KnE Social Sciences

Culture, Personality, Society
XXIV International Conference "Culture, Personality, Society in the Conditions of Digitalization: Methodology and Experience of Empirical Research"
Volume 2022

Knowledge E
enriching | engaging | empowering

Research article

Society and State Responsibilities for Security in the Digital Network Space: The Opinions of Citizens and Experts

V.V. Zotov[1,2,*], and A.V. Gubanov[3]

[1]Moscow Institute of Physics and Technology, Dolgoprudny, Moscow Region, Russian Federation
[2]Finance University under the Government of the Russian Federation, Kursk branch, Kursk, Russian Federation
[3]Belgorod State University, Belgorod, Russian Federation

ORCID
V.V. Zotov: https://orcid.org/0000-0003-1083-1097
A.V. Gubanov: https://orcid.org/0000-0003-4810-6165

Abstract. This article is devoted to the study of the role of state bodies and civil structures in ensuring the security of the digital network space. The purpose of this work was to determine the subjective opinions of citizens about the boundaries of society and state responsibility for security in the digital network space. This sociological study included a combined online and offline survey, as well as a survey of experts. A sample of 1,000 respondents aged 16 years and older was recruited, which was representative on gender and age grounds. The sample for the expert survey consisted of 90 specialists across areas of activity. Based on the results, the authors concluded that in order to legitimize power, it is necessary to re-distinguish states and societies from the responsibility of ensuring personal and public security. Respondents considered the state and society to be equally responsible for the moral components of personal security, and that the state is responsible for protecting the personal data of citizens and ensuring public security. Experts were inclined to believe that both personal and public security in the digital network environment should be provided by authorities.

Keywords: digitalization, responsibility, state, society, security, digital network space

Corresponding Author: V.V. Zotov; email: om_zotova@mail.ru

Dates
?????

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the Culture, Personality, Society Conference Committee.

1. Introduction

Currently, there is a new stage in the development of information and telecommunications technologies related to digital technologies: artificial intelligence (machine learning), big data, virtual reality, blockchain, geo-positioning, semantic web, and the Internet of things. It is they who determine the essence of digital transformation. In turn, this is an unconditional driver of social development. Today, almost the entire population of the country is users of the Internet and its applications. Digitalization is the creation of an electronic platform that has analytical and predictive functions. It is based on information interaction, realized not only by direct input of data by a person into a computer or mobile device but also by data from sensors, cameras, and smart devices.

Note that during the period of quarantine caused by the COVID-19 pandemic, all human life began to be realized on these platforms: job, study, and everyday interaction with other people.

Digitalization of society pushes the boundaries of human capabilities, but invariably creates risks and threats. Moreover, the latter acquire a mass and devious character in the context of globalization. This updated the subject of research related to the security of digital network platforms [1, 2] and relationship management issues in the digital environment [3, 4, 5]. For example, Mireille Hildebrandt discusses how smart technologies undermine, reconfigure, and overturn the rule of law in a constitutional democracy, jeopardizing the law as an instrument of justice, legal certainty, and the public good. He therefore appealed to civil society not to reject smart technologies, so that the continued use of those technologies would help reinvent the effective protection of the rule of law. Here, in the authors' opinion, it is necessary to place in the focus of research a discussion of the role of the state and civil society in digital society, the foundations of public administration. In the latter case, according to Vasilenko, "it is necessary to revise the semantic accents of the term 'public administration', shifting them towards the term 'controllability' and 'public' in the process of implementing the state digitalization program in Russia" [6]. This will avoid the contradiction of the concept of "public administration": the term means the participation of society, but it is not considered here as an independent structure.

The crisis caused by the spread of coronavirus infection COVID-19 is not an ordinary crisis, but a blow to democracy. It can lead to a change in the social structure towards increasing totalitarian trends through the introduction of digital technologies under the auspices of the fight against the pandemic. It can be assumed that the problem lies in the need to renew the social contract, in the receipt by the authorities of a new consent of the administrations in order to preserve legitimacy, in the discussion of the separation of society and the state of responsibility for the security of the digital network space.

The issue of the responsibility of the parties is central to the social contract. Issues of responsibility arise whenever agreed social development goals are required. If something goes wrong in digitalizing society, then they should be called "responsible" for what happened. Today, the main responsible bodies are the authorities and structures of civil society, whose balance of interests determines the areas of responsibility. Note that the state in this case should be interested in sharing responsibility for what is happening in the field of digital technologies, so as not to be extreme in a situation of crisis or failure in the future.

