scientists to facilitate their research, the Internet has become a worldwide network, a means of communication that increasingly affects all aspects of human life. The world of politics does not remain aloof from this trend.

The world wide web is challenging traditional institutions and mechanisms of the political process, putting increasing pressure on governments to perform their functions more effectively. At the same time, information and communication technologies are opening new effective means of communication between citizens, political cooperation and government.

Keywords-*legal law in communication policy, imagology, Internet technologies, image of Russia, international information policy*

I. INTRODUCTION

The research of information technologies in the political process and especially technologies of political Internet communication is a topical subject and is determined by the following provisions.

First, Internet communication technologies have penetrated the political environment relatively recently, and their study by domestic political science is at the beginning.

Secondly, the identification of the role of Internet technologies in the process of political communication requires that in recent decades in modern Russia, as well as in other countries, the crisis of traditional forms of political communication is growing, which is its basis for the search for both its new forms and its intensification.

Thirdly, the Internet is increasingly recognized as an effective channel of political communication. A new structure of communication participants is being formed, new technologies and means of its implementation are emerging. Internet communication technologies differ significantly from traditional ones and require separate study.

Fourth, we have accumulated considerable empirical material on the study of the main components of Internet communication (communicators, Internet resources, virtual space in General). There is also considerable experience in the use of Internet technologies in the political process. Both require theoretical understanding.

Some theorists of communication design, in particular J.Vin, suggest to accept the website and web pages for a certain model of behavior focused on the

organization of effective ways of interaction of users [1]. If we consider the set of communicative projects in the Internet space in this way, in the end, we can conclude that the purpose of communicative strategies is the most effective and productive transfer of information and the formation on its basis of the desired for the subject of communication meanings and behaviors. In other words, it is a model of communicative behavior that leads to a more productive variant of communicative interaction, both between the source of the message and the target audience, and between end users.

The media environment of the Internet contributes to the development of a pluralistic, if not democratic, type of communication. Under these conditions, political power finds itself in an unusual competitive environment (many sources of information and semantic texts), requiring new approaches to the development of communication strategies. In modern society, power is no longer the main center of political communication, and a significant number of sources of information (especially in the Internet) allows people to implement their own technology of choice (different from the conditions of domination of traditional media). Forming a communicative strategy, the government should take that it becomes quite difficult to impose its own position.

II. MATERIALS AND METHODS

Despite significant General theoretical studies of new information technologies in political communication, there is still a lack of systematization of experience in the application and evaluation of the effectiveness of various Internet technologies in the process of political communication, their advantages and disadvantages are not disclosed holistically.

The object of the research is Internet technologies in the modern political process. The subject of the study is political Internet communication at the present stage of development of the information society in Russia.

To date, there are practically no special theoretical works in the field of analysis of political and communicative characteristics of specific projects of political power. In our understanding, the analysis of communicative strategies of power on the Internet should be based on their reconstruction, based on analytical schemes of theories and models of mass communication. In the conditions of inaccessibility of the analysis of the communicative strategy publicly presented by the political power (due to the closeness of the power and the mechanism of decision-making), as well as the complexity of the development of a unified and unambiguous communicative strategy by the power, the reconstruction of communicative strategies (reproduction-conducting of communicative processes based on the analysis of specific projects and their political prerequisites, based on models of mass communication) seems to be an adequate way for their analysis. Current communication practices confirm the idea that the study of natural functions of perception and representation of socio-political information

involves the assessment of the communicative potential of the strategies of the regime, means of information-communicative design.

The aim of the study is a comprehensive analysis of the effectiveness of the use of means and forms of Internet communication by political actors in Russia at the present stage of development of network technologies.

To achieve this goal, tasks are set:

1. To reveal the main theoretical approaches to the study of new information technologies in the political process. To concretize the concept of political Internet communication.

2. To analyze the experience of using network communication technologies in political practice. Identify and systematize the main technologies, forms and means of political Internet communication at the present stage of their development.

