Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Ensuring information security in social networks: experience of Uzbekistan and Kazakhstan

Shokhjakhon KHUJAYEV[1]

Tashkent State University of Law

ARTICLE INFO

Article history:
Received April 2021
Received in revised form
28 April 2022
Accepted 20 May 2022
Available online
10 June 2022

Keywords:
information security,
crime,
information space,
coronavirus,
information threats,
virtual world,
blogger.

ABSTRACT

Currently, information security in social networks is increasingly becoming the focus of public attention, arousing interest among scientists and specialists. In this article, based on the norms of the legislation of the Republic of Uzbekistan and the Republic of Kazakhstan on information security and informatization, the features of the legal regulation of information security mechanisms in social networks were analyzed. The legislation of the Republic of Uzbekistan and the Republic of Kazakhstan does not provide for a separate regulatory legal act in the field of regulation of social networks, including ensuring information security, in connection with which the author points out the importance of taking preventive measures. According to the results of the article, it is indicated that when distributing content that threatens the information security of an individual, society and the state, measures of filtering and blocking content, as well as restrictions on access to social networks, can be applied. In general, it is noted that effective legal regulation should be based on the simplicity of the legal mechanism, the maximum simplification of the legal burden, as well as a clear and fair restriction of access to social networks.

DOI: https://doi.org/10.47689/2181-1415-vol3-iss5/S-pp322-329

[1] PhD in Law, Head of Department at Tashkent State University of Law. Tashkent, Uzbekistan.
E-mail: intertoto50@gmail.com

Ижтимоий тармоқларда ахборот хавфсизлигини таъминлаш: Ўзбекистон ва Қозоғистон тажрибаси

АННОТАЦИЯ

Калит сўзлар:
ахборот хавфсизлиги,
жиноятчилик,
ахборот муҳити,
коронавирус,
ахборот хавф-хатарлари,
виртуал олам,
блогер.

Бугунги кунда ижтимоий тармоқларда ахборот хавфсизлиги тобора жамоатчилик диққат марказида бўлиб, олим ва мутахассисларда қизиқиш уйғотмоқда. Ушбу мақолада Ўзбекистон Республикаси ва Қозоғистон Республикасининг ахборот хавфсизлиги ва ахборотлаштириш тўғрисидаги қонун ҳужжатлари нормаларига асосланиб, ижтимоий тармоқларда ахборот хавфсизлигини таъминлаш механизмларини ҳуқуқий тартибга солиш жиҳатлари таҳлил қилинган. Ўзбекистон Республикаси ва Қозоғистон Республикаси қонунчилигида ижтимоий тармоқларни тартибга солиш, шу жумладан, ахборот хавфсизлигини таъминлаш соҳасида алоҳида норматив-ҳуқуқий ҳужжат кўзда тутилмаган, шу муносабат билан муаллиф бу масала юзасидан профилактика чораларини кўриш муҳимлигини таъкидлайди. Мақола натижаларига кўра, шахс, жамият ва давлатнинг ахборот хавфсизлигига таҳдид соладиган контентни тарқатишда уни фильтрлаш ва блокировка қилиш чоралари, шунингдек ижтимоий тармоқлардан фойдаланишни чеклаш каби чораларнинг қўлланилиши мумкинлиги кўрсатилган. Умуман олганда, самарали ҳуқуқий тартибга солиш ҳуқуқий механизмнинг соддалигига, ҳуқуқий мажбуриятнинг максимал даражада соддалаштиришга, шунингдек ижтимоий тармоқлардан фойдаланишни аниқ ва адолатли тарзда чеклашга асосланиши кераклиги таъкидланган.

Обеспечение информационной безопасности в социальных сетях: опыт Узбекистана и Казахстана

АННОТАЦИЯ

Ключевые слова:
информационная безопасность,
преступность,
информационное пространство,
коронавирус,
информационные угрозы,
виртуальный мир,
блогер.

