# Legal Framework for Counter-Terrorism in Social Networks in Russia and Abroad

*Vladislav* Romanovsky[1,*], *Rifat* Kildeev[2]

[1] Department of Criminal Law, Institute of Law, Penza State University, 440026 Penza, Russian Federation
[2] Department of Legal Disciplines, Institute of Law, Penza State University, 440026 Penza, Russian Federation

**Abstract.** The article discusses measures to counter terrorist threats in social networks and instant messengers. It is emphasized that the modern form of communication using digital technologies has started to be actively used by terrorist organizations for recruiting supporters, raising funds, and preparing terrorist attacks. The article analyzes the German (Act on Improving Law Enforcement in Social Networks) and Chinese (Chinese Great Firewall) experience of introducing restrictions and prohibitions in the framework of regulating the activities of companies moderating information through applications and social networks. It is shown that implementing the requirements of the legal regime has not only a legal, but also technological aspect. The peculiarities of the Internet functioning contribute to free implementation of information, including illegal information. This circumstance significantly complicates the tasks of law enforcement agencies in countering terrorist threats.

## 1 Introduction

Over the years, social networks have become an essential way of communication, which allow connecting people with similar interests who are at a considerable distance from each other. Communication, information exchange, search for business partners, advertising of goods and services, interaction with public authorities and much more take place thanks to social networks. Taking into account their mass distribution and multiple functionality, social networks have become the object of close attention of criminal elements.

Terrorist organizations have also learned to use many of today's digital technologies. With the help of social networks, they recruit supporters around the world, popularize destructive ideas, develop and coordinate terrorist attacks, raise funds, etc. Digital technologies have changed the very model of terrorist activity. Previously, terrorism had a pronounced political character, which united a common agenda for the country (or a group of adjacent countries). For example, ETA in Spain fought for the autonomy of the Basques, the "Red Brigades" and RAF came out with left-wing radical ideas for developing their own countries (Italy and Germany, respectively). The Irish Republican Party fought to secede North Ulster from Great Britain.

All these organizations had a clearly defined structure, hierarchical connections, distribution of roles, social foundations that allowed them to conduct their activities in various directions. Accordingly, the fight against such organizations involved identifying and neutralizing the leaders, and opposing the ideological foundations. Moreover, the fact that many organizations were limited by national borders did not make it necessary to combine international efforts.

Now the situation has changed. Terrorist organizations use a network management model based as much as possible on redistributing various functions, so that it is most difficult to identify a single control center. Even the removal of a clear leader does not harm the organization itself, which quickly redistributes leverage over its supporters. Lack of adherence to one name creates additional difficulties in approving sanctions and restrictions both at the international and national levels. This tactic has been tested, which is why in many countries, when an organization is banned, its possible alternative names are pointed out. Social networks, due to their communication opportunities, have also become the platform that various criminal elements have quickly mastered.

## 2 Results

### 2.1. Law and Social Networks

In the short history of their existence, social networks have become an indispensable element of human communication, which makes it impossible not to use them. In the age of information technology, each state is well aware of the degree of influence of such communication platforms on society and an individual. In addition, one can observe a certain concentration of a large number of users based on a particular social network. Here are just some of the figures. Facebook has over 3 billion users, Instagram over 1 billion, with

* Corresponding author: demid0vvladislav1991@yandex.ru

Twitter approaching 1.5 billion. Russian networks are also included in the list of the most popular in the world. For example, the VKontakte audience is about 500 million users. Social networks can be classified according to various parameters, such as professional orientation, target audience, circle of users' interests, priority of a particular type of content, etc. It is enough to look at the statistics published by Mediascope to see the coverage of almost every Russian citizen's attention by the Internet, as well as the ranking of a number of information networks, which often exceeds the audience of the country's main television channels.

There is a significant number of networks in the world, some of which were created for domestic use, which does not mean they have no perspective on the global media outreach. An example is the Chinese Sina Weibo, originally created as an alternative to American social networks (which were banned in China). Now the service is available to citizens of other countries, including the Russian Federation.

