Keeping Minors Safe in Cyberspace: Extremist and Terrorist Threats

O V Nardina[1]

[1]Yelets State University. I.A. Bunina, Yelets, Russia

E-mail: nardina-oksana@yandex.ru

Abstract. Minors are active users of cutting-edge communication technologies; joining virtual communities or messaging with remote users, they face numerous threats and risks. The Internet has an increasing population of websites and social media pages that seek to promote extremist and terrorist ideas and practices. Minors tend to lack the knowledge and skills for identification of destructive manipulations; when mingling with such communities, they risk devaluing their moral foundations, losing their family values, and degrading as personalities. Then they become involved with extremists and coerced to commit terrorist attacks.

The state has undertaken to keep minors safe in cyberspace. However, digital technologies advance at a far greater pace than the legal frameworks to address the challenges they create.

1. Introduction

Cutting-edge communication technologies open up ample opportunities to convey and disseminate information, making them an efficient tool for manipulating persons and groups alike. However, unconstrained (and anonymous) exchange and dissemination of information on the web coupled with the lack of legal framework to regulate it as well as with the novelty of such relations has given rise to problems that threaten people's information security and may disrupt civil peace and social harmony.

Extremist and terrorist cells use digital communications to improve organization, collect data for the arrangement and conduct of mass riots and terrorist attacks, train their 'champions' and manipulate the target audience to recruit more; ICT also helps fuel their fundraising campaigns based on donations, extortions, etc. Notably, the organizations that promote violence and justify extremism and terrorism while inciting interracial, national, and religious intolerance invest well in their websites. These websites usually offer a good theoretical overview and argumentation for what they promote; they try to pose themselves as liberators and use a broad set of psychological manipulation methods while enjoying outstanding protection of their resources against governmental intervention.

Extremist and terrorist websites target a broad audience; however, minors are the most vulnerable part of that audience. For one, minors lack the knowledge, life experience, and professional skills it would take to adequately evaluate the incoming information; secondly, they are often prone to aggression and extremism; thirdly, they are the most socially vulnerable population. These and other factors first deteriorate minors' moral and spiritual values as well as their views of the state and society; then it is easy to recruit a minor for crime.

In this context, many democratic governments try to minimize extremists' and terrorists' access to the benefits of ICT; to that end, they use various means to block websites. This is an arguably necessary evil, relying on which creates a multitude of legal problems as it violates the fundamental human rights.

Countering terrorism and extremism in cyberspace is an urgent matter researched worldwide. Prominent is a paper by A.N. Odhiambo, N.M. Ochara, and A. Kadymatimba, Structuring of the Terrorism Problem in the Digital Age: A Systems Perspective [1]. Researchers insist that widespread Internet access is in direct correlation with the rise of terrorism. Terrorist cells such as ISIS use the Internet to innovate the processes of recruitment, training, and ideology spreading. M. Bogdanovsky in his paper Link Between Cyberspace and Today's Terrorism [2] overviews the opportunities cyberspace opens up for terrorists. While he does delineate such concepts as 'use of cyberspace by terrorists', 'cyber attacks', and 'cyberterrorism', he analyzes all of them from the standpoint of the threat they pose to national and global security. N.S. Grove in her Weapons of mass participation: Social media, violence entrepreneurs, and the politics of crowdfunding for war [3] analyzes social media and online money transfer tools as the platforms extremists and terrorists can use to get moral support and funding.

Cyberspace is clearly a dangerous tool in the hands of violence advocates. Governments that try to combat such negative content focus on protecting the critical information infrastructures and databases, which overshadows the fundamental human rights to information. K. Huszti-Orban in her report at a cyber conflict conference noted the importance of adhering to the international human rights standards when trying to control the Internet [4]. Paper [5] analyzes cybersecurity from the human point of view. Such human rights as the freedom of expression and the right to privacy, as she argues, must be covered by the cybersecurity programs and well-protected in the digital environment. However, how could we adapt the constitutional human rights to the digital environment and exercise such rights ubiquitously if the law itself is transformable? M. J. Espinosa in his Privacy [6] analyzes the right to privacy from the standpoints of comparative law. He compares the constitutional norms and their enforcement in different countries, and notes that privacy links to such broad concept as freedom and dignity; for him, privacy is an evolving concept that continues to expand so as to confront the new demands and the challenges of a changing context.