В настоящее время информационная безопасность в социальных сетях все чаще оказываются в центре внимания общественности, вызывая интерес среди ученых и специалистов. В данной статье на основе норм законодательства Республики Узбекистан и Республики Казахстан об информационной безопасности и информатизации были проанализированы особенности правового регулирования механизмов обеспечения информационной безопасности в социальных сетях. Законодательство Республики Узбекистан и Республики Казахстан не предусматривает отдельного нормативно-правового акта в сфере регулирования социальных сетей, включая обеспечение информационной безопасности, в связи с чем автор указывает важность принятия профилактических мер. По итогам статьи указывается, что при распространении контента, угрожающего информационной безопасности личности, общества и государства могут быть применены меры фильтрации и блокировки контента, а также ограничения доступа к социальным сетям. В целом отмечается, что эффективное правовое регулирование должно основываться на простоте правового механизма, максимальном упрощении юридического бремени, а также в четком и справедливом ограничении доступа к социальным сетям.

To date, the widespread use of the Internet has become a key factor in the formation and development of relations in the virtual space. The issues of protecting information on the Internet, as well as the Network users themselves from illegal information influence, have become particularly relevant. Now, when more than 400 million cases of coronavirus have been detected in the world, the whole world is forced to spend most of its time at home. In Uzbekistan, this figure exceeds 236 thousand, in Kazakhstan – 1,39 million some of whom are under observation in home or inpatient quarantine. In these conditions, more than ever, it is the Internet that remains the most widespread and effective mechanism for spending leisure time. Therefore, a very topical issue arises on the agenda – the relationship between the Internet and information security in the context of the coronavirus pandemic. In our opinion, the negative aspects in relation to information security can be traced in the following:

1. Dissemination of false and defamatory information in social networks.

As a result of the spread of the coronavirus pandemic, it was the Internet that became the resource through which people began to receive information quickly. During the coronavirus pandemic, the flow of information increased in the virtual space, resulting in an increased flow of unprocessed and false information on the Internet. Fakes have become difficult to distinguish due to the following reasons:

– these news items are often disguised as ordinary news and therefore easily cause panic;

– users believe a source with a large number of subscribers, so the bulk, or rather every fifth fake news falls under existing websites that can easily be found on Google [14];

– the presence of a huge array of fakes, and therefore it is difficult to determine the legitimate information. So, according to the HSE statistics, every tenth Russian is sure that the pandemic is "the invention of interested parties" and does not believe the official statistics [3]. All this proves that people trust fakes more than official sources.

In our opinion, these problems require consistent and non-repressive measures, in particular, the creation of Information and analytical centers for monitoring the media and social networks, as well as other resources on the Internet under the Public Fund for the Support and Development of National Mass Media, established at the end of January 2020 [4].

2. Content on the Internet clearly indicates the presence of a low level of legal awareness, and also contributes to a decrease in the level of trust in social networks.

In the last month on the Internet, you can observe a certain decline in the level of legal awareness of the population. This can lead to examples of disobedience to the authorities, expressed in violation of the rules of quarantine, established prohibitions, as well as public peace and security. Thus, it can be noted with regret that during the first month of quarantine in the Republic of Uzbekistan, 51182 administrative offenses were committed [5], which indicates that certain categories of offenders do not perceive or ignore the established prohibitions. Such offenses seem insignificant, but in the future they can provoke much more serious crimes. There is also concern about the low culture and nihilism of celebrity individuals. By their actions, these individuals not only set a bad example, but also create a sense of collective irresponsibility among the population.

Evidence of low legal awareness is also an insufficient level of knowledge and outlook. Analysis of texts on the Internet has shown that every year the number of cases of using illiterate and sometimes stupid texts with errors is growing. According to the site https://hype.tech almost every user makes mistakes, including abbreviations and other errors. About 2 % of users can't correctly identify the endings of words. It is also worth noting that public criticism of their illiteracy sometimes causes discontent, great indignation of the Internet community, due to the overwhelming number of them [6]. Such a case may indicate that the Internet “encourages” illiteracy in a certain way.

