*European Research Studies Journal*
*Volume XXI, Special Issue 2, 2018*

*pp. 253-262*

# Acquisition, Storage and Dissemination of Socially Dangerous Information: Theoretical and Methodological Issues of the Legal Prohibition

A.S. Klementev[1], O.V. Khlopkova[2], E.V. Chervonnykh[3], V.N. Sizova[4]

***Abstract:***

*The research project is focused on the Russian and foreign practice of the legal prohibition of acquisition, storage and dissemination of socially dangerous information on the Internet.*

*Other objects of studies include legal restrictions on freedom of the media in order to protect the constitutional order, the interests of the citizens and the security of the state.*

***Keywords:*** *Modern technologies, socially dangerous information, modern computing technologies, negative content, legal prohibition, dissemination of socially dangerous information, Internet, Legal restrictions on freedom, extremism on the Internet.*

**JEL Classification Codes :** *K14, K49.*

[1] *PhD in Law, PJSC «RusHydro», Moscow, Russia, E-mail: alex_klem@list.ru*
[2]*PhD in Philosophy sciences, Associate Professor of Department of Sociology and Management of Moscow Automobile and Road Construction State Technical University (MADI), E-mail: oksana-hlopkova@mail.ru*
[3]*PhD in Law, Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia, E-mail: kazanceva83@bk.ru*
[4] *PhD in Law, Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia, E-mail: svnn@inbox.ru*

## 1. Introduction

This article is devoted to the study of some problems acquisition, storage and dissemination of socially dangerous information. Their study has a high degree of relevance, because it allows understanding and evaluating the processes of the dissemination of negative information in the Internet and assesses emerging consequences. The authors aim of this article to expand details the content of put forward author's idea about the social conditionality of the legal prohibition on the dissemination of the socially dangerous information is determined by social, moral, cultural, historical, economic, political and legal factors and the criteria for imposing restrictions on the dissemination of information should be based on the principle of information and humanitarian balance. The authors substantiated the need for integrated and interdisciplinary approach to understanding the phenomenon of socially dangerous information on the Internet is justified.

## 2. Literature review

The research includes the findings based on grounds and works of Bunn *et al.* (2011), Frank (1967), Wright *et al.* (2018), Hyman (2005), Singer (2010), Sieber (1992).

## 3. Methods of carrying out research

At various stages of the study we use scientific methods such as comparative legal analysis, sociolinguistic (text analysis), psychological (the study of psychological reactions of population) as well as other methods. We rely on the international law and the legal practice of such countries as Russian Federation, China, US, Japan, Australia, UK, etc.

## 4. Results and Discussion

The development of modern technologies related to creation and transmission of information led to the formation of a new social reality. Due to the World Wide Web information in contemporary society is distributed without major restrictions and many aspects of its spreading is wide and practically unregulated. Older technologies designed for the creation and transmission of information (press, radio, television) have certain boundaries of freedom, imposed by the interests of owners. Easy accessibility, low cost and a huge scale of the Internet remove many boundaries and lead to contradictory consequences.

It is worth to mention that the ability of an individual and a group of persons to produce information and knowledge valuable for the development of weapons of mass destruction is higher than in the pre-Internet era. Modern computing technologies, fast and efficient search of necessary technical data and information, very fast information exchange between the team members – all this factors

facilitates the danger from extremists (large groups of terrorists or even pseudo-states based on danger ideologies capable of large-scale research and development and production of dangerous items).

On the one hand, the society has new technological opportunities for the development of democracy and transformation of the social system, caused by the widespread use of the Internet. The emergence of fundamentally new social tools is based on new information and telecommunication technologies, it opens many ways to rationalize human society, to realize the creative potential of individuals and to find optimal answers to many threats and challenges of our time.

On the other hand, the lack of control and the speed of information transfer facilitate activities with destructive purposes. The most dangerous manifestation of this phenomenon is the spread of negative content. With the rise of new technologies and the growing access to the Internet, the state regulations of the Internet are important and can't be neglected when dealing with cybercrime, terrorism, threats to national security.