Russian cybersecurity researchers are also concerned with that of minors. L.A. Burayeva analyzes the issues of combating extremism and terrorism in the global information space; she notes that such cells first of all target minors for recruitment [7]. Ye.I. Deshina and A.N. Merkulova in their paper Young People on the Net: Most Susceptible to Extremism and Terrorism [8] note a need for cutting-edge national information security technologies that would curb the popularization of extremist and terrorist idea with the youth. O.V. Nardina generally agrees with Ye.I. Deshina and A.N. Merkulova; however, she believes their approach to curbing extremism and terrorism is too narrow [9]. Efforts to tackle that must cover not only the cyberspace, but also the culture and the ideology.

2. Freedom of information and how it has evolved

Despite the fact that information society is a relatively recent phenomenon, freedom of information is not a new subjective human right; rather, it is a manifestation of traditional freedom of though and of speech. Those have been enshrined in multiple international laws such as Article 19 of the Universal Declaration of Human Rights; Articles 10 and 11 of the European Convention on Human Rights and Fundamental Freedoms; Articles 19 and 20 of the International Covenant on Civil and Political Rights; as well as in the constitutions of democratic nations. Research into the fundamental international acts and constitutional norms leads to a conclusion that information rights are essential to the information and legal status of a human person, of a citizen. Secondly, it is the exercise of such rights that furthers cultural, scientific, and economic ties. Thirdly, a rule-of-law state is expected to guarantee such rights. However, the social significance of the right to search for, disseminate, and convey information does not make it absolute. The European Convention sets forth the right could be limited for the benefit of democracy, e.g. when the right to disseminate information is contrary to the public interests: national security, health and life, other rights and freedoms.

The right to access telecommunications is a transformation of such constitutional rights as the freedom of information, freedom of opinion, and freedom of expression. The April 29, 1982 Council of Europe Declaration on the Freedom of Expression and Information directly links the freedom of expression to the access to communications. Human rights issues as affected by the modern technology are now on the agenda of multiple international organizations. Thus, the UNGA Resolution of December 18, 2013 (A/RES/68/167) *The right to privacy in the digital age* formulates the concept of applying the human right guarantees to the virtual environment: "the same rights that people have offline must also be protected online, including the right to privacy", see Clause 3. Based on that principle, the UNGA calls upon all states to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, see Clause 4. In this regard, the UNGA Resolution of 13 June 2014, 68/276, *The United Nations Global Counter-Terrorism Strategy Review* urges all states to respect and protect fundamental human rights in the fight against terrorism, to ensure that the restrictions of this right are not arbitrary, properly regulated by law, subject to effective supervision and are covered by appropriate legal protection mechanisms, including through judicial supervision or other legal means.

However, some countries seek to combat the propaganda of violence, extremism and terrorism; their attempts result in adopting laws that limit the constitutional human rights, including the right to disseminate information. For instance, China, North Korea, Iran, and some other countries have imposed total control over their national providers' gateways to the international information networks to filter or block information. In fact, these governments censor the Internet. We believe such measures will hinder the development of the information society. The UNGA Resolution of July 1, 2016 70/291 urges to ensure that any restriction of the freedom of expression in global computer networks be necessary and coherent while not violating human rights to access the Internet and the information it might provide, nor compromising the related important rights such as freedom of thought, conscience, religion, denomination, and belief. This resolution calls upon States, while countering terrorism and preventing violent extremism conducive to terrorism, to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy, by ensuring the full and effective implementation of all their obligations under international human rights law.

Thus, the international acts based on the exercise of right to information on the Internet on two principles: minimum government intervention; and adopting strict rules only in cases where lack of legal regulation of such public relations will threaten the information security of persons, society, and state. This requirement is a legitimate reason to restrict one's freedom of expression. It is also in line with the constitutional requirement to ban hate speech or any calls for violence and discrimination on whatever basis.

