Legal Aspects of Information Threats in the Form of "Fakes" in the Conditions of Spread of COVID-19

Kovaleva N.N.* Anichkin S.A. Anisimova A.S.

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

ABSTRACT
The article discusses issues related to the spread of fake information during a pandemic. It is noted that the situation with coronavirus infection COVID-19 has led to significant changes in the habitual way of life of citizens - there has been a massive digitalization of most spheres of life, which has brought in both positive and negative aspects. One of the negative trends of what is happening is the widespread spread of false information about coronavirus infection. The research provides data from a survey of citizens in relation to fakes. The analysis of the regulatory legal framework of a number of foreign countries, including the Russian Federation, is carried out. It is noted that in order to combat the spread of fake information, including in the context of coronavirus infection COVID-19, coordinated actions are needed between federal, regional and municipal authorities.

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

1. INTRODUCTION

In the context of the spread of the new coronavirus infection COVID-19, information technology, which has become a priority among ordinary citizens, business, and the state as a whole, has acquired special attention. It is safe to say that the pandemic has had an unprecedented impact on various areas of human life, including its modern technological structure - almost all areas (except for industry) have switched to remote operation. Entire economy sectors have switched to telecommuting: primarily education, science, partly online services and trade.

On the one hand, this trend had a rather positive effect on both employers and employees of organizations - employers more and more willingly allowed their employees to work wherever they deem necessary. In the end, it doesn't matter if the task was completed on the couch, in a cafe, on the beach or at the office table, only the result matters. Thus, there is a transformation of existing jobs, causing the need for employees to acquire new skills to perform new tasks that, in turn, cause the need for continuous professional development, obtaining new knowledge throughout life, the ability to use new software, new automated and robotic technological processes [1, 2].

In addition, according to the OnePoll study, 69% of employees consider themselves to be more efficient when working remotely, 83% believe that this type of work will allow them to better balance work and personal life, and 77% said they would save money by not having to travel every day to the office [3].

At the same time, one can note the negative aspects of such changes, among them are the layoffs, unwillingness to pay compensation, the mandatory availability of equipment and Internet access to perform work, and, most dangerous, cybersecurity challenges.

2. MAIN CONTENT OF WORK

The increased attention to the coronavirus in the information and cyberspace became noteworthy, which inevitably highlighted the problematic issues of cybersecurity of information systems of all levels - from personal to international.

The relevance of information security issues is due to a synergistic effect, mainly determined by two factors (Fig. 1):

- a surge in attention to the problem at the media level, which led to a sharp increase in computer intrusions based on the social engineering methods;
- the quarantine measures that implement modern capabilities of remote work, which changed the established modes of safe and stable operation of systems on the Internet [4].

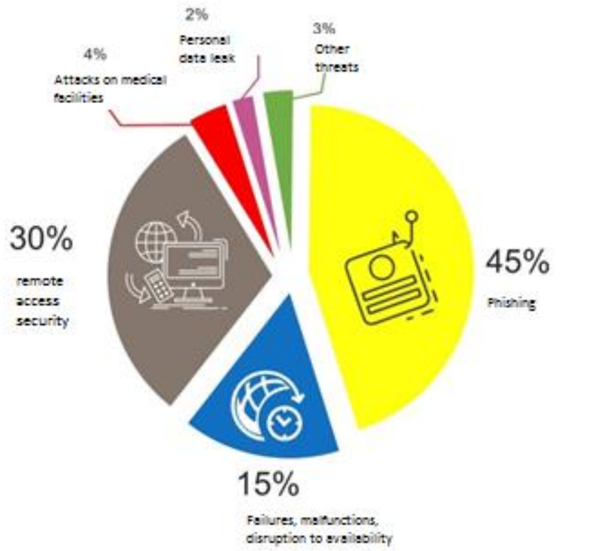

Figure 1 Distribution of threats relevant to coronavirus, according to their mentioning on the Internet

In addition to the above, there is an increase in cyberattacks on the healthcare and biomedical organizations; the leakage of personal data of subjects undergoing treatment, quarantine or self-isolation; the cyberattacks against online trading companies.