The theoretical and methodological basis of the thesis was the theory of information society and political communication contained in the works of domestic and foreign scientists who studied these problems. The study used General scientific and special methods of cognition, as well as empirical methods. The theoretical and methodological basis of the study is based on the structural and functional, systemic and institutional approaches of political science.

The empirical base of the research is represented by the data of state statistics, materials of sociological research of the public opinion Foundation, the all-Russian center for the study of public opinion, the Research holding "ROMIR Monitoring", the Agency for marketing research "MA8M1", normative legal documents, materials of scientific conferences, media data, information from Internet resources.

III. DISCUSSION

The "non-state security sector" is developing rapidly. The researcher noted that "an indirect manifestation of this trend in the "economic culture" was the renewal of business approaches to security issues" [2]. Based on the study of the company's business Outlook Pricewaterhouse Coopers (according to which more than 42% of the business now considers the cost of security as a strategic initiative), A. Yu. Poltorakov points out: "instead of reacting to attacks and intrusions, companies want to be proactive in deploying defense systems in order to prevent possible trouble in the future. This, in turn, affected the "quality" of economic intelligence, which began to openly dominate the political" [2]. In our opinion, the privatization of security is reflected in the growing diversity of private security structures and is a feature of modern practices and structures of information security or General practice of information security. The mobility of security practices and the privatization of security are closely linked.

The goal of information warfare is to gain and retain information superiority over the opposing side"

[3]. We also share the definition of information warfare A.V. Manoilo, who notes that "information warfare is a rivalry of social systems in the information and psychological sphere about the impact on certain areas of social relations and the establishment of control over the sources of strategic resources, as a result of which some participants in the rivalry get the benefits they need for further development, and others lose them" [3]. The second definition, in our opinion, outlines the external social contour of the practice in question.

The information space has practically become a part of the space of conflicts, a theater of military operations, where each of the warring parties seeks to gain and hold the advantage as long as possible, and, if necessary – to defeat the enemy. "It becomes obvious that a party that does not understand or underestimates this circumstance is doomed to be on the side of the "pillar road" of civilizational development" [4].

Many analysts believe that information warfare is today the leading tool in resolving geopolitical conflicts. Thus, A.V. Manoilo points to "the goals that are carried out by the state through information warfare: – ensuring geopolitical and information and psychological security of the state; – achieving military and political superiority and unconditional leadership in the field of international relations; – ensuring the achievement of the goals of national economic, ideological, cultural, information and psychological expansion; – providing favorable conditions for the transition of its own national system of socio-political relations to a new, more highly developed and high-tech stage of evolutionary development; – transformation of the structure of national economic, political, socio-cultural, information and psychological spaces in accordance with its own principles of formation of the information picture of the world" [3]. Information warfare is analyzed by the authors through such concepts as information warfare, information warfare and the fight against information crime, which are interpreted as forms of warfare. There are also two types of information warfare: information technology and information psychology. In social practices of information and technical confrontation the main objects of influence and protection are information and technical systems (communication systems, telecommunication systems, data transmission systems, electronic means, information security systems, etc.).

There are three levels of information warfare practices: strategic, operational and tactical levels. Strategic level practices are carried out by the highest bodies of state power. Special services and large national capital implement information security practices at the operational and tactical levels.

IV. RESULTS

The practice of building communication projects on the Internet, within the framework of communication strategies, consists of two main elements - the development of an information concept and information architecture of the project. To pen-sustainable were the identification of potential key audience groups; analysis of groups of visitors and to

identify their interests; the formulation of goals and ways to achieve them for each group, the wording of the main goal of the communication project; basic principles of presentation of information; identify the ways of development of the project. Building the information architecture of the project (website, forum, portal, project and other Internet resources) involves the answer to the following questions: how long will it take the visitor to understand what the resource is dedicated to, whether it will be easy to navigate, whether the visitor will notice important information, whether he will form a certain installation.