3. Russian legislation to curb extremist and terrorist activity in cyberspace: enforcement experience

Like any other state, the Russian Federation today has not only to enforce and protect the constitutional rights and freedoms of its citizens while furthering its economic, scientific, and technological potential, but also to ensure the information security of persons, society, and state. The country's *Strategy to Counter Extremism for Until 2025* recognizes the elevated public danger of unlawful use of IT, which manifests itself as the diffusion of destructive ideas, ideologies, and information via terrorist, extremist, and rebel websites.

The regulations to counter dissemination of extremist and terrorist material on the Internet include the Laws No 2124-I dd. December 27, 1991 *On Mass Media*; No. 114 dd. July 25, 2002 *On Countering Extremism*; No. 126 dd July 7, 2003 *On Communications*; and No. 149 dd. July 27, 2006

On Information, Information Technology and Protection, etc. These regulations have been fundamental to the Unified Register of Domain Names and(or) Website References that lead to content banned in Russia, such as pornography or similar images; promotion of drugs and psychotropic substances; as well as any attempts to predispose a child to self-harm, including suicide; any other extremist materials. According to Roskomnadzor, in Q4 of 2018 58,111 websites were added to the Register [10]. Registered resources are to be removed by their owners upon providers' notification. Besides, the Prosecutor's Office is empowered to ban websites that call for violence, riots, and extremism. Registering some information as prohibited or restricting access to it might well be necessary; however, it is how this is done that requires rigorous revision.

First, the extrajudicial procedure for blocking websites specifies no exact criteria on what is prohibited and what is not; as such, the procedure is prone to abuse. The very possibility of such abuse points to the violation of the constitutional right to equality as well as possible encroachments on the rights to information. Even access to legal contents can be denied, as blocking mechanisms are not selective. If one IP address hosts multiple websites, banning any of them will also block the rest. Researchers have presented statistics on it: for 40 thousand directly blocked resources, there is another 800 thousand sites that are blocked inadvertently [11].

Second, those who might be in for a crime will quickly adapt to, and bypass, such bans. For instance, they can relocate their data to another IP address if blocked; create mirror websites; use technical tools and software to bypass the restrictions; or even restrict access to their resources by requiring password; etc.

Thus, the regulatory framework on diffusing the extremist and terrorist materials contradicts Art. 10 of the European Convention on Human Rights as well as Art. 29 of the Russian Constitution. Limiting the rights to information and its dissemination, in fact, has so far had no effect on extremist and terrorist resources. That is because offenders are capable of evading the law.

4. Keeping minors safe in cyberspace

The Russian law has not only the general provisions to limit the dissemination of extremist and terrorist materials in cyberspace; it also has special provisions to enable minors to surf the Web safely and productively. What we are speaking of is the Federal Law dd. December 29, 2010 No. 434 On Protecting Children From Health and Development Compromising Information, which mandates filtering to reduce the diffusion of information intended to spread violence, extremism, or terrorism. However, the legislation is far from perfect in this regard. As the law does not specify where exactly such restrictions should apply, law enforcement agencies tend to abuse it. In 2016, a bus operator was fined in Saratov as the public WiFi on the bus did not have filters [12]. Besides, content filtering reduces other users' access to information, which qualifies as censorship.

Seeking to protect children against undesirable information, the Ministry of Education has obliged educational institutions, libraries, and other agencies to have content filtering in place. However, the existing filters are far from being perfect. Law enforcement inspections often find that "despite content filters in place, computer users, including minors, can still access websites that publish literature on the Federal List of Extremist Materials." [13]. Besides, not every school has specialists competent enough to configure such software. This places some schools at a disadvantage. We believe that if the government wants schools and universities to filter contents, it should also enable them to do so, i.e. contract software developers to write, maintain, and continually improve software for school network infrastructure. Schools should be provided with ready-for-use software, which must be the same for all schools, as discriminatory access to protection is unacceptable. However, instead of taking constructive measures to protect minors in cyberspace, the government only raises the penalties [14].