One of the most dangerous and massive threats in the context of COVID-19 is the spread of fake news. The threat consists in that inaccurate information is mostly published via the Internet - social networks, news feeds, various video hosting sites, etc.

Therefore, the danger of fake news consists in that:

1. fake messages are difficult to distinguish from real ones;
2. as a rule, they are based on reliable information, while the news authors bring their own tint thereto;
3. the dissemination of fake information can bring panic into society and a negative attitude towards real, reliable data, fear in relation to the actions of the state [5], and as a consequence to the entire system of the state;
4. the motive for disseminating unreliable information can be completely different: from a simple transfer of rumors, and ending with the purposeful provision of knowingly false information to the masses.
5. the coronavirus disease (COVID-19) has spread rapidly across the globe, having a devastating impact on the global economy, as well as on the social-and-economic structures of the region and society and the lifestyle of a huge population. The world is facing local contextual challenges that call for locally relevant and culturally appropriate COVID-19 interventions [6]

3. POLL DATA

In August-September 2020, a study on the topic "Fake information in the context of the spread of COVID-19" was conducted among the users of Vkontakte, Facebook and Odnoklassniki social networks. The survey results indicate that the absolute majority of respondents (100%) are familiar with the concept of "fake". When studying information on the spread of coronavirus infection, 81.8% believe that false, fake news takes place, and it can be found both in official and unofficial Internet sources.

1. Are you familiar with the concept of "fake" (Figure 2)

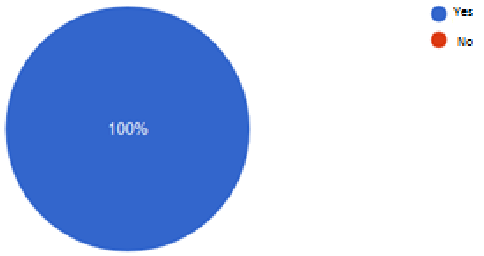

Figure 2 Poll result. Question No. 1

2. Is there any fake information about COVID-19? (figure 3)

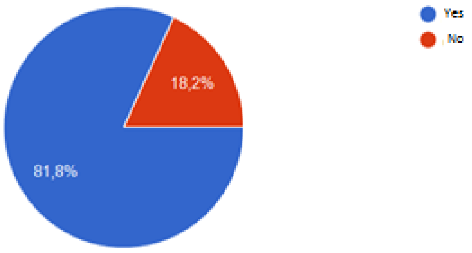

Figure 3 Poll result. Question No. 2

3. Have you encountered it?

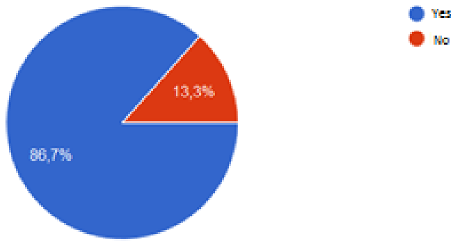

Figure 4 Poll result. Question No. 3

35% of respondents consider information about the real, relative to the pandemic, the situation in the country to be fake, 27% are sure that various sources publish false information about the number of people infected, 17% consider false information about methods of treatment. 21% drew attention to the propaganda on the Internet of various "myths" about the occurrence of coronavirus infection.

In connection with the above, a natural question arises: "How and by what criteria can an Internet user distinguish the information received into true and false?". The survey identified the following popular ways to determine the degree of truthfulness of information presented on the Internet:

- I compare information from several sources; the true one is the interpretation favored by more sources (45%);
- the information contradicts official sources, which means that the information is false (39%);
- I trust the author, because I know him/her personally, which means that the information is true (11%).

In addition, the respondents expressed the following individual opinions:

- I trust foreign official sources (1.2%);
- I compare several sources with a good reputation and analyze (1.2%).
- I try not to dwell on this topic (0.6%);
- Russian citizens are often deceived in official sources, therefore I have more confidence in information from eyewitnesses or scientists (but not those who appear on television, but who shoot their videos on the Internet and soon get blocked) (0.6%);
- assessment of information in a complex, taking into account the known (0.6%);
- I rely on intuition (0.6%).