Cyber fraud has also become one of the biggest problems of trust on the Internet. In the last two or three years, the number of scammers in the Internet segment has increased significantly for a number of reasons. So, with the advent and growing popularity of such a phenomenon as social networks [7], the number of Internet users who came to the Internet in order to search for their friends and acquaintances has increased, which is actively used by scammers themselves, luring “victims” into virtual relationships. On the other hand, the spread of social services has become a bad example for trust, especially in cases where there are cases of spam and phishing that violate information security and contribute to the extortion of electronic money on the Internet. Of particular concern are the facts of the activation of virtual scammers during the coronavirus pandemic, when scammers use the topic of coronavirus as a “bait” and ask to click on the link in letters allegedly sent from the bank. These emails may contain a “trap site”. So, in the Russian Federation during the pandemic, the number of domains with the word "coronavirus" increased-by 4 thousand at once. In addition, the number of phishing mailings increased by 30%. The purpose of such mailings is to find out passwords, usernames, and card details by faking messages from a trusted source. Phishing pages are very similar to the original pages of the banks' website, as a result of which people become victims of criminals [12].

In our opinion, one of the reasons for this level of low legal awareness and credulity of users is the lack of educational support. The lack of necessary knowledge in the field of the Internet and information and communication technologies creates a favorable ground for reducing the overall level of legal awareness. In this regard, it is necessary to form a three-stage system of education for appropriate skills in the information and communication space:

1) today, the skills of using information and communication technologies are generally taught in the framework of computer science, but there is no special subject study of information security issues in general terms, and therefore a special discipline should be introduced in general education schools regarding the concept and essence of the Internet, this discipline should also provide training in primary use skills and behavior in virtual space;

2) it is necessary to create a program of advanced training and retraining of personnel engaged in operational search activities, inquiry or investigation of crimes related to information security in law enforcement agencies.

In general, the problem of legal awareness and trust in the Internet is a complex problem. In this part, it is necessary to form a kind of **Internet culture** on the part of users of the virtual space by conducting courses and introductory lessons (including video lessons that can be viewed offline), brochures and other interesting materials.

3. Inciting conflicts in social networks.

Freedom of speech and increased opportunities for the comprehensive use of information and communication technologies do not fully ensure the reliability and public utility of the information disseminated. It is no secret that today any person, especially a blogger, has a more impulsive and effective impact on the consciousness of society than, for example, the media. At the same time, bloggers can post unlimited information of various kinds. According to statistics, users prefer to use the Internet most of all to access political (54%), medical (46%) or government information (42%) [8]. At the same time, the publication of information about the activities of terrorist organizations is not excluded. Facebook Instagram, Facebook, Twitter, Instagram, and Friendica, the main propagandists of the Islamic State, have effectively used Western communication technologies to cover the war zone and recruit foreign citizens. Thousands of accounts, the use of Twitter Storm during combat operations to create panic behind enemy lines, thousands of videos of supporters of the movement and tens of millions of views testify to the destructive power of the impact of information. These media resources mainly carry out their activities on the World Wide Web due to its availability.

The coronavirus has created the ground for manipulating public opinion and consciousness. For example, content analysis of destructive propaganda texts during the coronavirus pandemic and comparison of these texts with the texts of journalists and experts writing articles on countering extremism at the same time demonstrated that the level of impact of destructive texts is much stronger and more convincing [10]. In Syria, President Bashar al-Assad, taking advantage of the coronavirus case, accused the US of trying to use the coronavirus to its advantage, and also expressed condolences to the Iranian citizens affected by the COVID-19 pandemic caused by the coronavirus, hence showing his loyalty to Iran. However, the political enemies of Assad, on the contrary, used this case as a good opportunity to discredit the leader of the country and call people to sabotage [15]. In the Russian Federation, the conditions of the coronavirus have become reasons for various kinds of rallies and marches. So, in Vladikavkaz on April 20, 2020, a popular gathering of several thousand citizens took place against the self-isolation regime, demanding the resignation of the head of the region and the dissolution of the republican parliament [14].

The most important condition that contributes to the violation of information security is the inconsistency of legislation in terms of regulating relations to ensure information security.

