"Fake" as an Information Security Threat in the Conditions of Distribution of COVID-19

Kovaleva N.N.* Tugusheva Yu.M. Anisimova A.S.

Saratov State Law Academy, Saratov 410056, Russia
**Corresponding author. Email: kovaleva.natalia@mail.ru*

ABSTRACT
The article is devoted to the analysis of the current state of the spread of fake information in the context of the spread of the coronavirus. The analysis of the definition of "fake" is carried out, its characteristic features are revealed, including: complete or partial deliberate falsity of information; based on real information, relevant in a certain period of time; intentionally distributed through various sources; the goal is mass misinformation of the population; used to conduct information wars. Given the current situation, the authors provide various examples of inaccurate information. It is noted that the problem of fake content is global, almost all countries pursue a certain policy to suppress its distribution (Germany, Italy, France). The paper presents the data of a survey, which made it possible to establish that the majority of citizens trust the ordinary sites, and are rather skeptical about sites that publish official information. The article identifies the main directions for maintaining the required level of information security considering the spread of fake news about COVID-19.

Keywords: *fake, false information, information security, COVID-19, legal regulation*

1. INTRODUCTION

The spread of COVID-19 has brought about significant changes in economic and social life in many countries. One of the most striking consequences of the current pandemic is the accelerated adoption of digital technologies in a wide variety of areas.

As part of the government-imposed travel restrictions and social distancing measures, businesses and consumers are actively adopting digital solutions to continue operating remotely. Digitalization contributes to the transition to the online environment of medicine, work, education, allows to make online purchases, get more data on the spread of the virus and exchange information about research. The development of this trend speaks not only of an urgent need, but also of the created material base for the widespread use of digital technologies.

Despite the achievement of a certain high level of use, the introduction of digital technologies in the context of the spread of COVID-19 in the daily life of society, we cannot ignore the negative aspects that take place. Thus, new technological opportunities are used by attackers to obtain political and financial benefits. In particular, technologies are used to create fake news.

Today, one of such problems is the spread of fake news regarding the situation with COVID-19.

The spread of misinformation related to the COVID-19 outbreak is an unprecedented case: The World Health Organization (WHO) has already called the situation "infodemic" - an information pandemic. Shortly after the emergence of the new coronavirus, the WHO presented an information strategy for countering fakes as one of its four priorities in the fight against it. Its website debunks the most popular myths about the coronavirus, such as whether it is possible to protect against it with cocaine, garlic, etc. [1]. Among the main "carriers" are mobile platforms, first of all - the popular messenger WhatsApp, part of the American corporation Facebook. Through it, false messages are instantly spread among the citizens.

As for Russia, only by the beginning of May, the Safe Internet League revealed 3,701 fakes about COVID-19. Most often, they came from Moscow, St. Petersburg, Astrakhan region, Tatarstan, Crimea and some regions of the North Caucasus [2].

The effectiveness of fakes in the "digital age" has significantly increased in its "efficiency" owing to communication networks and technologies that enable the instant dissemination of a fake message among the "target audience" and multiply the impact on mass consciousness due to resonance in the media space and digital media.

2 MAIN CONTENT OF WORK

The very definition of "fake" in a broad sense is translated as "forgery, tampering, false" and means something deceitful, false, untrue, misleading [3]. It shall be noted that the abundance of fake messages disguised as news deserves serious scientific analysis. A number of authors have already turned to theoretical understanding of the "fake news" phenomenon [4-7].

Despite a number of scientific works aimed to the analysis of fake news, there are still no clear criteria for the definition and methodology of this concept. As M. Buyakevich notes, if we proceed from the fact that news is an operative informational message about events that have occurred recently or are occurring at the current moment having the political, economic or public interest for the audience in its freshness, then "fake news" is a message, which is stylistically created as real news, but false in whole or in part [8].

Fake news is considered as deliberately false "news" stories, deliberately spread through the media for the purpose of misinforming citizens, influencing the political and economic processes, for the information wars [9, 10].