The modern generation of confrontation assumes not so much military and power methods of struggle as media-humanitarian: 1) creating an atmosphere of lack of spirituality and immorality, a negative attitude to the cultural heritage of the enemy; 2) manipulation of public consciousness and political orientation of social groups in the country in order to create political tension and chaos; 3) destabilization of political relations between parties, associations and movements with the aim of provoking conflicts, inciting mistrust, suspicion, aggravation of political struggle, provoking repression against the opposition and even civil war; 4) reducing the level of information support of authorities and management, instigation of erroneous management decisions; 5) misinformation of the population about the work of state bodies, undermining their authority, discrediting government; 6) provoking social, political, national and religious clashes; 7) initiation of strikes, riots and other actions of economic protest; 8) difficulty in making important decisions by the governing bodies; 9) undermining the international authority of the state, its cooperation with other countries; 10) damage to the vital interests of the state in the political, economic, defense and other spheres.

So, among the General practices in information security, we distinguish: 1. practice of information warfare, is represented by two generations; 2. information society; and, including 3. state policy on Informatization of society, ensuring information security of the country and independence of information infrastructure. It is important to note that the development of the information infrastructure of the society provides the "mobility infrastructure" of social actors. The developed information industry, as well as cognitive structures and institutions of society, providing activation, reproduction and development of the information resource, are considered by us as social structures in ensuring information security of subjects.

Finally, the most important type of information security practices is the very formation and further development of information law at all levels of security: the security of the individual, organization, region, state and international security. V. P. Sherstyuk notes that "in the field of international information security, the most urgent is the development of existing norms of international security law and international humanitarian law in the direction of creating an effective system of prevention and suppression of possible aggressive actions carried out by information and communication technologies. New legal

mechanisms should help to preserve the positive potential that has already been accumulated in international law, as well as its use to counter new threats to information security" [5]. In General, the idea of the structures (and in part institutions) of information security today is systemic. The main segments of these structures, their normative and legal character are developed by such branch of knowledge as information law.

Within the Institute of information law, information security is understood as the process of ensuring the confidentiality, integrity and accessibility of information, where confidentiality – ensuring access to information only to authorized users, integrity – ensuring the reliability and completeness of information and methods of its processing; availability – ensuring access to information and related assets of authorized users as necessary.

The purpose of the implementation of information security of any object is to build a system of information security of the object. For this purpose, the normative acts of the state prescribe several functions, the implementation of which also implies the existence of appropriate structures to identify the requirements for the protection of information specific to this object of protection. In the Russian Federation, normative legal acts in the field of information security include acts of Federal legislation: – international treaties of the Russian Federation; – the Constitution of the Russian Federation; – laws of the Federal level (including Federal constitutional laws, codes); – decrees of The President of the Russian Federation; – Resolutions of the Government of the Russian Federation; – normative legal acts of Federal ministries and departments; – normative legal acts of subjects of the Russian Federation, local governments, etc. Also allocate normative and methodical documents: 1) methodical documents of state bodies of Russia (the Doctrine of information security of the Russian Federation; guidance documents of FSTEC of the Russian state Commission; orders of the FSB); 2) information security standards (international standards; state standards of the Russian Federation; recommendations for standardization; guidelines).

Depending on the application of activities in the field of information security (within the state authorities or commercial organizations), the activity itself is organized by special state bodies (divisions) or departments (services) of the enterprise. The state bodies of the Russian Federation that control the activities in the field of information security are the security Council of the Russian Federation, the state Duma Committee on security, the Federal service for technical and export control (FSTEC Russia), the Federal security service of the Russian Federation (FSB Russia), the Federal security service of the Russian Federation (FSO Russia), the foreign intelligence Service of the Russian Federation (SVR Russia), the Ministry of defense of the Russian Federation (Ministry of defense of Russia), the Ministry of internal Affairs of the Russian Federation), Federal service for supervision of communications,