2. Methodology and methods

In methodological terms, the ongoing research will be based on an intuitive-rational method [7], which gives priority to empirical data and their interpretation. The empirical basis of the study was a sociological study conducted in order to obtain reliable and substantiated information about the opinion of the population on the boundaries of the society and state responsibility for security in the digital network space. Sociological research included mass and expert surveys. Due to the epidemiological situation, the mass survey was carried out by means of a questionnaire survey in a combined way: 1) an online survey using the Google service; 2) a field survey using personal interviews using a paper questionnaire. The general population of the study was over 18 years old. The sample population in the volume of n = 1000 respondents was a quota for sex and age (up to 30 years old, from 30 to 60 years old, over 60). Questionnaires were excluded from the processing, from which it was clear that respondents did not have computers, did not use the Internet, could not say anything about digital technologies, since these were not related to their daily practices. The expert survey was carried out among government officials, representatives of science and education, municipal employees, members of public organizations and political parties. A total of 89 experts were interviewed. Additionally, the results of the study on the attitude to digitalization were attracted [8] and information security in digital networking [2].

3. Results and Discussion

The results of the study by Lukov and Lukova show that in Russian society there is no positive attitude towards digitalization, moreover, “there is no euphoria about these advantages, although the implementers of social projects on digitalization see only its bright sides, and the opinion of the population is not taken into account” [8]. According to the data of surveys conducted under the leadership of Krivoukhov, respondents generally note that today, due to the introduction of information and telecommunications technologies, life activities in modern society are becoming more dangerous or rather more dangerous (as 18% and 40%, respectively) [2]. It should be noted that his study mainly touched on security problems from criminal threats in the digital space. At the same time, the respondents were asked in fact two questions, since they had to express consent or disagreement with such statements “The authorities should ensure security in the information and communication environment to all members of society” and “Everyone should take care of security in the information and communication

environment". According to the survey, more than 2/3 of the respondents believe that everyone should take care of security in the information and communication environment, and half of the respondents said that the authorities should ensure security in the information and communication environment to all members of society.

Other aspects of personal and public (national) security were included in our study. The question itself had an alternative character, that is, for each question position it was proposed to choose the person responsible: "state" — "society" — "together". The results of the survey show that when distinguishing responsibility between the state and society in matters of activity on the Internet, respondents have their own position within the framework of personal security and public safety. At the same time, personal security was understood as the state and conditions of life of an individual, in which the threat of harm to his/her private space is absent or minimized. This should include combating insults and other manifestations of hatred on the Internet, combating the dissemination of false information on the Internet, as well as ensuring the security of the personal data of Russian Internet users. Public (national) security will be understood as the state and conditions of life of society, in which there are no or minimized threats of harm to the public space of society. This applies primarily to the fight on the Internet against the activities of criminals (cheaters), foreign special services, and extremist and terrorist organizations.

The survey data show that with regard to personal security, 52% of the participants in the survey expressed confidence that the state and society should jointly be responsible for combating the dissemination of inaccurate information on the Internet, a similar position (52% of respondents) was recorded on the issue of combating insults and other manifestations of hatred between Internet users. Detailed information is provided in Table 1.

It should be noted that society plays a significant role, according to respondents, in combating insults and other manifestations of hatred (19%), as well as combating the dissemination of false information on the Internet (14%). Although for these areas, respondents are inclined to joint responsibility of the state and the citizens themselves. It can be said that the above-mentioned components of personal security fall more under the moral regulation of relations between citizens than under the normative.

Exclusive areas of responsibility of the state, according to the respondents, are: safety of personal data of Internet users (63%), fight against cheaters (66%), fight against attempts of destabilization of a situation from foreign intelligence agencies (67%), and control of activity of the extremist and terrorist organizations in the intern space (68%).

TABLE 1: The distribution of answers to the question "Who do you think is more responsible for regulating the following areas of the Internet?", in %.

	State		State and Society		Society	
	citizens	experts	citizens	experts	citizens	experts
1. Combating insults and other forms of hatred on the Internet	29%	47%	52%	36%	19%	18%
2. Combating the dissemination of inaccurate information on the Internet	34%	52%	52%	32%	14%	16%
3. Security of personal data of Russian Internet users	63%	70%	32%	26%	5%	4%
Fighting crime (cheaters) on the Internet	66%	78%	28%	20%	6%	2%
5. Combating attempts to destabilize the situation by foreign special services through the Internet	67%	82%	30%	16%	3%	2%
6. Monitoring the activities of extremist and terrorist organizations on the Internet	68%	84%	29%	12%	3%	3%

[a] The table shows the percentage of responses from citizens and experts.

Ensuring national security in the field of digital network platforms, improving the regulatory framework, and developing the latest technical tools to counter the dissemination in the information space of ideas both extremist and destabilizing the situation are already among priority tasks for the state authorities of the Russian Federation. However, world practice indicates that such problems are characteristic not only for Russia. Therefore, with particular urgency, the irresponsibility of hopes for a good start in the human person and the need to develop mechanisms for the legal regulation of the use of the latest information, telecommunications, and digital technologies begin to be felt. Article 12 of Federal Act No. 114-FZ of 25 July 2002 "On combating extremist activities" expressly prohibits the use of public communication networks for extremist activities. These are mainly sites where hostility and hatred against representatives of other peoples are aroused, there are calls for extremist activities. Here, it is possible that such actions will infringe on the constitutional right of citizens to freedom of speech, so this aspect should become the basis for the division of responsibilities between the state and society.