In order to provide clarifications and a unified interpretation of such information, the Supreme Court of the Russian Federation, in a new Review of judicial practice on the application of legislation and measures to counter the spread of a new coronavirus infection, stated the following: "the deliberately false information, including the data on the circumstances of the spread in the territory of the Russian Federation of a new coronavirus infection (COVID-19) and (or) on the measures taken in this regard to ensure the safety of the population and territories, methods and methods of protection from these circumstances, one shall understand such information, which initially does not correspond to reality, of which the person who disseminated it was reliably aware" [11].

In addition, it was indicated that the circumstances of the spread of a new coronavirus infection (COVID-19) in the territory of the Russian Federation are the circumstances posing a threat to the life and safety of citizens, since their spread has now entailed and may still entail human casualties, damage to human health, the significant material losses and disruption of living conditions of the population, and measures taken to ensure the safety of the population and territories are aimed at countering its spread.

Considering the above, a number of specific features of fake news may be specified:

they are the wholly or partly deliberately false information;

they are created on the basis of reliable, real information that is relevant in a certain period of time;

they are deliberately distributed through the media, the Internet and other sources;

the goal is mass misinformation of the population;

they are used to conduct information wars.

Indeed, COVID-19 is the main news of 2019-2020, directly related to the life and health of every person, and the spread of fake news regarding him/her is a massive threat that brings confusion to society and casts doubt on reliable information about the situation in the country. Thus, in a number of regions of the country, the following unreliable data on coronavirus were revealed: a citizen spread false information about a high mortality rate from COVID in a local hospital; a YouTube video was revealed, in which it was reported that the new coronavirus infection is in fact "Feigelson-Jacobsen disease, the existence of which is hidden, it can only be infected by persons of certain nationalities" (the authors of the video claimed that "under the guise of combating coronavirus infection is a mass removal of internal organs from healthy people and their subsequent sale for transplantation); an article was published in which the authors argued that the COVID-19 virus was invented in the Vector laboratory, because, according to the authors, biological weapons were produced there, the article also questioned the official statistics [12].

The foregoing indicates that the spread of fake news in the context of the spread of COVID-19 poses a colossal danger in relation to information security of both a single region and the country as a whole.

2.1 Sociological research within the problem framework

In order to conduct the most complete research, we conducted a sociological survey of users of social networks Vkontakte, Facebook and Odnoklassniki on the topic "Fake as a threat to information security in the context of the spread of coronavirus".

The study results showed that the overwhelming majority of respondents (89.1%) believe in the existence of coronavirus and, of course, consider the stated topic to be very relevant.

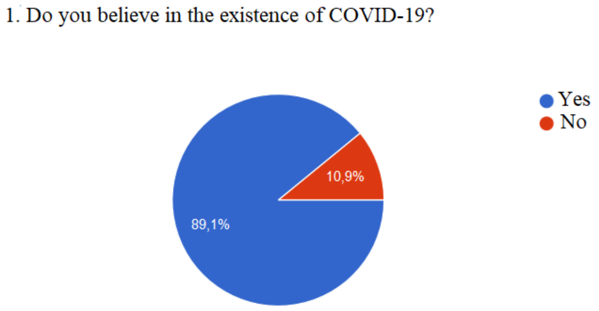

Fig 1. Do you believe in the existence of COVID-19?

The relevance of the declared topic is also confirmed by the fact that 86.1% of respondents are regularly interested in the latest news, publications about COVID-19, posted in various Internet sources, including the official and the so-called fake sites. Thus, for example, 59.4% of respondents prefer to find out the necessary information on such official sites as https://стопкоронавирус.рф, https://coronavirusstat.ru/, https://www.who.int/ru, rosminzdrav.ru, rospotrebnadzor.ru. The remaining 40.1% are aware of the presence of official sites, however, they prefer to receive information from unofficial sources.