While analyzing the crackdown on extremist and terrorist publications on the Internet, it should be noted that minors themselves are not immune to the law, as they can be brought criminal or administrative charges against for reposting extremist materials, incitement of hatred or hostility, propaganda or public display of Nazi symbols and swastikas. In Tomsk Oblast, two teenagers have been find for posting Walt Disney's classic Der Fuehrer's Face, an anti-fascist cartoon featuring

Donald Duck [15]. Such broad interpretation of extremism by law enforcers is unacceptable. Law enforcers, not to mention courts, must note not only the act of publication, but also the context of it. Legal and law-enforcement uncertainty often results in horrendous abuse that might ruin a teenager's life. Herein lies the fundamental problem, "...drawing a borderline between undesirable yet permissible behavior and punishable acts is a challenge that is far from being addressed, especially when it comes to the Internet." [16].

Computer games, including online games, contain display of violence and murder, which is a serious threat to minors' mental health. The minor player themselves often acts as a murderer and picks up the role model the game gives. As a result, disturbed minors commit shootings, explosions, and arsons at schools and other public places. To protect children from dangerous content, the Upper House of the Parliament drafted a bill on mandatory labelling of computer and video games in May 2019 [17]. It was, indeed, only the first step to regulating the distribution of video and online games; however, minors might well ignore the age labels.

There is a whole multitude of other issues concerning minors' safety and security in cyberspace; the government states the problems to the public but is not able to solve them. One major problem is the recruitment of minors to extremists and terrorist cells. Recruitment is anonymous and unmonitored; it thrives on social media. I.Yu. Sundiyev in his research of how extremists recruit minors notes that IT provides such destruction-oriented cells with a "global power and coverage while not necessarily putting them at risk of exposure. They might have given up meetings in person, but they can well make use of virtual environments for training and propaganda." [18]. Extremists have devised a multi-level system to identify and engage minors, first to actively support extremist ideas, then to commit crime. Online games on extremist websites are important to the process. The virtual environment might induce the player to take specific actions, e.g. to overthrowing the existing regime and to act against the statehood. To reach a higher level, the player must reproduce their virtual 'achievements' in the real world and then report to the organization. "Each level has a variety of quests of varying difficulty. The higher the level, the more difficult are the real-world 'quests'. Analysis of quests such online games have shows that their target audience is the youth, as the borderline between reality and virtual worlds is often blurred for younger games [18].

The list of issues of minors' safety in cyberspace is far from exhaustive herein. Still, lack of, or inappropriate governmental and public response to the information challenges of today boosts the legal nihilism among minors while infringing on the fundamental rights to freedom of information. If focusing solely on extremism and terrorism among the youth, it should be noted that the government actually recognizes the need to protect minors from negative information. However, there is no efficient mechanism for organizational and legal regulation of information. Governmental actions fail to address the issue; "in some cases, legal means are either far behind the IT controls or not applicable at all." [19] In other cases, such regulations breach a multitude of constitutional rights. Besides, not all the relations that exist in cyberspace can be handled by law enforcement.

Attempts to curb the dissemination of extremist and terrorist materials in general and among the minors must be systemic in nature; only that will prevent negative information from affecting the society. A system designed to prevent the publication of harmful information on the Internet cannot solely use penalties or other types of punishment; it should also propagate counter-terrorism. As noted by the UN Secretary General, the Internet can also be harnessed as a powerful tool in counterterrorism to draw attention to the plight of victims, to tie communities and educational institutions in different countries, to collect and exchange information on suspected terrorists [20]. Effort should be taken to diminish the negative impact of cyberspace upon the society; to channel the energy of potential terrorists' aggression and their supporters to personal enhancement; to seed confusion and disunity among terrorist supporters. Counter-terrorism propaganda might be extremely efficient if joined by social media and major search engines.

5. Conclusions

Global cyberspace is an efficient tool that gives access to the knowledge and resources humanity has collected so far. ICT advances at a rate far beyond that of creating organizational and legals means to regulate the cyberspace. This enables extremist and terrorist cells to better organize themselves, to collect the data they need, and to be in touch with the target audience while remaining virtually immune to governmental intervention.

Action to combat extremists and terrorists on the Internet, where they seek to engage minors, shouldn't be reactive-only. This problem requires attention from every public institute, from higher and secondary education to the church, from cultural institutions to mass media, etc. Government-public cooperation should produce new measures to control communications and the Internet, which will be able to:

– enable the Internet and communications to be used widely and efficiently, to become even more sophisticated and widespread;

– devise mechanisms to protect Russia's citizenry and telecommunications from extremism and terrorism while continually enforcing the constitutional rights to opinion, acquisition and dissemination of information, as well as improving personal, public, and national cybersecurity.

