УДК 343.26
DOI 10.52452/19931778_2024_1_94

КОНТРОЛЬ ГОСУДАРСТВ НАД ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ КАК МЕТОД БОРЬБЫ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ: СРАВНИТЕЛЬНО-ПРАВОВОЕ ИССЛЕДОВАНИЕ

С.С. Мельник, В.Э. Карпович

Московский государственный институт международных отношений, Москва

big-benac@yandex.ru

Поступила в редакцию 05.07.2023

В данной работе анализируется правовое регулирование информационного пространства в сфере противодействия терроризму и экстремизму как наиболее актуальной глобальной проблеме и угрозе. Существенной основой исследования является сравнительно-правовая характеристика законодательства в сфере контроля над информационным пространством государств-членов ЕС, а также стран мусульманской правовой семьи. На примере государств с наиболее комплексной нормативно-правовой базой демонстрируется необходимость всеобъемлющего контроля за информационным пространством как средства противодействия комплексу террористических и экстремистских угроз. Также принимаются во внимание доказательства снижения уровня безопасности в государствах, которые в настоящее время подвержены подобным вызовам и угрозам. Особое внимание уделяется опыту таких государств, как Монако, Турция, Франция, Великобритания и Северная Ирландия. Авторы обосновывают полисистемный характер международного сотрудничества в борьбе с терроризмом и экстремизмом в информационном пространстве, а также выдвигают классификацию стран в зависимости от выбранного криминологического подхода к противодействию террористическим и экстремистским угрозам в информационном пространстве.

Ключевые слова: экстремизм, терроризм, информационная безопасность, борьба с терроризмом и экстремизмом, Европейский союз, страны мусульманского права.

I. Introduction

The information space in the XXI century has acquired special significance. Due to the emergence of the Internet that the processes of globalization have become more large-scale and dynamic [1]. Meanwhile, a threat of new technologies active usage in the wrongful purposes has arisen. Some of the forms of information space usage by terrorist organizations are video hosting, social networks and other tools that might also have a negative impact on society in general and individuals in particular. All these factors have led to the fact that information space control has become a necessity and a key responsibility of every State.

Information space control is crucial in terms of new challenges and threats, such as the spread of terrorist and extremist ideas with the use of information and communication technologies (*hereinafter referred to as ICT*), recruitment of citizens by terrorist groups and direct cyber-terrorist attacks [2]. The emergence of such problems has eventually to adoption of new decisions and formulation of new aspects of international agenda. Thus, the European Union (hereinafter referred to as the EU) legislation sets a number of provisions establishing a systemic struggle in the information space with the influence of a terrorist and extremists on society [3]. Moreover, it'd be reasonable to mention quite a few interesting tactics and methods used by law enforcement agencies of the respective States whose duty is to prevent terrorist and extremist crimes [4].

With the development of information technology, performing daily tasks have become easier in many ways. We can search the Internet for the necessary information in a few moments. Taking into account all the existing pros and cons, opportunities have been introduced for online learning in schools and universities. Undoubtedly, information and communication technologies have virtual communication easy and convenient, allowing to maintain warm relationships with the loved ones who live in other parts of the world. However, this article will focus not on the electronic communications benefits, but rather on the other side of electronic progress.

II. Methodology of research

The information space is a unique environment for the interaction on various topics. The primary responsibility of any State is to ensure security in all spheres of human life and society. That is why the authors have consistently analyzed the mechanisms of influence on this part of social relations.

Taking into consideration the fact that the subject of this research is the information space control (in the broad sense of this term) as a set of methods and means of combating terrorism and extremism, the experience of integration regulation as a whole was touched upon. This enabled us to outline the boundaries of cooperation between the States in the respective area. However, most of the information space control measures are based on national regulation in each individual state. Therefore, this study was based on the comparative legal method.

There are various techniques of the comparative legal method. With regard to this study, common aspects were identified at the first stage, functional comparison and macro comparison were applied afterwards, which made it possible to establish unique features of the EU member States regulations. In addition, the European Commission materials, international and European publications, the EU member States court practice, media coverage of terrorist acts were observed as well. All of the aforementioned allowed us to conduct systematic and comprehensive analysis of the information space control forms and methods.

The present research is specific in terms of use of criminology fundamental principles. This approach makes it possible to assess the existing methods and means of combating crime, as well as to identify drawbacks existing in certain countries. The authors took into account regionalization, which significantly influenced the States legislation in various spheres, particularly criminological characterization of measures taken by States.

Moreover, the authors have resorted to a formal legal method based on the formation of new legal concepts and categories in the context of information space control. The normative method was used for studying and interpretating various regulatory and legal acts enacted by the EU Member States.

III. The link between ensuring individual freedom and public safety

The extent of state involvement in information space control varies. Publication of materials on social networks can provoke sympathy for acute social, economic or political problems which subsequently contribute to the development of radicalization [5], due to various circumstances, and have a negative impact on those who are especially vulnerable to the influence of criminals. In order to take actions, individuals offer citizens “alternative” and rapid achievement of so-called desired results. Terrorist and extremist ideas can be disseminated over the Internet in multiple languages to reach a diverse audience. UNODC identifies the following ways of Internet usage by the terrorists: propaganda, recruitment, incitement to hatred, radicalization, terrorist financing, terrorist training, planning terrorist attacks, assisting in crime perpetration, cyberattacks [6].