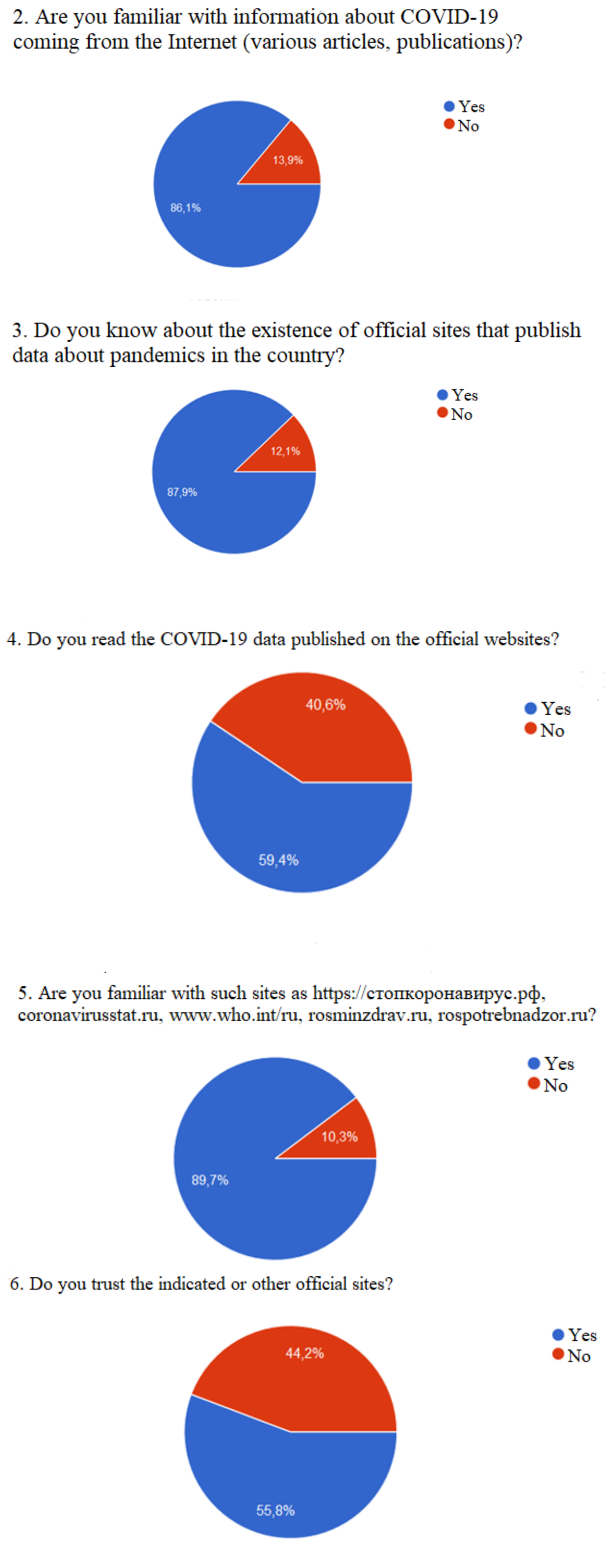

Fig 1. Any questions

The polling showed that only half of the surveyed audience (55.8%) expresses confidence in the above official sites regarding the information published there on COVID-19. Therefore, it can be assumed that it is precisely with the fact of "lack of trust" in official publications that the rest of the respondents (44.2%) turned to unofficial sources.

2.2 Legal analysis

The spread of fake news in the context of the spread of COVID-19 poses a threat to information security, by virtue whereof the tasks of combating fake content, which has considerable negative potential for socio-economic and political destabilization both in the regions and in the country as a whole, and here it is important to use the experience of different countries.

For instance, Germany has a Network Enforcement Act [13], also known as the Facebook Act. It is primarily aimed at combating fakes, defamation and hate speech on the Internet. In recent years, German politicians have increasingly expressed concerns about the virtual lack of responsibility for such acts on the Internet. Under the new "Alternatives for Germany" (AfD) (Censorship Act) law, the online platforms are now facing fines of up to € 50 mln if they do not delete "knowingly illegal" messages aimed to kindling hatred and other messages within 24 hours of being officially notified thereon [14].

An online portal was created by the Italian government in 2018 through which citizens can report fake news or fraudulent advertising. The Red Button project [15], invites users to provide their email address, a link to disinformation, and any social media sites where it is found.

The French National Assembly adopted a bill to counter the spread of false news. It was supported by the presidential party "The Republic On the Move", as well as the "Democratic Movement" party.

The main objective of the law, according to its developer Naima Moutchou, representing the ruling party, is "to prevent attempts at destabilization, in particular from outside France, which are based on the malicious dissemination of false information" [16].

The law provides for the administrative liability for disseminating false information in the period of three months before an election (presidential, parliamentary or European Parliament elections).