For example, according to the Article 43 of the National Security Strategy of the Russian Federation (Approved by Edict of the President of the Russian Federation 31 December 2015 No. 683) the main threats to the state and public security include activities connected with the use of information and communication technologies to disseminate and promote the ideology of racism, extremism, terrorism, separatism, threats to civil peace and political and social stabilities in the society.

The Article #29 of the Constitution of the Russian Federation proclaims the freedom of ideas and speech. Thus, "the propaganda or agitation instigating social, racial, national or religious hatred and strife shall not be allowed. The propaganda of social, racial, national, religious or linguistic supremacy shall be banned". According to article #55 "the rights and freedoms of a man may be limited by the federal law only to such an extent to which it is necessary for the protection of the fundamental principles of the constitutional system, morality, health, the rights and lawful interests of other people, for ensuring the defense of the country and the security of the State".

The Criminal Code of the Russian Federation contains a few articles related to the criminal liability for dissemination of the following types of socially dangerous information ( slander (articles 128.1, 298.1); Obstruction of the Exercise of the Right of Liberty of Conscience and Religious Liberty (article 148); false information (articles 185.3, 207, 306-307, 354.1); Public Calls for Committing of Terrorist Activity or Public Justification of Terrorism (article 205.2), Public Appeals for the Performance of Extremist Activity (article 280); Public Appeals to Unleash an Aggressive War (article 354); Incitement of Hatred or Enmity, as Well as Abasement of Human Dignity (article 282); the rehabilitation of Nazism (article 354.1); Illegal Making and Distribution of Pornographic Materials or Objects;

Making and Distribution of Materials or Objects with Pornographic Pictures of Minors (articles 242, 242.1); Insult of a Representative of Power; Insult of a Serviceman (articles 319, 336). The Russian legislation includes other important content restrictions. For example, the Unified Register of the domain names, website references and network addresses that allow identifying websites containing illegal and forbidden information controls:

– methods of developing, preparation and usage of narcotics, psychotropic substances and their precursors, places of acquisition of such substances and their precursors, as well as methods and places of narcotic plants cultivation;
– information on how to commit suicide and incitement to commit suicide;
– material with pornographic images of minors and (or) the announcements of minors as performers to participate in pornographic entertainment events that are distributed through the Internet.

In contemporary situation, the counteraction to the dissemination of socially dangerous information is an important mission of the State, the implementation of which is possible only within the framework of various branches of law. Legal restrictions on the dissemination of information can be conditionally divided into the following groups:

*1. Legal restrictions on freedom in order to protect the interests of the citizens and the security of the state and the control of the intangible components of weapons of mass destruction.*

Reduction of nuclear arsenals of the "nuclear club" leading powers reduces the risk of mutual destruction, but is not able to completely eliminate the risk of a nuclear threat. In particular, nuclear terrorism is a real and urgent threat (see [1, 2] and references therein).

In the majority of "nuclear states" the nuclear stockpiles and sensitive facilities are well-protected in terms of physical security. However, if the probability of stealing nuclear weapons can be assessed as very low, the probability of taking possession of fissile material is much higher. Weapons-grade fissile material is used in dozens of countries, in particular in research reactors.

It's worth to analyze in detail the ability of terrorist organizations to access information on the design and technology of nuclear weapons. In this regard, quite significant experiment was organized in the 60's in the US (the so-called Nth country experiment). Two physics department graduates (Dobson and Selden), while in the Lawrence Livermore National Laboratory (LLNL), were able to develop a detailed design (up to drawings and specifications) of a nuclear bomb in a relatively short time. This design was considered operational according to the LLNL experts. It should be noted that the participants had no working experience in nuclear physics and no access to private sources of information, the results of calculations and tests, they could not come in contact with the developers of nuclear weapons. The results were classified.