Discussions on drafting a single universal document in the field of countering cybercrimes have been in place for a very long period. It is generally accepted that various legal acts have been adopted by the States within the framework of regional organizations. July 27, 2021 is worthy of note. On that day the Russian Federation introduced a draft Convention on countering the use of information and communication technologies for criminal purposes [7, 8]. It depicted new challenges and threats in the field of information security, specified the actual elements of crimes (including transnational ones), as well as set out provisions on international cooperation between states and their competent authorities in this environment. The draft Convention will be subject to consideration during the 78th session of the UN General Assembly in 2023. The first negotiating session will also be held in New York in January 17–28, 2022 within the framework of the *ad hoc* committee. This universal international convention might become a new international legal basis for States cooperation in the sphere of combatting cybercrime.

As an example of organizing control over the information space, we should look at the activity of such an integration association as the European Union for a number of objective reasons. First of all, the EU activity is worthy of attention due to the fact that the list of its member States comprises countries that have managed to achieve a zero rating of terrorism perception, and, on the contrary, some of the most unfavorable countries in terms of security in the sphere of terrorism and extremism. Secondly, it is generally recognized that the legislation of the EU and its individual member states is considered one of the most progressive in the modern world. It is confirmed by the relevance of regional conventions within the EU and the Council of Europe (hereinafter referred to as the CE), as well as the harmonization or reception of EU legislation by other countries, including, but not limited to neighboring states.

The basis of the EU legal framework in the field of information space control consists of the following regional acts: Council of Europe Convention on Cybercrime, art. 16, 36, Council of Europe Convention on the Prevention of Terrorism arts. 23–24, Council of the European Union Framework Decision 2008/919 / JHA of 28 November 2008 amending Framework 22 Decision 2002/475 / JHA on combating terrorism and Council of Ministers. In its report, the European Commission notes that digital evidence is required in about 85% of all crimi-

nal investigations [9]. It was also proposed to create a digital evidence exchange system (eEDES). The Budapest Convention on Cybercrime is the international framework for cooperation between states in this area. Provisions concerning cooperation in the field of criminal justice between the EU States police forces and judiciary are also set out in Chapter V of the Treaty on the Functioning of the European Union. Article 83 of this treaty specifically refers to terrorism as a serious crime.

Several member States of the European Union (Belgium, United Kingdom, Northern Ireland) have indicated that data storage records are the only means of investigating certain crimes related to the Internet communication, as chat messages, for instance, can only be tracked using the Internet data-traffic. We observe that many messengers and social networks such as WhatsApp, Facebook[1], Telegram, Viber, VKontakte can be used by terrorists and extremists for their own purposes [10, 183–197]. This is evidenced not only by numerous studies by scientists, but also by the well-known sad events in various regions of the world, including the EU. That is why it is necessary to control social networks in order to adequately and legitimately identify potential terrorists and extremists, or in order to eliminate the possible consequences of such communication.

On March 16, 2021, the EU Council adopted a decree on combating the spread of terrorist content on the Internet [11]. Competent member States authorities are now empowered to require providers to remove or disable access to the relevant information (specifically, terrorism-related content) in all member States [12]. The respective shall be satisfied within an hour. On the one hand, such a measure can prove extremely effective in the fight against terrorism and radical associations, since their ideas can be perceived by the public who is unprepared and unaware of the threat of such activities to the world community stability. On the other hand, it can be considered as “postmeasure”, since it does not prevent posting such content, but rather blocks or erases it. Criminals successors can save information on their devices and follow their instructions [13].

Generally speaking, we can state the fact that the states of the Asian region are the most dangerous in the context of terrorist attacks threat or extremist ideas spreading. However, in the EU, many countries still occupy a fairly high position in specialized ratings. Thus, in the European Union the following states were most susceptible to terrorist threats: Turkey (18th place), Great Britain (30th place), France (38th place), Greece (44th place), Sweden (61st place), Ireland (62nd place), Spain (63rd place) [14]. In the same rating there were also the member states of the European Union with a zero rating – Croatia, Iceland, Monaco, Portugal, Romania, Slovenia. To conduct a qualitative study, we consider it necessary to analyze the crime situation both in states with a high level of crimes of terrorism and extremism, and with a low or even zero.

IV. Geography of information control over terrorism and extremism

The Republic of Turkey is ranked highest in Europe in the global terrorist index. Counter-terrorism in Turkey takes place at two independent, but logically interconnected levels – international and national. Such an integrated approach is associated with a well-known awareness of terrorist attacks scale and consequences. Restriction only at the national level leads to the absence of systemic approach, and, consequently, inability of the State to ensure the safety of their own citizens [15].

