

Information Security of Digital Communication: How to Stay Safe?

Vladimir D. Nikishin^a and Elena I. Galyashina^b

Department of Forensic Expertise, Kutafin Moscow State Law University, Sadovaya-Kudrinskaya Str., 9, Moscow, Russia

Keywords: Information Security, Information Law, Worldview Security, Cyber Threats, Ugc, Web 2.0, Big Data, Information Bubble, Destructive Content, Terrorism, Extremism, Hate Speech, Nazism, Columbine, School Shooting, Neo-Paganism, Prison Subculture, Cyberbullying, Suicide, Self-Harm, Sexting, Cyber Grooming, Fake News.

Abstract: The article is devoted to legal, forensic and organisational problems of information security of digital communication. The authors characterise the main Internet features that contribute to the spread of destructive content online: network externality, user-generated content, filter bubbles, 'tunnel' of virtual reality, Internet determinism etc. The study was based on the hypothesis that virus-like, massive dissemination of destructive information in the Internet environment, for the users of which the main criterion for the truth of information becomes its virality, creates a real threat to the information security of Internet users. The research was interdisciplinary and included both direct monitoring of Russian speaking segment of social networks (mainly VKontakte) for destructive propaganda, and analysis of other empirical materials: court decisions, expert opinions, media materials, statistics from government bodies and non-governmental organizations, Russian and foreign legislation, etc. The article covers the following cyber threats to information (worldview) security: propaganda of terrorism and extremism, including Nazism, Columbine (school shooting), radical 'neo-paganism'; prison subculture propaganda; cyberbullying; propaganda of suicide, self-harm and other autodestructive ideas; advertisement of cyber communities that create a negative image of motherhood and childhood, conduct pro-abortion and child-free campaigns; sexting; cyber grooming; fake news etc.

1 INTRODUCTION

The digital environment is favourable for the massive, virus-like dissemination of radical propaganda, defamatory, fake and other destructive information.


This is largely facilitated by the spread of the two fundamental mechanisms of 'Web 2.0':


- network externality – the effect that each participant of the network has on changing the value of the entire system;
- user-generated content (UGC) – content (information material) created by users of a product or service and posted in the public domain (social networks, online platforms, etc.) (Gurov, 2019; Chubina, 2020).

These mechanisms, together with the use of algorithms for processing big data, cause informational 'web determinism' ('filter bubbles':

the user's past clicks determine his/her future clicks), i.e. they ensure the formation of an 'information bubble' of an Internet user, modify his/her 'tunnel' of virtual reality. The Internet user gets only those information flows that correspond to his/her previously expressed interest and do not give alternative assessments and opinions. All of this creates the ground for the implementation of propaganda activities, including radical campaigns (Nikishin, 2020).

The Internet has become a global communication platform that has contributed to the development of the network phenomenon of echo chambers (Sunstein 2001a; Potseluev, Podshibiakina, 2018). Internet users, regardless of their territorial affiliation, unite into virtual communities, communicate and become even more consolidated in their ideological attitudes, and everything that is not consistent with the values of these communities is ignored without any criticism, i.e. the mechanism of the so-called 'group

^a  <https://orcid.org/0000-0003-2819-8517>

^b  <https://orcid.org/0000-0001-8989-1003>

polarization', about which K. Sunstein wrote, is launched (Sunstein 2007).

According to Canadian professor W. McKay, cyberspace can be compared to a large uncontrolled public playground where unscrupulous participants can harass, intimidate and defame others, causing emotional and psychological stress with relative impunity (MacKay, 2012). As F.N. Gurov remarked, 'in the information era, an individual becomes an object of manipulation in order to provide the "customer" with the necessary user behavior' (Gurov, 2019).

Virus-like, massive dissemination of destructive information in the Internet environment, for the users of which the main criterion for the truth of information becomes its virality (i.e. the very fact of its widespread distribution), creates a real threat to the information security of World Wide Web users. Information attacks in Internet media transform the 'tunnel' of the user's virtual reality imposing the content that will attract users' attention (based on an algorithmic analysis of their behavior in the Internet, including the history of web pages). The danger is that such information attacks are used not only for marketing and advertising purposes but also for criminogenic purposes violating the information security of a person. The 'modified' tunnel of reality (representing a narrow spectrum of ideas about reality inside an algorithmically generated virtual reality) supplemented by harmful (destructive) information 'endows' this criminogenic information with the property of virality, i.e. this information begins to spread on the Web on its own, with the help of ordinary users and attracting new 'adepts' in a virus-like manner.

In the context of informational 'Internet determinism', when the user's past clicks determine their future clicks, the user is actually limited by the information presented to him/her on the basis of algorithms within the tunnel of reality. The user does not see an alternative analysis of situations and opinions, all of which creates favorable conditions for the determination of his/her worldview and radicalization of consciousness (Nikishin, 2020).

2 METHODOLOGY OF RESEARCH

The study was interdisciplinary and included both direct monitoring of social networks (mainly VKontakte) for destructive propaganda, and analysis of other empirical materials: court decisions, expert

opinions, media materials, statistics from government bodies and non-governmental organizations, Russian and foreign legislation, etc.

The analysis of foreign legislation (Golovanova, 2019; Filippov et al., 2019; Golovanova, 2018) demonstrates that most democratic states are following the path of toughening (introducing) legal responsibility for destructive speech behavior in the network, thus limiting freedom of speech in order to protect other benefits. The tragic events of 2019 in California (USA), Texas (USA), Christchurch (New Zealand), Ohio (USA), etc. forced the United States and New Zealand authorities to issue calls for drastic measures to restrict Internet freedom in order to limit the spread of propaganda of extremism and other forms of violence (Amelina, 2019).

