

Criminal Law Means of Countering Extremist Manifestations on the Internet

James E. Gonzales¹ and Denis Mikhailovich Vladimirov²

¹Chicago Police, Chicago, USA

²Academy of the Federal Penitentiary Service of Russia, Ryazan, Russia

Keywords: Extremism, crimes of an extremist orientation, extremist manifestations, information and telecommunication networks, the Internet.

Abstract: This article examines criminal extremist manifestations committed with the use of information and telecommunication networks, especially the Internet. The relevance of the chosen research topic lies in the active use of the Internet by the majority of the planet's population. The Internet has become an essential part of people's lives and an excellent way of spending leisure time, having communication, obtaining various kinds of information and knowledge, making money, etc. Unfortunately, the criminal community has found its use for the Internet and it consists in the realization of its illegal goals by means of its use. Extremist organizations, which in the 21st century actively use the World Wide Web to spread their radical views, are no exception. This study examines the criminal law means of countering extremist crimes on the Internet. The official statistics reflecting the dynamics of the studied category of crimes are analyzed. The reason for the dramatic change in the number of registered crimes of an extremist nature in 2019 is revealed. The features of committing extremist crimes by means of using the Internet, in contrast to traditional methods, are considered. The main reasons for the high popularity of the Internet among extremist organizations and individual representatives of radical ideology are given.

1 INTRODUCTION

At present, extremist manifestations can range from images of Nazi symbols on clothes and humiliating posts on the Internet, to its extreme manifestations and specific excesses called terrorist acts. Even the most seemingly insignificant manifestations of extremism and the relatively small number of extremist crimes committed in comparison with other categories pose a serious threat to the life and health of citizens, and also cause harm to the security of our state and threaten the foundations of its constitutional system.

In Russian dictionaries, extremism is understood as adherence to extreme views and measures, mainly in politics (Ushakov, 2008). But in fact, the destructive impact of individual occurrences of extremism can go far beyond the political sphere, causing significant harm to national and religious values (Petryanin et al. 2017, Oganessian et al. 2018, Orekhoyskaya et al. 2019), economic and environmental spheres (Korennaya, 2018, Tavstukha et al. 2018), youth morality (Balatsky, 2017), etc.

Unfortunately, extremist and terrorist organizations, as well as individual followers of their ideology, do not stand still and are in constant search of new ways and means to realize their radical goals.

The process of informatization of society taking place in the world community, which influenced the rapid growth in the production of technical means of transmitting information, as well as the development of information and telecommunication networks, including the Internet, had a strong influence on the transformation of the usual ways of committing a crime.

Certain extremist crimes were no exception, the commission of which is increasingly taking place with the use of the mass media or information and telecommunication networks. This is evidenced by the growth of the quantitative indicator of this category of crimes according to the statistical data of the bodies keeping records of the state of crime in the Russian Federation. This forced the domestic legislator to adapt to modern realities and improve criminal legislation in the field of countering

extremist crimes committed in the still poorly studied and legally regulated Internet.

Criminal legal means of countering criminal extremist manifestations in the Internet space are poorly studied and are in constant improvement due to the constant technical and informational development of society, its radicalization and politicization. The choice of the research topic is due to the complexity, controversy and relevance of the problems described above.

2 MATERIALS AND METHODS

Materials used in the course of this study:

- fundamental works devoted to the problem of extremism, as well as research by contemporary authors;
- modern scientific research devoted to various forms of manifestation of extremism;
- scientific publications devoted to the problem of the spread of extremism directly in the Internet space;
- modern scientific research devoted to public relations, which can be harmed by certain extremist manifestations.
- official statistics of law enforcement agencies of the Russian Federation reflecting the state of crime;
- regulatory legal acts aimed at countering extremist manifestations on the Internet;

Research methods: hermeneutic and dialectical method of cognition, comparative analysis, formal legal method, as well as scientific abstraction, grouping and classification.

3 RESULTS AND DISCUSSION

According to official statistics, in 2017, 1,521 extremist crimes were committed, in 2018 – 1,265, in 2019 – 585 and in 2020 – 833.

The statistics show that in 2020 there was an increase in registered crimes of the studied category by 30%. However, in 2019 there was a dramatic decrease in the number of committed extremist crimes by 53%. This was due to the partial decriminalization of Art. 282 of the Criminal Code of the Russian Federation «incitement to hatred or enmity, as well as humiliation of human dignity» and addition to the Code of Administrative Offenses of the Russian Federation Art. 20.3.1 providing for liability for a similar act in December of 2018. Now criminal liability under Art. 282 of the Criminal Code

of the Russian Federation occurs only for the commission of these actions after he was brought to administrative responsibility for a similar act within one year (Gavrilov, 2020).