Special attention should be paid to instant messengers (instant messaging system), which operate on the principle of a social network, but use a real-time communication service. The most popular are WhatsApp, Viber, Telegram. We should add Chinese WeChat, but it is limited for Asia (although its combined user base makes it one of the top five).

Many countries have started to understand the information dependence on technological products of global companies, which, we must not forget, have their own internal filtration system. Thus, there is a number of significant factors that each state tries to analyze and then they draw appropriate conclusions. Let's designate some of them:

1) instant access to the news feed. Any event that happened in the world becomes known to an unlimited number of people, which is actively used by terrorist organizations [1]. This allows them to employ intimidation tactics anywhere in the world. Regardless of the crime scene, information about it will be disseminated throughout the world [2]. In the context of fast publication, filtering becomes more complex, which allows information to be conveyed to a wide range of people;

2) the possibility of disseminating prohibited information. Government-set barriers are easily circumvented due to the location of key technology companies in the United States and Western Europe. The very creation of the Internet took place under the main slogan - No censorship! Subsequently, general restrictions were introduced, which do not always satisfy the needs of individual states, especially those where political confrontation is taking place;

3) the subordination of the interests of a wide range of people to artificially generated requests. The special term "filter bubble" includes the involvement of personalized preferences in a search engine. It is believed that this facilitates the search for the necessary information based on the user's location, their past requests, and other processed meta-data. On the other hand, the filter bubble cuts off what the programme considers to be unnecessary information. In addition, the search engine can be pre-configured for a complicated search for certain pages on the Internet. The internal policy of moderation of user content by social networks and search engines is being under close study in many countries;

4) the emergence of a new type of terrorist, who is a product of self-radicalization. There is no personal processing, no personal contact. Information content is placed so as to attract the attention of any consumer. As a result, new criminological characteristics of potential terrorists appear, in particular, «homegrown violent extremist (HVE)» [3], «lone wolf» [4]. Norwegian A. Breivik and "Pittsburgh shooter" R. Bowers are examples of such consistently radicalized criminals thanks to communication on the Internet.

The fact that instant messengers and social networks are easy to use is one of the main arguments for users. This is at the same time an additional factor for involving their abilities in criminal activities. An interesting point, in 2016 information appeared about the development of a special application for Android by ISIS called "The Alwari" (a kind of analogue of WhatsApp). Its vulnerability (the developers were never able to create a full-fledged product) led to the fact that the development of such a "specialized" messenger stopped. The ideologists of Islamist terrorism urge their supporters to use more open networks to facilitate the maximum dissemination of information about themselves, involving the whole world in the so-called "electronic jihad" [5]. An analysis of foreign sources (including public reports prepared by law enforcement agencies and special services) shows that the Telegram messenger is the most popular among terrorist organizations, featuring a high speed of information exchange, accompanied by security and end-to-end encryption.

### 2.2 Telegram and counter-terrorism

P. Durov, the creator of Telegram, has repeatedly emphasized that there is no possibility of external control over the transmitted information due to technical reasons. This was one of the reasons for the confrontation between the company and Roskomnadzor (Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications) in 2019-2020. Russian rules oblige all providers to install special equipment that allows law enforcement agencies to remotely perform special functions assigned to them by the legislation on intelligence-gathering. However, P. Durov's company refused to fulfill this obligation, referring at the same time to Article 23 of the RF Constitution, which provides for privacy protection. Let us mention that this conflict reflects a general discussion about the admissibility of general restrictions on this right. In contrast to the established restrictions, a position of their rejection is formed due to the fact that thereby the state initially suspects everyone of committing unlawful behavior [6]. The precondition of the concept of a potential criminal is introduced [7]. Let us recall that until recently, any

restrictive action on the part of law enforcement agencies was conditioned by the presence of specific facts and suspicions. The introduction of total control marks the refusal to provide grounds for such restrictions. It turns out that there is a fixation of the contacts of each citizen, regardless of whether there is data on his unlawful activities. On the other hand, the need to prevent terrorist attacks is directly related to preventive activities to control the Internet space. Currently, Roskomnadzor has dropped all possible charges and stopped blocking the messenger.