The present research analyzes the national-level measures only, as the initial actions in order to ensure a safe, "non-contaminated" information space are elaborated at national levels. For instance, more than 1/3 of the Turkish population use social networks as their main source of information [16]. Among the most popular networks is Facebook, used by 51 million Turkish users in 2020 [17]. Therefore, the necessity for enacting a new law is justified, at least in order to solve the problem of the so-called “digital fascism”. With the beginning of the digital era, the possession of information has become a special instrument of pressure in various spheres. The skillful use of such electronic tools poses a new threat to humanity. With the primary purpose of protecting its own citizens, the necessary measures were taken by the Turkish government [18].

According to the new law № 7253 of 07/29/2020, all sites of which the number of visits in the country exceeds 1 million users per day must appoint a legal representative so that the site's bandwidth is not reduced (in fact - blocking access for users) [19]. In case of this norm violation, legal entities shall pay a fine in the amount of one million Turkish lira (Article 3). At present, almost all Internet services have met this requirement, including the appointed official representatives of such companies as: Google, Facebook[1], Twitter[2], Pinterest, VKontakte, etc.

That’s the way how information space control in Turkey is exercised. Legal regulation of the media allows to ensure appropriate response to the Internet content, posted on websites and social networks [20]. The appointed legal representative of the media giants may be held criminally liable for failing to comply with the requirements imposed by the Turkish authorities [21].

Control over the information space in the Principality of Monaco (country with a zero index) has a number of distinctive features. Unlike Turkey, Monaco does not have a similar law, but, nevertheless, the formation of a safe cyberspace is a priority task of the state [22]. A cybersecurity agency (AMSN) and a cybercrime unit within the police department were created specifically to carry out this task. Special recommendations were developed for all citizens, and AMSN is making every effort to stop access to those information resources that pose a potential threat to the national security of the state [23].

The UK is ranked 30th in the global terrorism ranking. In the United Kingdom, legislation and case law allows British authorities to extend jurisdiction over extraterritorial terrorist and extremist crimes, including on the Internet. In doing so, it must be shown that a "substantial portion" of the criminal activity took place in the United Kingdom and that the perpetrator should not be prosecuted by another party. In the United Kingdom, section 3 of the Terrorism Act 2006 provides for content "blocking" notices that may be sent to Internet service providers by law enforcement (see section 172 et seq.). Blocked and that information that is considered illegal by law enforcement agencies, related to terrorism and extremism. ISPs that have been ordered to block certain content are required to remove it within two business days. It might seem that 2 days is a reasonable time to remove the relevant information. However, in reality, a few hours are enough for the implementation of criminal intent with the help of terrorist and extremist material of the "call to action" type. In this regard, numerous problems arise both in terms of preventing the emergence of such content and subsequent nonproliferation measures. Chapter VI of the Terrorism Act also contains a number of offenses that may serve as a basis for bringing charges against individuals who have used the Internet to support terrorist activities.

In the *United Kingdom R. v. Roshanara Choudhry*, the case of a self-taught terrorist was considered [24]. Chowdhry has been influenced by terrorists to commit violent acts using materials on the Internet, in particular video hosting websites. Chowdhry's case gained an international resonance due to the availability of user-generated content, which allowed her to find and view videos of extremist Islamic content, as a result of which the conviction of a terrorist act was formed through consistent viewing of the content for several months [25, 26]. In 2010, following discussions with the governments of the United Kingdom, led by the Counter Terrorism Online Division, and the US, where YouTube's servers are located, YouTube's parent company, Google Inc., implemented a potential terrorism-related content mechanism. This mechanism is an important tool for identifying content that may incite terrorist attacks.

Online payments can also be used by scammers. Identity theft, credit card theft, wire fraud, stock fraud, intellectual property crime and auction fraud are far from the entire spectrum of criminal activity. An example of the use of illegal proceeds to finance terrorist acts is the case in the *United Kingdom v. Younis Tsuli* [27]. The laundered money was used both to finance the registration of Tsuli 180 websites hosting Al-Qaeda propaganda videos and to provide equipment for terrorist activities in several countries [28]. Approximately 1,400 credit cards have been used to obtain almost £ 1.6 million in illicit terrorist financing.

Northern Ireland is ranked 62nd in the global terrorism ranking. The Criminal Justice (Terrorist Offences) Act 2005 [29] gives effect to a number of international instruments aimed at countering terrorism and responds to obligations within the European Union and the United Nations [30]. In particular, pursuant to article 63 of this act, police commissioner may ask the provider to retain for 3 years data traffic or location data, or both, for the purposes of preventing, detecting, investigating or prosecuting crimes (including but not limited to terrorist crimes), or ensuring the security of the state. Article 64 provides for cases where the provider is required to provide the relevant information. In Ireland, intelligence gathered about terrorists can amount to prima facie evidence that a particular person is a member of an illegal organization. The Irish Supreme Court has upheld the use of such intelligence as evidence, albeit in some circumstances. In 2010, the European Commission approved and provided funding for a project involving collaboration between academics, industry and law enforcement to establish a network of Cybercrime Centers of Excellence for Training, Research and Education (2CENTER) in Europe [31]. The network currently provides training through national centers of excellence located in Ireland and France. Each national center is based on a partnership between law enforcement officials and academics who develop relevant training programs in the fight against cybercrime.