4. How can you determine the falsity/truthfulness of information from unofficial sources? (figure 5)

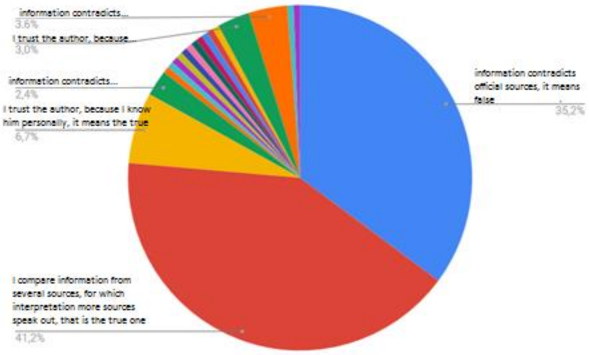

Figure 5 Poll result. Question No. 4

4. LEGAL FRAMEWORK ANALYSIS

At a time when a common strategy for combating fake news is being developed at the European level, certain shifts have already taken place in the legislation of some Asian states towards the introduction of such control or the tightening of the existing regime.

For example, in April 2018, Malaysia passed a bill against fake news. Their distribution is subject to serious sanctions. Punishment up to 6 years in prison can be imposed not only for initiating false information, but also for reposts. The law is aimed not only at the media, the Internet, but also at society as a whole. Therefore, any person who published a post with unverified or false information on a social network becomes an offender. Legislators imply that the functioning of a civil society is possible only with the full responsibility of everyone for his/her actions.

According to the law, fake is considered "any news, information and any data that fully or partially do not correspond to reality, in the form of articles, audiovisual recordings or any other form capable of transmitting/suggesting words and ideas" [7].

The Malaysian authorities believe that such a law is aimed primarily at protecting citizens and businesses from online attacks. According to Sally Said Kerouac, the Minister of Communications and Multimedia: "Society wants a law that could protect the citizens of the country from fake news. If you become a victim of something virtual and at the same time false, your life can be destroyed" [8].

India has had a separate Ministry of Information and Broadcasting for a long time. It is it that resolves conflicts related to news and publications. Thus, in 2018, it issued a decree according to which journalists will be punished for spreading fakes by revoking their license for a certain time.

The tendency to regulate false information is generally observed in many countries. For example, the Philippines passed the Malicious Distribution of False Information and

Other Related Violations Act. The main emphasis is put on the criminogenic feature in the form of consequences. According to the definition contained in the document, information that "causes panic, chaos, discord, violence or hatred, as well as information containing propaganda elements aimed at denigrating or discrediting a person" is considered false. Any publicly available publication can form a directly socially dangerous act. In the event of an admission of guilt, the subject is liable in the form of a fine or imprisonment. The punishment by a fine can reach up to 100 thousand dollars, and the punishment of imprisonment can be calculated for a period of up to 5 years.

It shall be noted that the law "On fake news" adopted in Russia is quite similar to the Philippine law. Thus, Federal Law No. 31-FZ of March 18, 2019 "On Amendments to Article 15.3 of the Federal Law "On Information, Information Technologies and Information Protection" establishes a ban on the dissemination of false information that may be socially significant. The publication of such false information that is disseminated under the guise of reliable messages and which creates a threat of harm to the life and (or) health of citizens, property, the threat of mass disturbance of public order and (or) public safety, or the threat of interfering with the functioning or termination of the functioning of facilities is subject to restrictions life support, transport or social infrastructure, credit institutions, energy facilities, industry or communications [9]. A special blocking procedure is established. According to the new law, the Prosecutor General of the Russian Federation or his/her deputies will apply to Roskomnadzor with a demand to take measures to restrict access to information resources disseminating such information. The punishment for such an offense is set from 30,000 to 10 million rubles, depending on the subject of the offense (Article 13.15 of the Code of Administrative Offenses of the Russian Federation), and criminal liability has been provided for public dissemination of knowingly false information about circumstances posing a threat to the life and safety of citizens (Article 207.1 of the Criminal Code of the Russian Federation), as well as for the public dissemination of knowingly false socially significant information, which entailed grave consequences (Article 207.2 of the Criminal Code of the Russian Federation).