One of the features of Telegram is the option to create secret chats that destroy information (after reading) from all the chat users by the timer. This function is much in demand. Another messenger, Signal, also followed suit of the Russian messenger, claiming to ensure complete confidentiality of messages. Features of Signal, tested by users, led to its explosive popularity in 2020 - 2021. In addition, Signal positions itself as a non-profit project. Its website contains the words of support by E. Snowden, which should add motivation for using it.

Foreign researchers admit that Telegram has played an important role in recruiting and coordinating ISIS terrorist attacks in Europe [8]. Despite the preventive work of administrators, Telegram channels are being created en masse, quickly consolidating supporters and spreading terrorist content. The speed of "filling" a huge information array indicates the fact that the organizers of information channels have good equipment for storing data in electronic form and their immediate placement. At the same time, it is believed that the main supporters (about 90%) of terrorist organizations do not have deep knowledge of the encryption system on the Internet. Just over 1% use DarkNet, encrypted emails and other secret platforms [9].

The emergence of such messengers should not mean a retaliatory prohibitive policy. In 2012, the Director of US National Intelligence in his annual report on threats as a risk factor for the mass transfer of terrorist ideas pointed to the global spread of smartphones and the development of cloud technologies for organizing information [10]. On the FBI website, the Internet and social networks are designated as current threats to the development of terrorism [11]. But this does not mean the introduction of a total ban on the use of advanced technologies. The same logic should be applied to instant messengers: their use by criminals should not mean rejection of them and total lock.

### 2.3 Law and social networks in Russia

The Russian Federation has formed a legal framework for regulating the transfer of information using Internet technologies. The key normative act is Federal Law No. 149-FZ of July 27, 2006 “On Information, Information Technology and Protection of Information”. It is also necessary to highlight the Federal Law of 07.07.2003 No. 126-FZ "On Communications", Federal Law of 26.07.2017 No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation", Federal Law of 27.07.2006 No. 152-FZ "On Personal Data" and Federal Law of December 29, 2010 No. 436-FZ "On Protecting Children from Information Harmful to Their Health and Development". The attention of the state to communications in the digital sphere is constant, as indicated by regular changes and amendments to the above-mentioned regulations. Over the past five years, "package amendments" have been adopted, including a set of changes, both in the indicated laws and in the links that are in unity with them. The overwhelming majority of such "package" acts were justified by the need to counter terrorism and ensure state security. Among them, the most public attention (including criticism) was attracted by the Yarovaya package, adopted in 2016, and the Sovereign Internet Law, adopted in 2019.

In the late 2020 - early 2021 amendments were made to the legislation on communications in terms of regulating the activities of social networks. In accordance with Federal Law No. 511-FZ of December 30, 2020, Article 13.41 appeared in the Russian Federation Code of Administrative Offences "Violation of the procedure for restricting access to information, information resources, access to which is subject to restriction in accordance with the legislation of the Russian Federation on information, information technologies and information protection, and (or) the procedure for deleting this information". This new law has been applied to Twitter lnc., Facebook, TikTok, and Google. If we only speak about the situation with Twitter, where there was an attempt to slow down traffic (thanks to the Sovereign Internet Law), then, to substantiate its position, Roskomnadzor indicated that in the period from 2017 to the present, it has sent Twitter Inc. more than 28 thousand requests to remove illegal content. The lack of actions on the part of Roskomnadzor for such a long time gives cause for concern (and the release refers to promoting suicide and drug dealing). This includes the sudden activity of the state body in an increasingly difficult political time (the country's legislative body has also been in no hurry to amend the Russian Federation Code of Administrative Offences for a long time). All of these companies were held administratively liable; currently, legal litigation is still taking place in titles of courts of the Russian judicial system.

When discussing the above-mentioned Russian initiatives, references were most often made to the German and Chinese experience of regulating the activities of social networks.