At first glance, such a component of personal security as the security of personal data of Internet users should be in the area of responsibility of citizens themselves, but they impose responsibility on state bodies. In the authors' opinion, this is due to the fact that scandals with the leak of personal data follow one after another. They use personal data not only for identification, conducting targeted advertising and political

campaigns but also for fraud. As a result, today 2/3 of citizens faced theft and misuse of confidential information on the Internet (as evidenced by the survey data). It should be noted that, most often, respondents in the middle age category faced problems of stealing confidential data — 72%, while among young people, this figure was 67%, older respondents — only 52%. The solution to these problems is impossible without the active legal and administrative participation of public administration bodies. It is especially dangerous when the goal of cheaters is older citizens, whose average level of Internet technology ownership is less than in other age categories.

Unfortunately, in order to encounter the collection of personal data in the network space, it is not necessary to visit sites infected with spyware or fraudulent resources, just go online and enter a request in any popular search aggregator. In the absolute majority of cases, the user him/herself indicates personal data when ordering in online stores, registering on sites, filling out a profile on social networks, or even when compiling a search query. Moreover, Internet users do not always understand how dangerous such a privacy disclosure can be. Almost half of the participants in the mass survey (46%) said they were well aware of the possibility of collecting web analytics systems by sites, another 36% of respondents have only general information. Only 8% of citizens have not heard of such functionality.

The results of the expert survey are presented in the same Table 1. Analysis of these data shows that experts are more radical in that it is the state that is more responsible for regulating the security of activities in the Internet space. Even in such “moral” spheres on the Internet as the fight against insults and manifestations of hatred, the fight against the dissemination of false information, experts consider it necessary to attract the state. Particularly strongly paternalistic attitudes are seen among experts representing state and municipal employees.

It can be assumed that the digitalization of society requires a certain agreement on the rules and principles of public administration with the corresponding legal form. This is generally confirmed by the answers to the question about the need at present to conclude a public contract, which will open up opportunities to search for new schemes and tools for organizing the interaction of authorities and the population in the digital space. The majority of the population (54%) said that the conclusion of a new public contract between civil society structures and authorities for joint work on digitalization of public administration in the interests of the country’s citizens was necessary, while only 16% held the opposite point of view, 30% found it difficult to answer. Experts expressed even more categorical opinions on concluding such a social contract (60% spoke in favor, 11% against). Among the experts, the group of those who found it difficult

to answer (29%) is also quite large. It should be noted that exactly half of the experts from among civil servants entered this category.

4. Conclusions

Thus, the digitalization of society pushes the boundaries of people's capabilities and offers more options for social development, but also violates the balance of interests of the state and citizens. Today, in order to legitimize power, it is necessary, on the basis of a reasonable compromise of the value priorities of the individual, society, and the state, to re-distinguish the areas of responsibility of the state and society in ensuring personal and public (national) security. Mass polls show that the population considers the state and society to be equally responsible for the moral components of personal security, and the state is responsible for protecting the personal data of citizens and ensuring public (national) security. Experts are inclined to believe that both personal, public, and national security in the digital network environment should be provided by authorities.

Acknowledgments

The reported study was funded by RFBR and EISR according to the research project No. 20-011-31535 "Public governance in a digital society: towards a new social contract".

References

[1] Acquisti A. Economics of information security. Camp LJ, Lewis S, editors. Boston, MA, USA: Springer; 2004. https://doi.org/10.1007/1-4020-8090-5_14

[2] Krivoukhov AA. To assess the level of personal security in the information and communication environment by the criminal. World of science. Series: Sociology, Philology, Cultural Studies. 2020;1(11 p.33).

[3] Hildebrandt M. Smart technologies and the end(s) of law: Novel entanglements of law and technology. Cheltenham: Edward Elgar; 2015.

[4] Nabbosa VL, Kaar C. Societal and ethical issues of digitalization. ICBDM 2020: Proceedings of the 2020 International Conference on Big Data in Management.New York, NY, USA: Association for Computing Machinery; 2020. https://doi.org/10.1145/3437075.3437093

[5] Royakkers L, Timmer J, Kool L, van Est R. Societal and ethical issues of digitization. Ethics and Information Technology. 2018;20(2):127-142.

https://doi.org/10.1007/s10676-018-9452-x

[6] Vasilenko LA. Public policy in digital society. Culture, Personality, Society in the Conditions of Digitalization: Methodology and Experience of Empirical Research Conference; 2020 Mar 19-21; Yekaterinburg, Russia. KnE Social Sciences. 2021;5(2):585-593. https://doi.org/10.18502/kss.v5i2.8404

[7] Babintsev VP, Sapryka VA. Opportunities of sociology in the time of troubles. World Applied Sciences Journal. 2013;26(12):1535–1537.

[8] Lukov VA, Lukov SV. Digitization in Russian society: Human dimension. Knowledge. Understanding. Skill. 2020;1:92-100. http://dx.doi.org/10.17805/zpu.2020.1.7