In Russia, amendments were also made to the current legislation regarding the distribution of fake news. These were adopted Federal Law of March 18, 2019 No. 27-FZ "On Amendments to the Code of Administrative Offenses of the Russian Federation", as well as Federal Law No. 31-FZ "On Amendments to Article 15-3 of the Federal Law "On Information, Information Technologies and Information Protection".

Both laws prohibit the dissemination of information on the Internet that creates "a threat of harm to the life or health of citizens, property, a threat of massive disruption of order and public safety, a threat of interfering with the functioning or termination of the functioning of vital facilities, transport or social infrastructure, credit organizations, energy facilities, industry or communications".

In order to ensure the activity of the constituent entities of the Russian Federation and municipalities and their executive authorities with comprehensive, operational, complete and relevant information, it is necessary, in the course of improving the information support of state and municipal authorities, to perform the intra-territorial integration and optimization of the information resource of the corresponding territories, regardless of the form of ownership. Information security of a constituent entity of the Federation and (or) a municipality is one of the essential factors ensuring the effective social-and-economic development of the respective territories. Information security is often understood as the state of protection of the vital interests of the individual, society and the state from external and internal threats in the context of the use of information technologies. At the same time, the implementation of information security measures allows to properly ensure the rights of right-holders to reliable information obtained in a legal way, protect all kinds of confidential information, preserve and enhance the cultural and spiritual and moral values, historical traditions and norms of public life [17].

Based on the foregoing, after analyzing the content of the Doctrine of Information Security of the Russian Federation [18], following main directions of activities for the implementation of information security measures in the subject of the Federation and in the municipality may be formulated:

forming, development and effective use of the state and municipal information resources;

identification of sources of threats to the vital interests of subjects in the field of information security;

creation of the safe information environment in which the information rights of citizens, the organizations and authorities are freely exercised;

ensuring safety of confidential information from unauthorized access to it as a result of implementation of prospecting actions of unfriendly subjects;

providing the reliable, complete, qualitative information provided in open access.

The listed areas shall be included in the list of powers of specific state bodies of the constituent entities of the Federation and municipal bodies.

According to V.B. Zotov, it is necessary to coordinate actions in the field of information security in connection with the complexity of emerging problems and the interconnectedness of activities. It is impossible to ensure such coordination only by the federal executive authorities, therefore it is advisable that the system coordinating actions in the field of information security be distributed over three levels: federal, subjects of the Federation and municipal, and also reflect the structure of scientific, technical, social and economic problems [18]. At the same time, the main coordinated problems at the levels of the constituent entities of the Federation and municipalities will be the following:

1. Development of models of threats to information security and forecasting the implementation of their consequences for a constituent entity of the Federation or a municipal formation.
2. Provision of an effective legal framework for the protection of the information resource of the subject of the Federation or municipal information resource, including the restricted information.
3. Systematization, accounting and provision of access to state and non-state information resources of a constituent entity of the Federation or a municipality on the basis of uniform legal norms [20].
4. Ensuring the general availability of information networks such as the Internet in a constituent entity of the Federation or a municipality.
5. Detection and suppression of the dissemination of tendentious and false information, manipulation of the public and personal consciousness of the population and authorities.
6. Preventing hacking of information systems and copying information by creating information security systems in a constituent entity of the Federation or a municipality.
7. Prevention of terrorism threats in relation to objects of information infrastructure of a constituent entity of the Federation or a municipal formation.
8. Providing state and municipal structures with the highly qualified information security specialists.

To implement the overall coordination of the resolution of the listed problems, the executive body of the subject of the Federation can create the Information Security Problem Scientific and Technical Council to define the specific approaches and methods of solution. At the same time, a network of coordinating councils at the most competent enterprises, institutions and organizations of the subject of the Federation could ensure the solution of specific organizational and technical issues.

Information security systems are currently being actively created in the constituent entities of the Federation, however, the inclusion of municipalities in this system is not yet active enough and represents one of the promising directions for the development of information security systems in Russia.