This experiment tells that a small group of scientists is certainly able to develop a project of nuclear weapons powers. Now a team of physicists from the best universities has even more options for the design of nuclear weapons. So, at the dawn of the era of nuclear weapons, the development was closely linked to testing, analytical calculations, simple numerical calculations. Nowadays scientists rely on multiprocessor high-performance computers, efficient software for the simulation of the neutron and gamma transport, propagation of shock waves, molecular dynamics.

In addition, the codes used in civilian applications such as the development of controlled thermonuclear fusion devices, the study of astrophysical objects (neutron stars, supernovae), neutron sources, can be applied to the development of nuclear weapons. The present level of simulations involving computer technology can help in the development of highly efficient nuclear weapons, including thermonuclear, would eliminate the stage of full-scale tests. Over many decades a lot of information about the basic principles of nuclear weapons devices became available to the general public.

Terrorists can get information from the output of qualified physicists [8, 10]. In this regard, in order to reduce the threat of nuclear terrorism, it is necessary to prevent the uncontrolled proliferation of "intangible technology". This will require to monitor the activities of groups and individuals to develop nuclear weapons. In addition, consideration should be given control over the use of high-performance codes for the calculation of neutron transport, transport of other particles and radiation. The log files should be sent to the control center to monitor the parameters used for each calculation.

Thus, joint disarmament of nuclear powers is not enough to eliminate the threat of nuclear weapons, international and comprehensive control of fissile materials, as well as control of the intangible components - knowledge and experience related to the development of nuclear weapons is of high demand.

Special accent should be made on a necessity of control over nuclear materials as well as non-material component — knowledge and experience, derived from weapons of mass destruction development.

In the domain of biology, biochemistry and other scientific fields related to the development of sophisticated biological weapons intangible components are of even higher value then real substances which are required for the synthesis of hazardous bio-weapons. A lab of motivated and strong biologists and biochemists is capable of the design and production of bio-weapons in the case of a bad will.

Well-trained scientists are able to outstrip the developers of anti-dots and counter-measures due to the possibilities of variation of viruses and bacteria. Thus, fighting a qualified and well informed and equipped team of developers is a difficult problem.

It is much easier to introduce preventive control over scientists with the necessary knowledge to develop weapons, over critical data bases, information exchange.

*2. Legal restrictions on freedom in order to protect the interests of the citizens and the security of the state and the counteraction to terrorism and extremism on the Internet*

The need for integrated and interdisciplinary approach to understand the phenomenon of Internet terrorism, providing information and semiotic, psychological, and linguistic components that enable the interpretation of the phenomenon. This approach allows, in accordance with modern scientific methodology of knowledge, to build a model that explains the specifics, the structure and dynamics of terrorism in the context of its information and procedural condition.

The need for proportionality of legal measures to counter the terrorist threat information to a real risk, given the fact that the Internet is not just the activities of terrorist and extremist organizations, but also the information space, symbolizing freedom and freedom of expression that is inherent in democratic states. Control system, search, tracking and analysis of the links on the Internet must not be contrary to democratic ideals such as freedom of speech and open communication, the privacy aspects of life. The Criminal Code of the Russian Federation contains a few articles related to the criminal liability for:

– Obstruction of the Exercise of the Right of Liberty of Conscience and Religious Liberty (article 148);
– Public Calls for Committing of Terrorist Activity or Public Justification of Terrorism (article 205.2), Public Appeals for the Performance of Extremist Activity (article 280); Public Appeals to Unleash an Aggressive War (article 354);
– Incitement of Hatred or Enmity, as Well as Abasement of Human Dignity (article 282);
– the rehabilitation of Nazism (article 354.1);

The systematic counteraction to terrorism/extremism in the global information network, taking into account the dynamics of the phenomenon of Internet terrorism, when Web sites suddenly appear, repeatedly changing their formats, and then instantly disappear and in most cases, create the appearance of extinction, changing the address domain, while maintaining its the previous contents.