The legal regulation of the information space in the countries of the Muslim legal system has a significant difference. First of all, it is worth noting the fact that initially the basis of the legislative framework of any Muslim country is based on the principles established in the Shaira, regardless of belonging to the legal school (Madhhab). Of particular importance, of course, are the historical and cultural features of the development of state and legal institutions in the country.

From the theory of Muslim law, it should be noted the theory of 4 roots of jurisprudence (uṣūl al-fiqh), which is equally reflected in almost all countries of the Muslim world. Traditionally, these include:

1. The Quran;
2. The Sunnah;
3. The Ijmā;
4. The Qiyas.

The Cairo Declaration of Human Rights in Islam of August 5, 1990, adopted within the framework of the Organization of Islamic Cooperation (OIC), is of key importance for the consolidation of fundamental rights and freedoms in the Muslim world. Article 9, paragraph b states: "Every human being has a right to receive both religious and worldly education from the various institutions of teaching, education and guidance, including the family, the school, the university, the media, etc., and in such an integrated and balanced manner that would develop human personality, strengthen man's faith in Allah and promote man's respect to and defence of both rights and obligations. Article 22 notes the special importance of information, paragraph C states: «(c) Information is a vital necessity to society. It may not be exploited or misused in such a way as may violate sanctities and the dignity of Prophets, undermine moral and ethical Values or disintegrate, corrupt or harm society or weaken its faith».

De facto, at the regional level, a qualitative characteristic of information data is established, and some restrictions are also imposed on the use of information that undermine the values protected and conserved by the Muslim law.

In addition to the above-mentioned sources, Muslim law also distinguishes:

1. Fatva;
2. Adat law;
3. Urf.

In the context of this research, a Fatwa deserves special attention, it is it that establishes some features of the regulation of the information space. At the same time, there is no unity in them, there is still no clear distinction between what is allowed and what is forbidden. In relation to the same phenomenon, various prescriptions can be established, for example, YouTube video hosting, which has repeatedly become the subject of analysis in terms of access to the data contained in it. One of the fatwas establishes a ban on its use because of the materials contained in it. However, another fatwa allows fair use with careful control of information that should not contradict the legal regulation of Fiqh.

For example, in Saudi Arabia, the question was raised whether an Internet cafe contradicts Muslim law? The answer was: "If this equipment can be used for false and malicious purposes that will harm Islamic beliefs or allow people to watch forbidden pictures and movies, or news about immortal entertainment, or conduct questionable conversations and play forbidden games, and the owner of the cafe cannot prevent this evil or to drive cars, then in that case he is forbidden to do it, because it helps in sin and forbidden things".

In some madhhabs, the question is raised about the use of the Internet space by women, as well as communication with men in the social networks, including emojis as the expression.

The regulation of the information space in Iran has been developing most actively in recent years. The authorities pay attention to monitoring not only on ordinary websites, but also on social networks. The priority task is also to block access to information prohibited on the territory of the state and those tools that allow access to prohibited information (VPN services are often used for this).

Instagram[3] and WhatsApp have been officially banned in the state. At the moment, there are difficulties in restricting users' access to virtual private networks (VPNs) – applications that provide an encrypted connection to a remote server, protecting user data, anonymizing his actions and thereby allowing circumventing censorship.

There is an active fight against applications that allow access to certain prohibited data. For example, the Signal application, which has been banned and blocked in Iran since January 2018. A phone number is required for registration and at the time of its setup, a text must be sent to the user's phone to confirm the number. These texts are blocked by the Iranian network, which prevents the completion of the Signal account creation.

Meredith Whittaker, president of the Signal Foundation, which is responsible for the support and development of the application, told RSF that the blocking "occurs at the level of telecommunications infrastructure that we do not control." This is a problem "for which there is no solution that we could implement," she said [32].

As for the situation in the French Republic, the French government has no legal authority to restrict Internet use, including during a state of emergency. Also, as of today, there have been no cases of government blocking web content for political reasons. However, France has become one of the few countries to block two prominent piracy websites, Sci-Hub and LibGen, which offer free access to millions of academic books, journals and articles. After filing a complaint by publishers Elsevier and Springer Nature, the court ordered the four main French Internet providers (Orange, Free, Bouygues Telecom, SFR) to block the two websites in April 2019.

Earlier, in December 2018, the court, after considering a complaint from six associations fighting

against copyright infringement of films, ordered the same Internet providers to block several illegal streaming services for distributing pirated content. After a series of terrorist attacks in Paris in November 2015, Internet resources were also censored, the materials of which were in one way or another related to terrorism or acts of incitement to hatred. In November 2018, a Paris court ordered nine French internet providers to block the anti-Semitic website *Democratie Participative*, which disseminated information about the activities of French far-right and extremist organizations.