The fact is that under Art. 282 of the Criminal Code of the Russian Federation, the largest number of crimes was committed annually in comparison with other extremist groups. Before decriminalization in 2018, 814 crimes were committed under Art. 282 of the Criminal Code of the Russian Federation, and in 2019 already 284. It should be noted that under the new Art. 20.3.1 of the Code of Administrative Offenses of the Russian Federation, 483 cases of administrative offenses were received by the courts in 2019.

Thus, from the analysis of the statistical data presented, it can be concluded that the number of extremist manifestations committed remained practically the same, but some of them due to the partial decriminalization of Art. 282 of the Criminal Code of the Russian Federation passed into the category of administrative offenses, while maintaining the level of public danger essentially unchanged.

The Federal Law of July 25, 2002 No.114-FL «On Counteracting Extremist Activity» defines the term «extremist activity» which the legislator has used as a synonym for «extremism». However, a specific definition with clearly defined features and distinctive characteristics is not given. The definition of extremist activity (extremism) is disclosed by means of enumerating acts related to it, and in addition to criminally punishable crimes (including of a terrorist nature), administrative offenses are also cited there.

Speaking specifically about criminal extremist manifestations, it should be noted that the Criminal Code of the Russian Federation contains the term «crimes of an extremist nature». Its definition is given in note 2 of Art. 282.1 of the Criminal Code of the Russian Federation, by which it is proposed to understand all criminally punishable acts, taking into account that they were committed for reasons of political, ideological, racial, national or religious hatred or enmity or for reasons of hatred or enmity in relation to any social group provided for by the relevant articles of the Special Part of the actual Code and paragraph «e» of the first part of Article 63 of this Code. (i.e. committed on a so-called extremist motive) (Bukalerova et al. 2016).

We agree with the remark of S.V. Borisov that the Criminal Code of the Russian Federation does not have a formed unified system of norms aimed at countering extremism, extremist compositions are

located in different sections and chapters (Borisov, 2012). In addition, the Criminal Code of the Russian Federation does not have an exhaustive list of articles of this category of crimes.

Thus, theoretically, it is possible to simulate a huge number of examples of the commission of crimes based on the reasons specified in paragraph «e» of Part 1 of Art. 63 of the Criminal Code of the Russian Federation using the Internet, which will be considered extremist crimes.

Due to such uncertainty, we consider it expedient and reasonable to consider in this study only those extremist norms that contain, as a mandatory constructive or qualifying feature, such a method of committing as using information and telecommunication networks, including the Internet. These are Art. 280, 280.1, 282 of the Criminal Code of the Russian Federation.

From the place of the relevant norms in the structure of the Special Part of the Criminal Code of the Russian Federation, it follows that the criminal offenses provided for by them infringe on the foundations of the constitutional order and the security of the state: Articles 280, 280.1 and 282 are located in Chapter 29 «Crimes against the foundations of the constitutional order and security of the state» section X «Crimes against state power» of this Code (Uzembayeva 2016).

In 2014, these compositions were supplemented by the Federal Law of June 28, 2014 No.179-FL «On Amendments to Certain Legislative Acts of the Russian Federation» indicating such an alternative way of committing them as using information and telecommunication networks, including the Internet.

Articles 280 and 280.1 of the Criminal Code of the Russian Federation contain it as the only qualifying feature (part 2), increasing the maximum term of imprisonment from 4 to 5 years in both cases. In addition, as the main type of punishment, coupled with imprisonment, the sanctions of these structures provide for the deprivation of the right to hold certain positions or engage in certain activities for up to three years.

It should be noted that there is an obligatory constructive feature necessary for the criminalization of these compositions, namely, «publicity», including through the means of using the Internet (part 2 of article 280, part 2 280.1 of the Criminal Code of the Russian Federation). For example, private closed correspondence between two Internet users excludes such a feature, as well as the corpus delicti provided for by the specified norms.

Unlike Art. 280 and 280.1, Art. 282 of the Criminal Code of the Russian Federation contains an

indication of such a method of commission directly in the disposition (again, in case of the presence of publicity). And as qualifying signs it distinguishes: committing with the use of violence or the threat of its use (item «a»), by a person using his official position (item «b»), by an organized group (item «c»).

It should be noted that statements on the Internet aimed at inciting hatred or enmity or humiliation of human dignity on various distinctive features are also characterized by other forms of complicity besides an organized group (clause «c», part 2 of Article 282 of the Criminal Code of the Russian Federation). In the comments under posts published on major social networks, one can often find verbal expressions of an extremist nature in relation to a certain nationality or its individual representative, aimed at humiliating human dignity, where other users join his words. This can happen by prior conspiracy or, as it often happens without it (that is, by such forms of complicity as a group of persons, or by a group of persons by prior conspiracy, parts 1 and 2 of Art. 35 of the Criminal Code of the Russian Federation). This undoubtedly increases the level of public danger, although such forms of complicity as a qualifying feature have not been consolidated in this norm.