information technologies and mass communications (Roskomnadzor). Services that organize the protection of information at the enterprise level are the economic security service, personnel security service (regime Department), personnel service, information security service. Within the framework of information security policy separately consider such areas of information system protection as protection of information system objects; protection of processes, procedures and information processing programs; protection of communication channels (acoustic, infrared, wired, radio channels, etc.); suppression of side electromagnetic radiation; control of the protection system. Information security policy is made in the form of documented requirements for a specific information system. Documents are usually divided into levels of description (detail) of the protection process.

Separately, it is necessary to dwell on such organizations of our time as "think Tanks" (Think Tanks). Think tanks or "think tanks" are public institutions that provide advice on government and corporate contracts, usually in the field of political production and assessment of the possible socio-economic consequences of political decisions. Intellectual production of these organizations – applied political expertise, research and Analytics, as well as fundamental theoretical works. As a rule, it is distinguished by strategic goal-setting, based on certain ideas about the desired socio-economic and political results. This allows politicians and society to make decisions based on the information provided by these institutions. This is the difference between the products of "thought factories" and the actual academic research.

Thus, the Russian state as the main institution (structure) of ensuring the security of society develops information policy, the main directions of which were originally laid down in the Doctrine of information security from 2000. This policy is aimed at maintaining and forming social structures of information security: these are various systems, institutions that protect and develop the information sphere of society; these are institutions of information law, management state structures, legislative structures, state intelligence services, their activities in the field of information policy and information security, etc.

V. CONCLUSION

In General, information law is today, in our opinion, the most developed area of knowledge in the field of information security. In Russian society, there are certain relations between the authorities and analytical centers. The system of decision-making in the field of domestic and foreign policy of the state almost does not provide for the involvement of third parties in this process. There are many analytical centers that want to offer their product to the authorities. However, most of them are PR firms.

The variety of processes of transmission, processing and storage of information leads to the formation of the information industry and, accordingly, the information infrastructure of the state.

The rapid convergence of information technologies, the expansion of the market of information services consumption have led to structural changes in the information industry. First, the combined organization, generate information, and the organization that owns the means of delivery of content to the consumer. Second, companies that manage various segments of the information economy-computer manufacturers and software developers, telephone operators of cellular and wired communications, cable broadcasting systems, publishing houses, etc. The merger of information companies, in turn, leads to the liberalization of the legal framework governing the different aspects of the information industry. The essence of this process in mitigating or complete lifting of restrictions on different types of activities, concentration of ownership and increased participation of transnational capital. The process of registration of the information world economy is accelerating. This is reflected in the globalization of telecommunications and information technology markets, the emergence of powerful media holdings and diversified corporations, certainly leading in the world trading platforms, the transformation of "electronic Commerce" using telecommunication channels in the dominant means of doing business. It is with the development of the information industry that a special area of law arises, which regulates human rights in the use of information resources, protection of copyright and intellectual property, the right to privacy, freedom of speech, etc.

Issues of information security of individuals and society acquire a qualitatively new status. From a technological problem, information security becomes a social problem affecting the very foundations of the functioning of modern society.

REFERENCES

- [1] J. Vin, *The art of Web design*. Saint-Petersburg: Peter, 2002.
- [2] A. Yu. Poltorakov, "Political and system aspects of security of post-industrial society", in *National Security*. Nota bene Publ. House, 2009, No 2, pp. 18-23.
- [3] A. V. Manoilo, *State information policy in special conditions*. Moscow, 2003, 388 p.
- [4] V. S. Pirumov, *Information confrontation. The fourth dimension of confrontation*. Moscow: Weapons and technology, 2010, 256 p.
- [5] V. P. Sherstyuk, "Threat to international information security in the context of the formation of the global information society and areas of cooperation", in *Law and security*, 2010, No 4 (37), pp. 24-27.