Regulation rules and legal acts in this domain should be in balance with the interests of the individual, society and state in the information sphere. However, in this way, we are faced with a number of factors that complicate this task.

Many technical intermediaries deny legal liability and moral responsibility for the profusion of racist sites and content on their web pages, which are accessible to Internet users of all ages in countries where such content is formally prohibited. We

need to take in consideration the fact that additional technologies can hide malicious content (Dark Web) (Quora, 2018; LaFave and Israel, 2009).

It is obvious that the development of law lags behind the formation process of new information and communication technologies, which can be used by extremist organizations. Traditional measures of territorial jurisdiction, administrative boundaries, etc. are largely meaningless with respect to the Internet. In the context of rising international issues it is necessary to keep in mind that the Internet was created and operated by global principles of construction, and hence the system to counter Internet terrorism and extremism should also be built largely on the basis of international cooperation. It is about the interaction of developers of dedicated facilities, law enforcement, information exchange, mutual recognition of certain organizations as tor extremist, on the formation of a single list of such organizations. Harmonization of the international legislation in this field is another crucial issue.

Nowadays there are no effective methods of dialectical combination of self-regulation mechanisms, and operating rules of the law in this area. The existing legislation is largely declarative in nature and limited mainly to the general provisions on the inadmissibility of the spread of extremist information on the Internet. Global practice issues of access to certain information on the Internet comes to the realization of the two approaches (methods of access): technical and administrative access restrictions, conduct promotional and preventive work.

Global practice issues of access to certain information on the Internet comes to the realization of the two approaches (methods of access): technical and administrative access restrictions, conduct promotional and preventive work. Integrated and interdisciplinary approach to understanding the phenomenon of information technology terrorism is needed.

*3. Legal restrictions on freedom in order to protect of honor, dignity and business reputation*

The Criminal Code of the Russian Federation contains a few articles related to the criminal liability for dissemination of the following types of socially dangerous information:

– slander (articles 128.1, 298.1);
– false information (articles 185.3, 207, 306-307, 354.1);
– Insult of a Representative of Power; Insult of a Serviceman (articles 319, 336).

*4. Legal restrictions on freedom in order to protect minors*

Counteraction is required against child pornography, sexual exploitation of minors, the activities of pedophiles against children in order to create pornographic products and other illegal activities; information about the means and methods of committing suicide, etc.). Depending on the objectives, the information disseminated can not only have a destructive effect on the formation of the personality (inflict substantial damage to mental and moral health), but be used by stakeholders as a tool that

simulates a person for a specific kind of delinquent behavior, causing physical harm to one's health.

The Criminal Code of the Russian Federation contains a few articles related to the criminal liability for Illegal Making and Distribution of Pornographic Materials or Objects; Making and Distribution of Materials or Objects with Pornographic Pictures of Minors (articles 242, 242.1); Incitement to Suicide (Article 110, part 2).

*Social request to restrict the spread of socially dangerous information.*
A social request to restrict the spread of socially dangerous information is formed in the society due to the growing threats related to the uncontrolled distribution of information. Many popular network resources rely not only on the users self-imposed responsibilities, but apply special technologies to block the spread of socially dangerous information. The users of YouTube, Facebook, Vkontakte, Instagram and other major social networks can inform the administrator of the network resources contaminated by socially dangerous information (for example, information that provokes social, racial, national or religious hatred and enmity, containing information on social, racial, national, religious or linguistic superiorities, pornographic materials, etc.).

The activity of civil organizations in countering the spread of socially dangerous information in the Internet (by, for example, the League for Secure Internet) is indicative of a strong public request for the development of a secure Internet, the "children" domain zone, where only the sites recommended for children are accessible, the development of software products and technologies that ensure the safety of the Internet (for example, Youtube Kids, Yandex parental control).