The period of quarantine in connection with the coronavirus has shown that the only thing worse than the coronavirus is the panic due to the coronavirus. Every day, various messengers or websites on the Internet publish news about mass infections and deaths, about the depletion of food resources, about the introduction of a curfew or a state of emergency. Despite the presence of official sources, cases of spreading fakes about the coronavirus have increased on the Internet. So, in Austria, an audio recording was distributed in which a woman says in an agitated voice that she is in the hospital, and everyone who has severe symptoms of the coronavirus has taken ibuprofen. The woman introduces herself as Pauline, the mother of a girl named Poldy. This is fake: doctors did not call ibuprofen the cause of the activation of the coronavirus, but users willingly shared the record, misleading their loved ones [9].

The coronavirus for Uzbekistan has also become a kind of push towards a critical revision of the legislation. So, during the period of the coronavirus, 16 presidential decrees and resolutions were adopted aimed at mitigating the impact of the pandemic on the economy.

One of the problems during the coronavirus was the lack of legislative norms establishing responsibility for the dissemination of false information about the coronavirus, as well as non-compliance without good reason in the conditions of the emergence and spread of quarantine and other dangerous human infections with the requirements for medical examination, treatment and arrival at the places designated for quarantine and non-admission of these places in the prescribed period, disclosure of information about persons., with whom there was contact and places of visit during the period of risk of infection with the disease, as well as other legal requirements of the state sanitary supervision authorities. The solution to this problem, albeit belatedly, was the introduction of amendments to Article 54 of the Code of the Republic of Uzbekistan of Administrative Responsibility and Article 257[1] of the Criminal Code of the Republic of Uzbekistan, as well as the establishment of criminal liability for the dissemination of false information about the spread of quarantine and other dangerous infections in the conditions of the occurrence and spread of quarantine and other dangerous infections.

The next problem is the freedom and irresponsibility of the blogger. The free use of information and communication technologies and the Internet can lead to certain negative consequences. For example, this has a particularly negative impact on everyday users. Like any State, the Republic of Uzbekistan also intends to address the issue of preventing the spread of negative content. Thus, in early April 2020, the Ministry of Internal Affairs of the Republic of Uzbekistan put up for discussion a draft resolution of the President of the Republic of Uzbekistan “On measures to further improve the system of prevention of offenses among minors and youth”. Paragraph 9 of the Roadmap for the implementation of the project provides for the creation of a virtual group of patriot bloggers from among the members of the Youth Union, students of the Tashkent State University of Information Technologies and volunteers, who are assigned the tasks of preventing negative content, filtering Internet resources, etc. However, this measure is not complete, but only helps to identify one of the sides of the problem. Considering the problems of the negative impact of the Internet on the consciousness of people, we can note that in the framework of our doctoral dissertation and scientific articles published within it, we pointed out an integrated approach to solving problems. To this end, we consider it appropriate to adopt a State program for the formation of Internet Culture, which includes a set of measures – conducting trainings, special courses in educational institutions, preparing and distributing propaganda materials (flyers, stands, presentations) in the media and on the Internet. In these conditions, social measures are becoming important, which are aimed at creating awareness among people, in particular young people, of the danger and negative consequences of crimes in the field of information technology and security.

In recent years, a number of measures have been implemented in the Republic of Kazakhstan to improve the information security system of the state. In accordance with the National Security Strategy of the Republic of Kazakhstan [13], the Concept of Information Security was developed and adopted, providing for the implementation of a set of legal, organizational, scientific and technical measures aimed at forecasting, identifying, preventing and suppressing threats in the field of information security.

The main regulatory legal act regulating relations in the field of security in Kazakhstan is the Law of the Republic of Kazakhstan "On National Security", which regulates legal relations in the field of national security of the Republic of Kazakhstan and defines the content and principles of ensuring the security of man and citizen, society and the state, the system, goals and directions of ensuring national security of the Republic of Kazakhstan. Among the types of national security, information security is singled out as a separate type. Information security is the state of protection of the information space of the Republic of Kazakhstan, as well as the rights and interests of man and citizen, society and the state in the information sphere from real and potential threats, which ensures sustainable development and information independence of the country [9]. Article 6 of this Law defines the following among the main threats to national security: reducing the level of protection of the country's information space, as well as national information resources from unauthorized access; informational impact on public and individual consciousness associated with the deliberate distortion and dissemination of false information to the detriment of national security. Accordingly, the level of security determines the quality of national security, allowing us to assess the effectiveness of measures to prevent modern threats and measures to prevent and eliminate them. In the sphere of the information space, these threats are especially dangerous, since it is through information that an individual forms an idea of the world around him, his worldview and motivations for certain actions.