5. CONCLUSIONS

In modern conditions of comprehensive development and implementation of information technologies, as well as all kinds of threats and risks, citizens need to increase the general level of public safety, law and order and safety of the environment through a significant improvement in the coordination of the activities of forces and services responsible for solving these problems [10,11].

Being aware of the scale, speed and strength of the negative impact on the economy of fake news spread through instant messengers and social networks, a number of American Internet companies (Facebook, Twitter, Microsoft, Google, YouTube, Reddit) recently announced that they were joining forces in the fight against fake news about COVID-19. [12] Understanding the impact of social networks on collective consciousness and behavior, nowadays almost all countries use social networks to influence the minds of citizens, while striving to control aspects of social networks. For example, China, in an effort to limit the influence of Western propaganda tools and reduce the destructive influence of fakes, uses the national social networks Weibo, WeChat, QQ as a means of propaganda and counterpropaganda as well. Social networks and messengers had a significant impact on the mass behavior of 7/12 people and became the reason for the adoption of various laws by countries in the field of information security [13]

The very activity of the legislator on the issue of protecting public interests and public safety is fully justified and necessary. This was also stated in the explanatory note to the bill: "in the modern conditions of development of information technologies, the uncontrolled dissemination of inaccurate information disseminated under the guise of reliable messages can have a wide range of consequences associated not only with the reputational losses of citizens and organizations, manipulation of public opinion and financial gain, but also create a real danger to life and health citizens, lead to riots, create a threat to state, public or environmental security. Awareness of the negative aspects of the dissemination of false information prompts government institutions in many countries to search for mechanisms to suppress it" [14].

One cannot but agree with what has been said, because there has always been false or inaccurate information from the very beginning of the mass use of digital technologies. And with the large increase in the number of Internet users, "negative" information has increased in direct proportion. The dissemination of information has long been a new weapon. And if the ordinary weapons are used to shoot at individual people, the provocations and fakes are often capable of shooting at an entire society.

The most common means of transmitting false information is primarily the Internet, which greatly complicates the entire process of tracking such information. The problem is that the country lacks an effective legal mechanism for regulating relations arising from the use of digital technologies, as well as inadequate coordination between the federal, regional and municipal levels.

According to V.B. Zotov, ensuring information security and the solution of the arising problems demand the coordinated actions. Such coordination cannot be ensured only by the federal executive power bodies. It would be more expedient to have a system of coordination of activities in the field of information security, distributed at the levels of federal, regional and local government, reflecting the structure of scientific, technical and social-and-economic problems in the field of information security [15].

General coordination of the solution to this problem can be carried out by the Scientific and Technical Council on Information Security Problems of the Administration of the Subject of the Russian Federation, and it is advisable to assign the solution of specific organizational and technical coordination issues to the most competent enterprises, institutions and organizations of the region. For this, appropriate coordination councils can be created thereunder.

Thus, the current situation with the coronavirus infection, the massive dissemination of fake information regarding it throughout the country, as well as abroad, contributed to the development of new means of combating such data, as well as the adoption of measures of responsibility for such actions.

REFERENCES

[1] Tomashevskiy K.L. Tsifrovizatsiya i yeye vliyaniye na rynok truda i trudovyye otnosheniya (teoreticheskiy i sravnitel'no-pravovoy aspekty) // Vestnik sankt-peterburgskogo universiteta. Pravo. 2020. № 2. T. 11. S. 398-413/

[2] Filipova I.A. Trudovoye pravo: vyzovy informatsionnogo obshchestva // Pravo. Zhurnal vysshey shkoly ekonomiki. 2020. № 2. S. 162-182.