The main goal of the research project is to improve the system of content restrictions that should be in balance with the interests of the individual, society and state in the information sphere. The purposes of the project are as follows:

1. A comprehensive study of the phenomenon of negative content in the global information environment, the essential features of harmful information.
2. Analysis of the legal approaches and international experience in the implementation of restrictions on access to Internet resources, consideration of domestic and foreign practice to identify and prevent cases of online dissemination of harmful information.
3. Analysis of developments in different countries to research how local and national authorities are kept up to date on latest legal, policy and practical developments in counteraction to racism, xenophobia and related intolerance in cybercrimes.
4. Analysis of the legal approaches and international experience in the implementation of restrictions on access to Internet resources, consideration of domestic and foreign practice to identify and prevent cases of online distribution incitement to commit terrorist acts and violent extremist crimes.

## 5. Conclusion

Based on the analysis of international and national regulations, as well as other documents regulating the content restrictions in Internet we arrive to the following conclusions:

1. The social conditionality of the legal prohibition on the dissemination of the socially dangerous information is determined by social, moral, cultural, historical, economic, political and legal factors. The combination of all these factors, which is manifested in the attitude to the socially negative content, demonstrates the need for the formation of a legal mechanism to limit the dissemination of socially dangerous information. The development of basic concepts and categories, criteria for referring to information whose dissemination should be prohibited is of high demand.
2. The criteria for imposing restrictions on the dissemination of information should be based on the principle of information and humanitarian balance, which must take into account the requirements of rationality and ensure the balance between the two major issues:
– the degree of public danger of the information and technology dissemination;
– the rights of citizens to access to information.
3. The need for proportionality of legal measures on content restrictions to a real risk, given the fact that the Internet is not just the Internet is not just malicious activity, such as activities of terrorist and extremist organizations, but, first, the information space, symbolizing freedom and freedom of expression that is inherent in democratic states. Control system, search, tracking and analysis of the links on the Internet must not be contrary to democratic ideals such as freedom of speech and open communication, the privacy aspects of life. Regulation rules and legal acts in this domain also should be in balance with the interests of the individual, society and state in the information sphere.
4. The need for integrated and interdisciplinary approach to understanding the phenomenon of socially dangerous information on the Internet is justified. This approach allows, in accordance with modern scientific methodology of knowledge, to build a model that explains the specifics, the mechanism of dissemination of negative content on the Internet.
5. As an outcome of the research a few contributions to the national Russian legislation in the domain of counteraction to dissemination of negative content on the Internet have been made. Harmonization of the international legislation in this field is another crucial issue.

## References:

Bunn, M., Morozov, Yu., Mowatt-Larssen, R. 2011. The U.S.-Russia Joint Threat Assessment on Nuclear Terroris. Belfer Center for Science and International Affairs.

Frank, W.J. 2003. Summary Report of the Nth Country Experiment UCRL-50249. The National Security Archive, available online: http://www.guardian.co.uk/world/2003/jun/24/usa.science

Klausen, J. 2015. Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq. Studies in Conflict & Terrorism, Vol. 38, 1-22.

Klementiev, A.S. 2015. Nuclear terrorism: myth or real threat. Counter-terrorism: problems of the XXI century, 3, 26-30.

LaFave, W.R., Israel, J.H. 2009. Principles of Criminal Procedure.

Olsen, R. 2018. The Dangers of Social Networking. Available online: https://turbofuture.com/internet/The-Dangers-of-Social-Networking-Why-you-need-to-be-careful.

Quora. 2018. What is the most dangerous information that people must be protected from? Available online: https://www.quora.com/What-is-the-most-dangerous-information-that-people-must-be-protected-from

Sieber, U. 1992.The international emergence of criminal information law. Köln, Heymanns, Vol. XIII, 144 p.

Singer, R.G., La Fond J.Q. 2010. Criminal law: examples and explanations. New York, Aspen Publishers, Austin, Wolters Kluwer.

Wright, D.K., Hinson, M.D. 2008. How Blogs and Social Media are Changing Public Relations and the Way it is Practiced. Public Relations Journal, 2, 2, 2-20.