### 2.4 German Act on Improving Law Enforcement in Social Networks

In 2017, Germany passed the Act on Improving Law Enforcement in Social Networks (Netzwerkdurchsetzungsgesetz, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerke, abbreviated as NetzDG). When explaining the need to adopt such a law, the German government referred to a number of key circumstances, including: 1) opposition to

the unlimited authority of Big Tech, 2) lack of cooperation activity between foreign companies and law enforcement agencies to remove unlawful content, 3) fight against criminal behaviour, extremism, and incitement to hatred. Such an extensive list of circumstances added arguments to opponents of such state regulation, citing its political meaning, aimed at returning censorship to the electronic sphere of communication [12].

The German law introduced the concept of a social network subject to a special legal regime. We point out that, due to a restrictive interpretation, many networks are not subject to its regulation (for example, networks created on a professional basis, where, in particular, users can look for a job). In other words, the target was precisely the "main players" such as Twitter, Facebook, TikTok, and Google. The law envisaged the list of prohibited information, which included data, the dissemination of which was criminalized by the German Penal Code (but even under these circumstances, only in cases directly established by the law, due to which some information prohibited by the criminal law was not included in the above mentioned list). The Internet giants themselves must monitor the content of messages and promptly delete the indicated information. In addition, a feedback service should be created, when each user can report on the emergence of criminal content. If the unlawfulness is obvious, then the social network should delete the entry. Appeal procedures are possible both from dissatisfied applicants and owners of deleted messages. Huge fines - up to 50 million euros in respect of legal entities - became a guarantee of compliance with the law.

Since the moment of its adoption and up to the present, the German Act on Improving Law Enforcement in Social Networks has been subjected to systemic criticism [13]. Let us outline the main arguments of the opponents:

- such regulation violates freedom of speech, hinders the realization of fundamental political and civil rights and freedoms of man and citizen;

- creates the basis for "privatizing censorship", since the social network itself takes the decision on unlawfulness of the content. Although the basis for unlawfulness is the law, within the framework of general prosecution, the final decision is made by the court, and for disseminating information on the network, the network itself acts as such an authority;

- there appears “overblocking”, when all questionable content or unfiltered content is blocked. In other words, any information can be banned, because due to the imperfection of its classification, it can be poorly identified. This can also happen due to the overcautiousness of the social networks themselves, when it is easier to delete than to be fined;

- minimizing the participation of the defendant party who posted the information and who was accused of unlawfulness. The very fact of filing a complaint in most cases for such a user becomes known after the removal of the information. Thus, the defendant is deprived of the opportunity to present their own vision of the situation. Such a development cannot be imagined in legal proceedings under criminal prosecution.

### 2.5 Chinese Great Firewall

For a long time, China has been implementing the Chinese Great Firewall, as it is called in foreign sources [14]. The PRC Law of November 7, 2016 "On Cyber security" can be considered as its legal peak; it imposes special requirements for creating and operating Internet networks on the territory of the state. It is based on the principle of network security, content filtering, limited access to prohibited data [15]. In other words, the Internet fragmentation has occurred within the limits of one state, while many other countries have already expressed their striving for it. The Chinese experience also attracts some democracies that claim to defend their information sovereignty. By the way, it is often Russia that is designated as a threat in cyber space among West European countries (suffice it to recall the company about Russian interference in the electoral process in the United States).

The Chinese experience is a relatively successful example of border building in cyberspace. However, here it is necessary to draw attention to the technical aspect of the solved problem. For about twenty years, China has consistently concentrated on implementing the following areas. First is creation of its own instant messengers and social networks, which made it possible to restrict the activities of foreign participants. Second is initial construction of all entry points with built-in special equipment that provides the necessary filter. Third is refusal of anonymity on the Internet; and finally installation of special tracking applications on all mobile devices circulating in China.

Even with such a total control model, it is possible to bypass the Great Firewall. Suffice it to turn to the websites of US travel companies specializing in organizing trips to China to see special tips for providing access to Facebook, which is banned in China. Despite the imposed bans, the technical capabilities of the Great Firewall are not unlimited. Even significant special knowledge is not required to bypass them. Instructions for using Proxy networks, VPN (Virtual Private Network) applications, Tor and FreeBrowser (this is the very browser popular in China for bypassing the Great Firewall) are simple and understandable to everyone.