[3] Novaya norma: kak udalennaya rabota menyayet biznes-protsessy. URL: https://www.comnews.ru/content/205478/2020-04-09/2020-w15/novaya-norma-kak-udalennaya-rabota-menyaet-biznes-processy (data obrashcheniya 10.09.2020 g.)

[4] Markov A.S. Informatsionnaya bezopasnost' v usloviyakh pandemii COVID-19. URL: https://expert.ru/2020/04/9/informatsionnaya-bezopasnost-v-usloviyah-pandemii-covid-19/ (data obrashcheniya 08.09.2020 g.)

[5] Erku D.A., Steadman K.J., Belachew S.A., Abrha S., Thomas J., Sinnollareddy M., Tesfaye W.H. When fear and misinformation go viral: pharmacists role in deterring medication misinformation during the infodemic surrounding COVID-19// Research in Social and Administrative Pharmacy. 2020. DOI: 10.1016/j.sapharm.2020.04.032 (Scopus)

[6] Renzaho A.M.N. The need for the right socio-economic and cultural fit in the COVID-19 response in sub-saharan AFRICA: examining demographic, economic political, health, and socio-cultural differentials in COVID-19 morbidity and mortality// International Journal of Environmental Research and Public Health. 2020. T. 17. № 10. S. 3445. DOI: 10.3390/ijerph17103445 (Scopus, WoS)

[7] As Malaysia Moves to Ba№ ‘Fake №ews,’ Worries About Who Decides the Truth // The New York Times Company. URL https://www.№ytimes.com/2018/04/02/world/asia/malaysia-fake-№ews-law.html (data obrashcheniya: 30.08.2020 g.).

[8] Kira Latukhina. V Kremle nazvali zakonoproyekt o feykovykh novostyakh produmannym // Rossiyskaya gazeta. URL: https://rg.ru/2019/03/13/v-kremle-№azvali-zako№oproekt-o-fejkovyh-№ovostiah-produma№№ym.html (data obrashcheniya: 25.08.2020 g.).

[9] Federal'nyy zakon ot 18.03.2019 N 31-FZ "O vnesenii izmeneniy v stat'yu 15.3 Federal'nogo zakona "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" // Sobraniye zakonodatel'stva RF. 2019. № 12. St. 1221.

[10] Pastukhov P.S., Losavio M. Ispol'zovaniye informatsionnykh tekhnologiy dlya obespe cheniya bezopasnosti lichnosti, obshchestva i gosudarstva // Vestnik permskogo universiteta. Yuridicheskiye nauki. 2017. № 36. S. 232.

[11] Facebook, Microsoft i Twitter pomogayut razrabotchikam borot'sya skoronavirusom //Vesti.ru. – 26 marta 2020. – URL:https://www.vesti.ru/doc.html?id=3251430 (data obrashcheniya 09.09.2020)

[12] Chamola V., Hassija V., Gupta V., Guizani M. A comprehensive review of the COVID-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact //IEEE Access. 2020. T. 8. S. 90225-90265. DOI: 10.1109/ACCESS.2020.299234 (Scopus, WoS)

[13] Kondrat'yev R.YA., Mironova N.G. Feyk-novosti kak instrument sotsial'nogo upravleniya i ob"yekt primeneniya metodov informatsionnoy bezopasnosti // Sovremennyye tekhnologii upravleniya. 2020. № 1 (91). S. 6.

[14] Zakonoproyekt № 606593-7 «O vnesenii izmeneniy v stat'yu 15-3 Federal'nogo zakona «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» // Sistema obespecheniya zakonodatel'noy deyatel'nosti. URL: http://sozd.duma.gov.ru/dow№load/22B01AE9-C148-4D7F-984E-2F7AFED09B9D (data obrashcheniya: 25.02.2020).

[15] Zotov V.B. Sistema munitsipal'nogo upravleniya v skhemakh: uchebnoye posobiye. 2-ye izd-ye. Rostov-na-Donu: Feniks, 2007. 180 s.