Government Decree 2015-125 sets out administrative measures to block websites containing materials that incite or justify terrorism, as well as portals that demonstrate child abuse. Soon after the decree was published, five websites were blocked for propaganda of terrorism. In subsequent years, the number of portals blocked for the same reason has increased significantly. According to the data protection agency (*CNIL – Commission nationale de l'informatique et des libertés*) and the Central Office for the Fight against Crime Related to Information and Communication Technologies (*OCLCTIC – Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication*) between March 2018 and February 2019, the French courts issued 879 orders to block websites by Internet providers. At the same time, 82 of these sites were blocked due to the posting of materials related to the propaganda of terrorism, and the remaining 797 - on the basis of demonstrating acts of child abuse.

In some cases, French government decrees instruct online platforms to remove or restrict access to content. For example, in December 2018, a French court ordered Google to hide search results containing links to streaming services that violate current French law.

According to Google's transparency report, in the first half of 2018, the French government sent 244 requests to remove posts posted on various portals, in most cases justifying this on national security grounds. Google satisfied 71 percent of these requests, while Twitter[2], after receiving 243 related requests, satisfied only 5% of them [24]. In 2018, Facebook[1] also restricted access to 667 content items in France, most of which are related to Holocaust denial. It is worth noting that the materials were removed or hidden not only at the request of the government, but also on the grounds of private actions for libel (208 out of 667 publications).

V. Research results

According to the results of this study, the following potential measures are proposed in relation to the information space in the framework of facing new challenges and threats of terrorism and radical formations: deanonymization, keyword recognition mechanisms, police and judicial cooperation, cooperation within European and international organizations.

With the purpose of identifying individuals prone to terrorism and extremism, a chain of sequences should be developed through which such users can be distinguished. For example, establishing for what purpose the crime-related content was viewed (educational, scientific, personal interest). Undoubtedly, that can be done through general analysis of the user profile. Naturally, it is impossible to watch every video on YouTube video hosting and determine its semantic content. Uploading a video and validating it for publication on the web should be one of the key factors in discouraging dissemination of this kind of content. Opponents of this approach may report censorship and periodic delays and difficulties when uploading content, on the other hand, the lack of such barriers makes almost impossible to restrict susceptible persons from viewing such content. It's high time we agreed on a middle ground between freedom and security. The problem of cyberterrorism and cyber-extremism is particularly relevant [33], the use of an information network by criminals allows promoting extremist ideology, which threatens the national security of any state. It is necessary to strengthen regional cooperation, in this regard, we can use the experience of the Shanghai Cooperation Organization, and expand the scope of interaction of competent authorities to maintain international information security.

VI. Conclusion

Analyzing the ways of organizing control over the information space, the following groups of states can be distinguished: EU countries, Turkey, Iran (preventing access to those data that contradict the constitutional provisions of the Islamic Republic of Iran)

What control options are there at the moment:

– full;

– moderate;

– low filtration level.

Cooperation with other countries:

– active cooperation, formation of a uniform approach to the legal regulation of the fight against terrorism and extremism;

– focus on national legal regulation, cooperation if necessary;

– priority of national legal regulation in the sphere of control of the information space.

The experience of Monaco, France, Turkey, Great Britain and Northern Ireland illustrates the most successful methodologies and practices in the area of combatting terrorism and extremism in the ICT field. It is necessary not only to regulate the

issue by legislation, but also to jointly organize competent authorities in the fight against crime, to create a network of interaction. This should also strengthen the integration processes within the European Union. A similar approach can be used by other countries in order to ensure the safety of their own citizens. This approach is also possible within the EAEU, taking into account the specifics of the national legislation of the participating countries.

The development of qualitatively new formulas for artificial intelligence trained to identify potential terrorists and extremists through monitor the users activity in social networks and analyzing behavioral features is also one of the desired measures. With the development of technology, criminals began to improve their methods. Meanwhile, the fundamental criminological principles developed by science for systemic counteraction to crime must be taken into account. Terrorism is a global problem of humanity, therefore regionalization cannot negate the fact that effective counteraction requires mutual cooperation of the global community.

Eliminating the ability for criminals to communicate with each is bound to aid in prevention of possible terrorist and crimes against the state and political system. This method of counteraction is viewed by the authors as the most effective. However, methods and means to be chosen by the States must meet technological and informational requirements of the 21st century.

The creation of a unified procedure for obtaining social media accounts can potentially eliminate the likelihood of information space use for the purpose of committing illegal acts [34]. For instance, the requirements shall concern indicating the purpose of registration, further usage of the online network, methods of communication, possible “friends”.

Acknowledgements: We would like to express our gratitude to Boagiy Emma for her valuable and constructive advice during the planning and development of this paper, particularly with the analysis of foreign sources. Her willingness to pay attention so generously to this paper has been highly appreciated.

The publication was prepared with the support of the MGIMO-University within the framework of the XIV MGIMO Young Scientists Competition "New Space for International Cooperation". The authors also expresses gratitude to Emma Boagiy for valuable comments during the planning and development of this paper.

Примечания

1. Facebook – принадлежит компании Meta, признанной экстремистской в РФ.

2. Twitter – заблокирована на территории РФ по требованию Генпрокуратуры.

3. Instagram – принадлежит компании Meta, признанной экстремистской в РФ.

Список литературы

1. Stalinsky S., Sosnow R. Encryption Technology Embraced by ISIS, Al-Qaeda, Other Jihadis, Reaches New Level with Increased Dependence on Apps, Software. The Middle East Media Research Institute, Inquiry and Analysis Series. 2015. Report № 1168.