Technology does not stand still. The idea of a space Internet, developed by the shocking billionaire Elon Musk, will soon come true. This will involve free operation of the Internet throughout the entire territory of our planet. Given the absence of "entrance" fixed locks, national control will be minimized. The Starlink project is gaining momentum (as is the decline in the price of the service). The People's Republic of China was initially very wary of this idea, but after the first successes of SpaceX, they developed their Galaxy Space project. Russia does not participate in any foreign project (although there have been proposals for cooperation). Moreover, a bill has been submitted to the State Duma of Russia, according to which a new corpus delicti should

appear in the Russian Federation Code of Administrative Offences - "Violation of the rules for the use of satellite communication networks under the jurisdiction of foreign states on the territory of the Russian Federation".

## 3 Conclusions

Social networks are not just a significant aspect of modern communications, but also an element of the economy. The worldwide spread of digital technologies determines the economic development of the state, defining its place in the international division of labor. At the same time, the transition to a new level of information exchange creates certain risks, including the spread of terrorist ideas and threats to the national security of states. The Russian Federation, like many other countries, is concerned about the emergence of such threats. Countermeasures are associated with imposing additional restrictions and introducing some prohibitions addressed to social networks and Internet providers. The problem of restrictions on the Internet has, among other things, two key aspects - legal (which can be ensured by the lawmaking activities of state authorities) and technical (the implementation of which depends both on the capabilities of the state authorities themselves and on the capabilities of communications providers). If in the first case the state has full sovereignty in resolving the stated issues, then the second is less and less dependent on the orders of public institutions. The story with Telegram, which was never blocked on the territory of the Russian Federation, is indicative.

There is another problem which comes to light. The Internet fragmentation is partly a global trend, emerging not only as a response to the use of digital technologies for unlawful purposes, but also as a model of resisting technological pressure from multinational companies (such as Facebook and Google).

However, at the same time, each state understands that the process of total closure can cause large-scale economic losses and a complete lag in the technological development race. Our country has achieved some success in the era of global digitalization. Suffice it to mention the Telegram messenger, the Yandex search engine, the Vkontakte social network. For example, in Germany, where they chose to create administrative barriers in the field of social Internet communications, there is no domestic messenger, social network, or search engine. A balanced approach should underlie the adoption of state decisions, combining both the economic interests of the state and the issues of ensuring state security and the availability of new digital technologies.

## Acknowledgements

The present article was completed as part of project MK-390.2021.2 of the grants of the President of the Russian Federation for state support of young Russian scientists – candidates of science (Tender – MK-2020).

## References

1. A. Tsesis, Fordham L. Rev., **86**, 605-631 (2017)
2. C.A. Honeywood, J. of Strategic Security, **9**, 28-48 (2016)
3. E. Southers, *Homegrown Violent Extremism* (Anderson, 2013)
4. A.E. Yashlavskii, Vestnik RUDN. International Relations, **19**, 632-642 (2019)
5. N. Prucha, Perspectives on Terrorism, **10**, 48-58 (2016)
6. N. Foggetti, Masaryk University Journal of Law and Technology, **3**, 365-376 (2009)
7. H.M. Verhelst, A.W. Stannat, G. Mecacci, Sci. Eng. Ethics, **26,** 2975–2984 (2020).
8. M. Bloom, H. Tiflati, J. Horgan, Terrorism and Political Violence, **31**, 1242-1254 (2017)
9. R. Torres-Soriano, Terrorism and Political Violence, **28**, 735-749 (2016)
10. Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence (2012). Retrieved from: https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/hpscifinalunclasssfrfeb022012).pdf
11. FBI, What We Investigate: Terrorism. Retrieved from: https://www.fbi.gov/investigate/terrorism
12. H. Adamski, GWP, **1**, 135-142 (2018)
13. R.A. Miller, B.C.L. Rev., **58**, 1545-1628 (2017)
14. J.D. Fry, U. Pa. J. Int'l L., **37**, 419-501 (2015)
15. J. Quinn, SMU Sci. & Tech. L. Rev., **20**, 407-436 (2017)