3. CONCLUSION

Considering the foregoing, the priority goals of using information technologies are the administration advancement, increase in the efficiency of the functioning of state and municipal bodies and the level of public safety, including:

– the modernization of information systems of state and municipal bodies, taking into account the goals and objectives of the administrative reform;

– the enhancement of the mutual influence of information flows of state and municipal executive authorities among themselves, as well as with legal entities and individuals on the basis of the creation and modernization of automated systems for personal registration of the population and other state registers and cadastres;

– the development and application of electronic regulations in the automation of various management and interaction processes;

– the provision of the effective interaction of automated control systems of government bodies responsible for security issues, as well as the prompt exchange of necessary information with citizens, organizations and other government bodies;

– the creation of effective systems for monitoring the state of public safety and emergency situations;

– the modernization of information systems for prompt response to violations of public order and emergencies.

All these areas of activity are inextricably linked with the ongoing administrative reform. Practically none of the projects for the deployment of information technologies in the sphere of state and municipal administration can be implemented without changing the corresponding functions and processes. Automation is preceded by streamlining of activities, the establishment of clear rules and the formalization of administrative procedures.

Thus, in order to maintain the country's information security in the context of the spread of fake news, a special role shall be assigned to mutual cooperation between all levels - federal, subjects of the Federation and municipal, whose coordinated actions will reduce the danger of such a phenomenon.

REFERENCES

[1] In secret all over the world, Rossiyskaya Gazeta. April 16, 2020.

[2] Fake-news and the pandemic: how legislation fights disinformation. https://pravo.ru/story/222165/

[3] E. N Shagalova, Dictionary of the latest foreign words. M., 2017.

[4] O.S. Issers, MEDIAFAKE: BETWEEN TRUTH AND HOAX, COMMUNICATION STUDIES 2 (2014) 112–123.

[5] S.N. Ilchenko, Fake journalism as an element of modern show civilization, Izvestia of the Ural Federal University. Ser. 1: Problems of Education, Science and Culture 153 (22-3) (2016) 14-18.

[6] I. Klishin, Maximum retweet: Fake propaganda on the new one, Vedomosti. 2014.

[7] A.P. Sukhodolov, Fake News as a Phenomenon of Modernity, Eurasian Cooperation: Humanitarian Aspects (2017) 87-105.

[8] M. Buyakevich, the Ministry of Foreign Affairs of the Russian Federation proposes to develop in the OSCE a clear definition of the concept of "fake news". URL: http://tass.ru/politika/4347718

[9] R. Ya. Kondratyev, N.G. Mironova, Fake news as a tool of social management and an object of application of information security methods, Modern Management Technology. 1 (91) (2020). URL: https://sovman.ru/article/9106/

[10] L. Tapia, Novel Coronavirus Disease (COVID-19) and Fake News in the Dominican Republic, The American Journal of Tropical Medicine and Hygiene 102 (6) (2020) 1172 - 1174

[11] Overview of selected issues of judicial practice related to the application of legislation and measures to counter the spread of a new coronavirus infection (COVID-19) N 1 in the Russian Federation (approved by the Presidium of the Supreme Court of the Russian Federation on April 21, 2020) // Bulletin of the Supreme Ships of the Russian Federation. 2020. No. 5.

[12] Fake-news and the pandemic: how legislation fights disinformation. https://pravo.ru/story/222165/

[13] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG).

[14] P. Oltermann, Tough new German law puts tech firms and free speech in spotlight, The Guardian. https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight

[15] Fake news: da oggi puoi segnalarle alla Polizia, Polizia di Stato. https://www.poliziadistato.it/articolo/155a6077fdb05e3865595940

[16] French Parliament adopts anti-false news law, TASS News Agency. https://tass.ru/mezhdu№arod№aya-pa№orama/5815447

[17] A.A. Vasiliev, Municipal Management System. M., 2010.

[18] Approved by the President of the Russian Federation on September 9, 2000 No. Pr-1895 (Rossiyskaya Gazeta. 2000, Sept. 28).

[19] V.B. Zotov, The system of municipal management in schemes: a textbook for the specialty "State and municipal management", Rostov, 2007.

[20] N.N. Kovaleva, A.Yu. Sokolov, K.S. Krotov. The establishment of digital law as the regulator of access to governmental information aiding the regional

development, Proceedings of the 1st International Scientific Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2019) / https: / /www.atlantis-press.com/proceedings/mtde-19/125907618 (WoS) https://doi.org/10.2991/mtde-19.2019.89