2. Ivanchenko E.A., Kulikova T.B., Zhukovskii V.I., Dovgolyuk N.V. Forms of Information Extremism on the Global Internet // Advances in Science, Technology and Innovation. 2022. P. 785–789. DOI: 10.1007/978-3-030-90324-4_127.

3. Бизина М.Ю. Сравнительный анализ законодательных актов о борьбе с экстремизмом и терроризмом в сети Интернет // Информационные войны. 2022. № 1 (61). С. 42–46.

4. Рузавина А.К. Интернет и социальные сети как фактор распространения молодежного экстремизма // Вопросы политологии. 2021. Т. 11. № 4 (68). С. 1174–1181. DOI: 10.35775/PSI.2021.68.4.024.

5. Huey L. This is not your Mother’s Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming // Journal of Terrorism Research. 2015. 6.

6. Pearson E. The Case of Roshonara Choudhry: Implications for Theory on Online Radicalization, ISIS Women, and the Gendered Jihad // Policy & Internet. 2016. 8. P. 5–33. https://doi.org/10.1002/poi3.101.

7. Russia has submitted the first draft of the convention on combating cybercrime to the UN // Rossiyskaya Gazeta. 2021. Issue № 168 (8519).

8. On submission to the UN Special Committee of the Russian draft of a universal international convention on countering the use of information and communication technologies for criminal purposes // MFA of the Russian Federation. 1504-28-07-2021.

9. Communication from the commission to the European parliament, the European council, the Council, the European economic and Social committee and the Committee of the regions. Brussels, 9.12.2020 COM (2020) 795 final.

10. Macdonald S., Correia S.,Watkin A. Regulating terrorist content on social media: Automation and the rule of law // International Journal of Law in Context. 2019. 15 (2). P. 183–197. https://doi.org/10.1017/S1744552319000119.

11. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online // Official Journal of the European Union. L172/79. 04.07.2023.

12. West Levi. Chapter 9: Counter-terrorism, social media and the regulation of extremist content. In Counter-Terrorism. Cheltenham, UK: Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781800373075.00016.

13. Macdonald S. Terrorist Narratives and Communicative Devices: Findings from a Study of Online Terrorist Magazines // In: Zeiger, Sara (ed.), Expanding Research on Countering Violent Extremism. Abu Dhabi/Perth: Hedayah / Edith Cowan University. 2016. P. 127–141.

14. Global terrorism index // Institute for Economics & Peace [Electronic source]. URL: https://nonews.co/wp-content/uploads/2021/01/GTI2020.pdf (date of access: 04.07.2023).

15. Turkey’s Contributions to International Community’s Efforts to Fight Terrorism. URL: https://www.mfa.gov.tr/turkeys-contributions-to-international-communit

ys-efforts-to-fight-terrorism.en.mfa (date of access: 04.07.2023).

16. Turkey's social media law: A cautionary tale // Politico Live [Electronic source]. URL: https://www.politico.eu/article/turkeys-social-media-law-a-cautionary-tale/ (date of access: 04.07.2023).

17. Recep Tayyip Erdogan targets social media in Turkey // DW. Retrieved from: https://www.dw.com/en/recep-tayyip-erdogan-targets-social-media-in-turkey/a-53792631

18. President Erdoğan attends opening ceremony of newly-restored Museum of Painting of the National Palaces // Presidency of the Republic of Turkiye. Retrieved from: https://www.tccb.gov.tr/en/news/542/123582/president-erdogan-attends-opening-ceremony-of-newly-restored-museum-of-painting-of-the-national-palaces#

19. Turkey's New Internet Law and Its Effects on Freedom of Media // ResetDOC Europe. Gülcin Balamir Coskun 12 July 2021. Retrieved from: https://www.resetdoc.org/story/turkey-internet-law-freedom-media/

20. Xu Jie, Daning Hu, and Hsinchun Chen. The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad // Journal of Homeland Security and Emergency Management. 2009. 6 (1). P. 1–33.

21. Borelli M. Social media corporations as actors of counter-terrorism // New Media & Society. 2021. https://doi.org/10.1177/14614448211035121.

22. Digital Security: a challenge for the future // Gouvernement Princier, Principaute de Monaco. Retrieved from: https://en.gouv.mc/Policy-Practice/A-Modern-State/Digital-Security-a-challenge-for-the-future

23. Best practices for protecting yourself from cybercrime // Gouvernement Princier, principaute de Monaco. Retrieved from: https://en.service-public-particuliers.gouv.mc/Security-safety-prevention/Digital-security/Cybercrime-prevention-and-recommendation/Best-practices-for-protecting-yourself-from-cybercrime

24. Mair D. Westgate: A Case Study: How al-Shabaab Used Twitter during an Ongoing Attack // Studies in Conflict & Terrorism. 2017. 40 (1). P. 24–43.