– promote the usage of Internet for education, science, and culture, to encourage linguistic and cultural diversity, which is largely capable of laying the sociopolitical and legal foundations for efficient counter-terrorism.

References

[1] Odhiambo N A, Ochara N M, Kadymatimba A 2018 Structuring of the Terrorism Problem in the Digital Age: A Systems Perspective Conference Paper Conference: 2018 Open Innovations (OI) pp 148-154

[2] Bogdanoski M 2018 The Nexus Between Cyberspace and Modern Terrorism (Book Chapter) Countering Terrorist Activities in Cyberspace pp 44-54

[3] Grove N S 2019 Weapons of mass participation: Social media, violence entrepreneurs, and the politics of crowdfunding for war *European Journal of International Relations* **25(1)** pp 86-107

[4] Huszti-Orban K 2018 Internet intermediaries and counter-terrorism: Between self-regulation and outsourcing law enforcement *International Conference on Cyber Conflict, CYCON* pp 227-243

[5] Liaropoulos A N 2018 Reconceptualizing cyber security: Safeguarding human rights in the era of cyber surveillance *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* pp 16-26

[6] Espinosa M J C 2012 Privacy (Book Chapter) The Oxford Handbook of Comparative Constitutional Law 1424 p

[7] Buraeva L A 2017 Radicalism and online recruiting on the Internet Socio-political sciences 4 pp 149-151

[8] Deshina E I, Merkulova A N 2019 Youth as the most exposed to the influence of extremism and terrorism on the Internet socially demographic group *Overview of the National Center for Information Counteraction to Terrorism and Extremism in the educational environment and the Internet* **1(16)** pp 54-61

[9] Nardina O V 2008 Counterterrorism in the Russian Federation: the formation of ideological and moral immunity from violence *Ekonomika polprivrede* **5-6** pp 22-27

[10] Reports on the activities of the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies and Mass Communications for 2018 http://www.rkn.gov.ru/plan/

[11] Kozlyuk A 2015 State regulation of the Network in Russia: from the Internet to the Middle Ages http://rublacklist.net/13040/

[12] 2016 The prosecutor's office of the city of Saratov conducted an audit of compliance with legislation in the field of combating extremism in Saratov: a case was instituted regarding the

lack of content filters on buses http://www.sarprok.ru/node/44461

[13] 2017 In Berezovsky, following a prosecutor's audit, a social service institution was fined for not taking measures to protect children from harmful information http://prokurat-so.ru/berezovskom-po-itogam-prokurorskoy-proverki-13545

[14] The bill of February 26 2019 No 654417-7 "On amendments to Art. 6.17 of the Code of the Russian Federation on administrative offenses (in order to strengthen administrative responsibility for offenses in the field of child safety in the information and telecommunication network "Internet") https://sozd.duma.gov.ru/bill/654417-7

[15] 2016 Donald Duck - anti-fascist came under the hand https://www.sova-center.ru/misuse/news/persecution/2015/09/d32717/

[16] Yudina N Anti-extremism in virtual Russia in 2017-2018 https://zona.media/article/2016/28/06/sova-center#sdendnote1sym

[17] Bill of May 16 2019 710629-7 "On Amendments to the Federal Law" On Basic Guarantees of the Rights of the Child in the Russian Federation "regarding the creation of additional security guarantees in the field of organizing recreation and health of children" https://sozd.duma.gov.ru/bill/710629-7

[18] Sundiev I Yu 2014 the use of information networks in extremist and terrorist activities *Scientific portal of the Ministry of Internal Affairs of Russia* **1(25)** pp 84-91

[19] Starovoitov A 2006 Law and information technology Comparative Constitutional Review **1(54)** pp 94-95

[20] Report of the UN Secretary-General of April 27 2006 A 60/825 "Unity in the fight against terrorism: recommendations for a global counter-terrorism strategy" https://www.un.org/ru/ga/documents/gakey. shtml