As we said earlier, after decriminalization, liability under Art. 282 of the Criminal Code of the Russian Federation occurs only in case of repeated commission of these actions within 1 year after being brought to justice under Art. 20.3.1 of Administrative Code of the Russian Federation.

Extremist corpus delicti contained in Chapter 29 «Crimes against the foundations of the constitutional order and security of the state», namely Art. 280, 280.1, 282, 282.1, 282.2, 282.3 of the Criminal Code of the Russian Federation, many scientists classify into a separate group. For example, D. M. Potapov proposes to classify these norms as «definitely extremist» (Potapov 2019), A. A. Mozhegova as «extremist crimes» (Mozhegova, 2015), etc.

We also consider it reasonable to separate these norms into a separate group. This is explained by the fact that they are extremist, regardless of the motive for the crime. For example, the organization of an extremist community (Article 282.1 of the Criminal Code of the Russian Federation) or the financing of extremist activities (Article 282.3 of the Criminal Code of the Russian Federation) can be committed solely for the purpose of obtaining greater material benefits in the future, that is, for a selfish motive. It's just that the actions themselves are in any case extremist manifestations, the list of which is given in

the domestic definition of the concept of extremist activity.

The growing popularity of information and telecommunication networks, especially the Internet, among extremists is explained by the fact that they:

- have an intercontinental coverage area that allows to wash off state borders, which cannot be done by traditional methods of committing crimes, especially when transfer between states is prohibited or difficult (such as during the COVID-19 pandemic);

- allow you to almost instantly receive, send or massively distribute information, subject to the availability of network connectivity. What currently has the majority of modern cellular communications, laptops, stationary computers and other technical equipment;

- allow you to simultaneously influence a different category of citizens, moreover, the number of these people can be practically unlimited. It depends on the place where the information is disseminated and the number of people visiting this Internet resource. Some pages on social networks or Internet sites have thousands, tens of millions and even hundreds of millions of subscribers. It is unlikely that in the real world, it will be possible to collect such a huge audience, which is undoubtedly a huge advantage of this method of committing extremist crimes;

- are one of the main sources for recruiting new supporters of radical ideology. The bulk of Russian Internet users are citizens aged 12 to 24 years. According to Mediascop, 97.1% of people of this age use the Internet. Due to the age characteristics of the younger generation, their not fully formed moral and ethical foundations, they become the main objects of propaganda influence (Bukalerova et al. 2020). For the same reason, some of them succumb to such influence based on pseudo-religious and pseudo-political convictions, after which they join extremist organizations.

Another reason for the active use of information and telecommunication networks by extremists, especially the Internet, is the difficulty in detecting and suppressing such crimes by operational units of law enforcement agencies (Shkabin 2020), as well as in establishing the identity of the criminal.

First, since many Internet systems are developed abroad, corporations that manage IP addresses and domain names are based in other countries. For example, the main offices of such popular services as Facebook, Gmail, Skype and others are located in the United States. And it is very difficult for Russian law enforcement agencies to obtain information about their users, and in most cases even impossible.

Secondly, the high anonymity and secrecy of information in cyberspace make it difficult to establish the identity of an extremist criminal and collect evidence. Social media accounts, websites and other Internet resources can be registered to non-existent names and surnames, someone else's phone numbers, specially created fake emails, etc. That is exactly what the criminals do. The most skillful radicalists use various kinds of programs to hide information about the sender, as well as, if necessary, destroy files from the network, which can be used as evidence of their involvement in a crime. Of course, sometimes information and files can be recovered, but unfortunately not always.

4 CONCLUSIONS

The definition of the concept of «crimes of extremist orientation» contained in note 2 of Art. 282.1 of the Criminal Code of the Russian Federation, should be supplemented with an exhaustive list of articles of the Criminal Code of the Russian Federation related to them. This will allow avoiding its too broad interpretation, which in turn unreasonably expands the range of crimes belonging to the studied category, and also burdens the implementation of state strategies to combat extremist activities and the work of law enforcement agencies.

Item «c» of Part 2 of Art. 282 of the Criminal Code of the Russian Federation should also be supplemented with such forms of complicity – by a group of persons and by a group of persons by prior conspiracy.

At the international level, it is necessary to develop an effective mechanism for cooperation in providing law enforcement agencies of other states with information about personal data and correspondence of extremist users of large Internet services.

In addition, if we are talking about cyberspace, the material and technical base of the workplaces of law enforcement officers should be constantly updated. In order to provide the latest technical means and software necessary to detect and suppress extremist crimes on the Internet, as well as to establish the identity of the offender. In addition, it is necessary to ensure regular training for employees of operational units in working with modern technical means.