25. Conway M., Jodie P., and Sean L. Online Jihadi Instructional Content: The Role of Magazines // In: Conway, Maura et al. (eds.), Terrorists' Use of the Internet: Assessment and Response. NATO Science for Peace and Security Series – E: Human and Societal Dynamics. 2017. 136. Amsterdam: IOS Press. P. 182–193.

26. Conway M. Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research // In: Anne Aly, Stuart Macdonald, Lee Jarvis and Thomas Chen (eds.), Violent extremism online: New perspectives on terrorism and the Internet. Abingdon: Routledge, 2016. P. 123–148.

27. 'Internet jihadist' jailed for 10 years // The Guardian. Retrieved from: https://www.theguardian.com/technology/2007/jul/05/terrorism.uknews

28. Shajkovci A. Engaging English Speaking Facebook Users in an Anti-ISIS Awareness Campaign // Journal of Strategic Security. 2018. 11(3). P. 52–78.

29. Criminal justice (terrorist offences) act 2005. Retrieved from: http://www.irishstatutebook.ie/eli/2005/act/2/enacted/en/html

30. Terrorism // An Roinn Dli agus Cirt, Department of Justice. Retrieved from: http://www.justice.ie/en/jelr/pages/terrorism (date of access: 04.07.2023).

31. The use of internet for terrorist purposes // UNODC. Retrieved from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

32. How the Islamic Republic has enslaved Iran's Internet. URL: https://rsf.org/en/how-islamic-republic-has-enslaved-iran-s-internet (date of access: 04.07.2023).

33. Awan I. Cyber-Extremism: Isis and the Power of Social Media // Society. 2017. 54 (2). P. 138–49. https://doi.org/10.1007/s12115-017-0114-0.

34. Farwell J.P. The Media Strategy of ISIS // Survival. 2014. 56 (6). P. 49–55. https://doi.org/10.1080/00396338.2014.985436.

35. Analysing social media // Interpol [Electronic source]. URL: https://www.interpol.int/Crimes/Terrorism/Analysing-social-media

STATE CONTROL OVER THE INFORMATION SPACE AS A WAY TO COMBAT TERRORISM AND EXTREMISM: A COMPARATIVE LEGAL STUDY

S.S. Melnik, V.E. Karpovich

The paper analyzes the legal regulation of the information space of states in the field of countering terrorism and extremism as the most pressing problems of the global society. The essential basis of the study is the comparative characteristics of the legislation of the member states and candidates for EU membership, as well as the countries of the Muslim legal family in the information space. Using the example of States with the most effective regulatory framework, the need for comprehensive and progressive control of the information space as a means of preventing and countering a set of terrorist and extremist threats is demonstrated. Meanwhile, the facts of a decrease in the level of security in the States currently affected by such threats are also taken into account. Particular attention is paid to the experience of such states as Monaco, Turkey, France, Great Britain and Northern Ireland. The authors substantiate the polysystemic nature of international cooperation in the fight against terrorism and extremism in the information space, as well as put forward a classification of countries depending on the chosen criminological approach to countering terrorist and extremist threats in the information space.

Keywords: extremism, terrorism, information security, combatting terrorism and extremism, European Union, Muslim law countries.

References

1. Stalinsky S., Sosnow R. Encryption Technology Embraced by ISIS, Al-Qaeda, Other Jihadis, Reaches New Level with Increased Dependence on Apps, Software. The Middle East Media Research Institute, Inquiry and Analysis Series. 2015. Report № 1168.

2. Ivanchenko E.A., Kulikova T.B., Zhukovskii V.I., Dovgolyuk N.V. Forms of Information Extremism on the Global Internet // Advances in Science, Technology and Innovation. 2022. P. 785–789. DOI: 10.1007/978-3-030-90324-4_127.

3. Bizina M.Yu. Comparative analysis of legislative acts on combating extremism and terrorism on the Internet // Information Wars. 2022. № 1 (61). P. 42–46.

4. Ruzavina A.K. The Internet and social networks as a factor in the spread of youth extremism // Questions of political science. 2021. Vol. 11. №4 (68). P. 1174–1181. DOI: 10.35775/PSI.2021.68.4.024.

5. Huey L. This is not your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming // Journal of Terrorism Research. 2015. 6.

6. Pearson E. The Case of Roshonara Choudhry: Implications for Theory on Online Radicalization, ISIS Women, and the Gendered Jihad // Policy & Internet. 2016. 8. P. 5–33. https://doi.org/10.1002/poi3.101.

7. Russia has submitted the first draft of the convention on combating cybercrime to the UN // Rossiyskaya Gazeta. 2021. Issue № 168 (8519).

8. On submission to the UN Special Committee of the Russian draft of a universal international convention on countering the use of information and communication technologies for criminal purposes // MFA of the Russian Federation. 1504-28-07-2021.

9. Communication from the commission to the European parliament, the European council, the Council, the European economic and Social committee and the Committee of the regions. Brussels, 9.12.2020 COM (2020) 795 final.

10. Macdonald S., Correia S.,Watkin A. Regulating terrorist content on social media: Automation and the rule of law // International Journal of Law in Context. 2019. 15 (2). P. 183–197. https://doi.org/10.1017/S1744552319000119.

11. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online // Official Journal of the European Union. L172/79. 04.07.2023.

12. West Levi. Chapter 9: Counter-terrorism, social media and the regulation of extremist content. In Counter-Terrorism. Cheltenham, UK: Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781800373075.00016.

13. Macdonald S. Terrorist Narratives and Communicative Devices: Findings from a Study of Online Terrorist Magazines // In: Zeiger, Sara (ed.), Expanding Research on Countering Violent Extremism. Abu Dhabi/Perth: Hedayah / Edith Cowan University. 2016. P. 127–141.

14. Global terrorism index // Institute for Economics & Peace [Electronic source]. URL: https://nonews.co/wp-content/uploads/2021/01/GTI2020.pdf (date of access: 04.07.2023).

15. Turkey's Contributions to International Community's Efforts to Fight Terrorism. URL: https://www.mfa.gov.tr/turkeys-contributions-to-international-community's-efforts-to-fight-terrorism.en.mfa (date of access: 04.07.2023).

16. Turkey's social media law: A cautionary tale // Politico Live [Electronic source]. URL: https://www.politico.eu/article/turkeys-social-media-law-a-cautionary-tale/ (date of access: 04.07.2023).

17. Recep Tayyip Erdogan targets social media in Turkey // DW. Retrieved from: https://www.dw.com/en/recep-tayyip-erdogan-targets-social-media-in-turkey/a-53792631

18. President Erdoğan attends opening ceremony of newly-restored Museum of Painting of the National Palaces // Presidency of the Republic of Turkiye. Retrieved from: https://www.tccb.gov.tr/en/news/542/123582/president-erdogan-attends-opening-ceremony-of-newly-restored-museum-of-painting-of-the-national-palaces#

19. Turkey's New Internet Law and Its Effects on Freedom of Media // ResetDOC Europe. Gülcin Balamir Coskun 12 July 2021. Retrieved from: https://www.resetdoc.org/story/turkey-internet-law-freedom-media/

20. Xu Jie, Daning Hu, and Hsinchun Chen. The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad // Journal of Homeland Security and Emergency Management. 2009. 6 (1). P. 1–33.

21. Borelli M. Social media corporations as actors of counter-terrorism // New Media & Society. 2021. https://doi.org/10.1177/14614448211035121.

22. Digital Security: a challenge for the future // Gouvernement Princier, Principaute de Monaco. Retrieved from: https://en.gouv.mc/Policy-Practice/A-Modern-State/Digital-Security-a-challenge-for-the-future

23. Best practices for protecting yourself from cybercrime // Gouvernement Princier, principaute de Monaco. Retrieved from: https://en.service-public-particuliers.gouv.mc/Security-safety-prevention/Digital-security/Cybercrime-prevention-and-recommendation/Best-practices-for-protecting-yourself-from-cybercrime

24. Mair D. Westgate: A Case Study: How al-Shabaab Used Twitter during an Ongoing Attack // Studies in Conflict & Terrorism. 2017. 40 (1). P. 24–43.

25. Conway M., Jodie P., and Sean L. Online Jihadi Instructional Content: The Role of Magazines // In: Conway, Maura et al. (eds.), Terrorists' Use of the Internet: Assessment and Response. NATO Science for Peace and Security Series – E: Human and Societal Dynamics. 2017. 136. Amsterdam: IOS Press. P. 182–193.

26. Conway M. Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research // In: Anne Aly, Stuart Macdonald, Lee Jarvis and Thomas Chen (eds.), Violent extremism online: New perspectives on terrorism and the Internet. Abingdon: Routledge, 2016. P. 123–148.

27. 'Internet jihadist' jailed for 10 years // The Guardian. Retrieved from: https://www.theguardian.com/technology/2007/jul/05/terrorism.uknews

28. Shajkovci A. Engaging English Speaking Facebook Users in an Anti-ISIS Awareness Campaign // Journal of Strategic Security. 2018. 11(3). P. 52–78.

29. Criminal justice (terrorist offences) act 2005. Retrieved from: http://www.irishstatutebook.ie/eli/2005/act/2/enacted/en/html

30. Terrorism // An Roinn Dli agus Cirt, Department of Justice. Retrieved from: http://www.justice.ie/en/jelr/pages/terrorism (date of access: 04.07.2023).

31. The use of internet for terrorist purposes // UNODC. Retrieved from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

32. How the Islamic Republic has enslaved Iran's Internet. URL: https://rsf.org/en/how-islamic-republic-has-enslaved-iran-s-internet (date of access: 04.07.2023).

33. Awan I. Cyber-Extremism: Isis and the Power of Social Media // Society. 2017. 54 (2). P. 138–49. https://doi.org/10.1007/s12115-017-0114-0.

34. Farwell J.P. The Media Strategy of ISIS // Survival. 2014. 56 (6). P. 49–55. https://doi.org/10.1080/00396338.2014.985436.

35. Analysing social media // Interpol [Electronic source]. URL: https://www.interpol.int/Crimes/Terrorism/Analysing-social-media