The second side of the problem is the lack of specific measures of responsibility. At the same time, the legislation provides for existing prohibitions on the "use" of the Internet in a negative sense. According to Article 12^1 of the Law of the Republic of Uzbekistan «On Informatization», the owner of a website and (or) a website page, including a blogger, is obliged to prevent the use of his website and (or) a website page on the world information network of the Internet, where publicly available information is posted, for the purposes of:

– call for violent change of the constitutional order, territorial integrity of the Republic of Uzbekistan;

– calls for mass riots, violence against citizens, as well as participation in meetings, rallies, street processions and demonstrations held in violation of the established order, as well as coordination of these illegal actions;

– dissemination of deliberately false information containing a threat to public order or security;

– propaganda of war, violence and terrorism, as well as ideas of religious extremism, separatism and fundamentalism;

– disclosure of information constituting state secrets or other secrets protected by law;

– dissemination of information that incites national, racial, ethnic or religious hostility, as well as discrediting the honor and dignity or business reputation of citizens, allowing interference in their private lives;

– dissemination of information, including those expressed in an indecent form, demonstrating disrespect for society, the state, and state symbols;

– promotion of narcotic drugs, psychotropic substances and precursors;

– propaganda of pornography, the cult of violence and cruelty, as well as incitement to commit suicide;

– dissemination of information aimed at inducing or otherwise involving citizens, including minors, in committing illegal actions that pose a threat to their life and (or) health or to the life and (or) health of other persons;

– committing other actions that entail criminal and other liability in accordance with the law [1].

However, the above actions do not entail liability under either the legislation of the Republic of Uzbekistan and the Republic of Kazakhstan, as a result of which **appropriate measures of responsibility should be established**, namely, to establish administrative and criminal liability for the illegal actions of the blogger. In turn, it is necessary to provide for the **possibility of closing websites or other resources on the Internet by a court decision, since the court is the final instance that administers justice**.

Thus, it can be noted that the main step that is advisable to apply is the formation of a kind of Internet culture, the implementation of which should be carried out not only by repressive measures, but also by educational measures. It is thanks to the conscious choice of the behavior of a person in the information and communication space that it is possible to ensure the protection of information security in the virtual space. It is also necessary to take appropriate institutional and organizational measures to ensure the protection of the interests of the individual, society and the state in the virtual space.

REFERENCES:

1. Law of the Republic of Uzbekistan “On Informatization” (the text in Russian is available at: https://www.lex.uz/docs/82956).
2. Law of the Republic of Kazakhstan “On National Security of the Republic of Kazakhstan” (the text in Russian is available at: https://online.zakon.kz/Document/?doc_id=31106860).
3. Rasulev A.K. “Improvement of criminal-legal and criminological measures of fight against crimes in the sphere of information technologies and safety: Doctoral (DSc) dissertation abstract on legal sciences”. (2018).
4. https://www.gazeta.uz/ru/2020/01/23/fund/.
5. https://pv.uz/ru/news/samoe-bolshoe-chislo-narushenij-po-karantinu.
6. https://hype.tech/@boevoy-homyak/problema-bezgramotnosti-v-internete-tak-li-vse-ploho-qqk4fmkw.
7. https://www.saferunet.ru/adult/news/790/.
8. www.statista.com.
9. https://www.bbc.com/russian/features-52066878.
10. https://crss.uz/2020/04/02/analiz-tekstovyx-i-vizualnyx-soobshhenij-propagandy-destruktivnyx-grupp-v-seti-internet-issledovanie/.
11. https://www.rbc.ru/economics/07/03/2020/5e6355ac9a7947a8e27817e6.
12. https://regnum.ru/news/economy/2915482.html.
13. https://articlekz.com/article/6210.
14. https://runet.rbc.ru/.
15. https://lenta.ru/news/2020/04/20/asadvsusa/.