It is necessary to develop and constantly improve a methodology for educating and informing various age categories of citizens about possible extremist manifestations on the Internet. This is especially true for parents and teachers, in order to prevent the

involvement of their children in extremist organizations, and indeed other criminal communities. Mediation services (Vasilenco et al. 2020), qualified specialists in the field of communication and child psychology, specialists in the field of communication technologies, lawyers, etc. should be involved in working with parents, teachers and children. leisure activities (Naurzalieva et al. 2020). In addition, it is important to inform all citizens about the possible administrative and criminal liability for participation in extremist activities on the Internet.

REFERENCES

- Aleksandra S. Vasilenko, Vladimir M. Filippov, Maria A. Simonova, Sergey A. Kovalenko, 2020. Probabilistic Model of Implementing Mediation into Russia's Criminal Procedure in the Conditions of Society's Digital Transformation. Conference materials: Scientific and Technical Revolution: Yesterday, Today and Tomorrow. *In Lecture Notes in Networks and System*. 129. pp.1286–1293.
- Bukalerova, L.A., Ostroushko, A.V., Rustamov, N.E., 2016. Determinants of murders motivated by political, ideological, racial, national or religious hatred or enmity or motivated by hatred or enmity towards a social group. *In All-Russian criminological journal*. 10(1). pp. 40-49.
- Balatsky, D.Yu. 2017. Measures to prevent youth extremism. *In Power and control in the East of Russia*. 4(81). pp. 162-169.
- Borisov, S.V., 2012. *Extremist Crimes: Problems of Legislation and Law Enforcement*. p. 45.
- Gavrilov, A.A., 2020. Extremist Crimes: Qualification Problems. *In Sustainable development of science and education*. 10(49). pp. 164-169.
- Korennaya, A.A., 2018. Economic extremism: criminal law aspect. Collection of scientific articles of the international conference «Lomonosov Readings in Altai: Fundamental Problems of Science and Technology». Barnaul. pp. 2744-2747.
- Liudmila A. Bukalerova, Alexander V. Ostroushko, Saule M. Naurzalieva, Anzhela V. Dolzhikova. 2020. There Is a Need of Protecting Children from Sexual Information Disseminated Through Information and Communication Technologies. Conference materials: Scientific and Technical Revolution: Yesterday, Today and Tomorrow. *In Lecture Notes in Networks and System*. 129. pp. 976–984.
- Mozhegova A.A. *Extremist Crimes and Extremist Crimes in the Criminal Law of the Russian Federation*. p. 27.
- Natalia A. Orekhovskaya, Alexey A. Chistyakov, Nina I. Kryukova, Julia A. Krokhnina Yuri V. Ospennikov, Elena V. Makarova, 2019. Orthodoxy and modernity their contact facets in Russian societ. *In European Journal of Science and Theology*. 15(2). pp. 67-77.
- Olga G. Tavstukha, Alla A. Korzhanova, Alexey A. Chistyakov, Kirill A. Chistyakov, Irina I. Shatskaya, Alexandra S. Vasilenko, Lyudmila D. Starikova, Elena V. Maleko. 2018. Personality Ecological Consciousness: Values Ethical Vector of Nature Safety Sustainable Development. *In Ekoloji*. 27(106). pp.1355–1364.
- Oganesyanyan S. S., Shamsunov S. K., 2018. Civilization mentality and environmental problems. *In Ekoloji*. 27 (106). pp.1639–1644.
- Petryanin, A. V., Petryanina, O. A., 2017. Modern types of extremism as a threat to national security. *Collection of scientific articles «Criminal law, criminal law: theory and practice»*. St. Petersburg. pp. 201-207.
- Potapov, D.M., 2019. Art. 282 of the Criminal Code of the Russian Federation: qualification issues. *In Bulletin of the Kazakh Humanitarian and Legal Innovative University*. 3(43). pp. 11-14.
- Shkabin, G.S., 2020. Criminal and operative-search legislation: problems of intersectoral relations and prospects for improvement (Review of the V Interdepartmental scientific and practical conference). *In State and Law*. 7. pp. 144–150.
- Saule M. Naurzalieva, Alexandra S. Vasilenko, Mariya A. Simonova, Dmitriy V. Bondarenko, and Piotr K. Dolzhikov, 2020. Causes of Juvenile Delinquency in the Republic of Kazakhstan. Conference materials: Scientific and Technical Revolution: Yesterday, Today and Tomorrow. *In Lecture Notes in Networks and System*. 129. pp. 1250–1258.
- Uzembayeva, G. I., 2016. *Crimes of an extremist nature, committed with the use of the media or information and telecommunication networks: criminal law and criminological characteristics*. p. 210.