According to the Safe Internet League, 43 million social media accounts are influenced by destructive content, 8.2 million accounts belong to teenagers (<http://ligainternet.ru/>). Monitoring showed that a wide network of destructive communities has formed in cyberspace (primarily in social networks), which is used for a massive attack on the worldview of users: depressive and (auto)aggressive content imposes certain behavioral patterns associated with violence on users. As the researchers note, the purpose of such information resources is to force Internet users 'to commit suicidal or aggressive (criminal) actions, which may or may not be attributed to socio-political, religious or other motivation' (Amelina, 2018).

Monitoring of VKontakte demonstrates that the 'contingent' of depressive and (auto)aggressive communities often overlap, the members of such communities do not have an established worldview; the ideology of a particular community is nothing more than the idea of violence for the sake of violence: The same web users can be members of ISIS (an organization banned in the Russian Federation), Columbiners, 'AUE' (prison subculture), Nazi groups and suicidal communities. The analysis of personal profiles and timeline posts on 'VKontakte' demonstrates how the preferences of adherents of the cult of violence have changed over time. The ideas of the struggle for Donbass are replaced by Islamist ideas, interchanging with the ideas of 'neo-paganism', school shootings, etc.

Many destructive communities also do not have 'ideological severity', for example, there are alternating posts of Probanderists (Bandera supporters), 'neo-pagans', adherents of the 'Caucasus Emirate' (an organization banned in the Russian Federation), stories about serial murders, etc. in the 'Time to hate' community (Amelina, 2018).

The story of A. Konev ('Khabarovsk shooter' who was killed during the attack on the Federal Security Service reception room) demonstrates the unity of neo-Nazis, politicized neo-pagans, religious fanatics and suicidal groups' views on the forms and methods of struggle for the capture of political power in the country. As in the case of the 'Khabarovsk shooter', a movement praising the so called 'cleaners' has grown on VKontakte (In 2017, a gang of young people was convicted of murdering street sleepers. 'Cleaners' were found guilty of murdering 14 people).

The social network VKontakte stores the content of communities under the general name 'Murderer's Logic' (and similar names) numbering thousands of subscribers and aimed at promoting mass murders. Some of these communities continue to be updated daily with new posts. There are also communities broadcasting the ideas of a bloody sexual violence, murder of sexual partners and parasuicidal ideas (see, e.g., the community 'Hate' with about 1500 subscribers – URL: <https://vk.com/h6a6t6e>).

There is the publicly available content of communities that do not openly call for violence but actively promote its cruelty and violence through various memes such as 'Reasons to kill' as well as stories of 'real' murders. Such communities have an audience of 1,500 to 350,000 or more subscribers (see, e.g.: 'World of Maniacs and Serial Killers' – URL: <https://vk.com/mandsm>); '1000 Reasons to Become a Killer' – URL: <https://vk.com/bykpuxo>); 'Serial Killer's World' – URL: https://vk.com/skillers_world), so there is a need to search for an organizational and legal model of counteracting the spread of this kind of destructive information.

It should be noted that a lot of VKontakte communities of the Columbine discourse were banned after the events of 02/03/2014 (Otradnoye), 09/05/2016 (Ivanteevka), 01/15/2018 (Perm) and the tragedy in Ulan-Ude (01/19/2018). At the same time, many 'Columbine' communities, the titles of which do not directly mention 'Columbine', continue to be open for public access. Some groups that justify and praise the Columbine assassins have changed their privacy settings to the 'private' mode.

In addition, the audience of such communities is actively moving to Telegram due to the aforementioned ban, while links to telegram channels are available on VKontakte.

Columbine propaganda in the digital environment and the threat of a repetition of the Columbine scenario are confirmed by the following facts. Firstly, despite the ban of Columbine communities on

VKontakte after the tragedy in Ulan-Ude, there were at least 4 more tragedies with a similar scenario: 03/21/2018 in Shadrinsk, 04/18/2018 in Sterlitamak, 10/17/2018 in Kerch, 05/28/2019 in Volsk (Saratov region). Secondly, during 2020, a number of attempts to repeat the 'Columbine' scenario were identified not only in schools. In the fall of 2020, journalists stated that the Russian regions were overwhelmed by the Columbine movement, and 13 teenagers, who lived in different regions of the Russian Federation but were part of the same closed Internet community, were detained on September 1. In August 2020, the Security 2.0 Center, operating under the Russian Peace Foundation, identified several thousand videos on TikTok, in which terrorist attacks in schools were justified. Videos tagged with the hashtag #columbine have over 3.5 million views on TikTok.

A dangerous tendency is the gradual change of the place of committing crimes from schools and other educational institutions to other places of mass gathering of citizens not related to the organization of the educational process (crowded stops of public transport, shopping centers, markets, etc.).

Another destructive trend in the digital communication environment is the advertisement of groups that create a negative image of motherhood and childhood, conduct pro-abortion and child-free campaigns, remove the moral barrier to the use of violence against children. In addition, there has been a significant increase in the number of videos about child sexual abuse distributed on the Internet (increased by 541% in 2019 (Amelina, 2019)).

The number of victims of cyberbullying increased in 2020 due to the pandemic, a total transition to digital communication, and increased emotional tension in conditions of isolation. The urgency of countering cyberbullying is growing every year, therefore, the legal models of countering this phenomenon require further studies.

Longitudinal study of the content of 'suicidal social media communities' and personal profiles of users who committed suicides demonstrates a formed 'suicidal cult' characterized by the ideology of devaluation of life, propaganda of the meaninglessness of human existence, devaluation of values such as love, friendship, family (Bychkova and Radnaeva, 2018).

In 2017, VKontakte began to ban the use of words with hashtags promoting a 'suicidal quest'. Delinquents reacted to this by posting truncated hashtags and switching to Instagram and Telegram.

Another threat to the information security of an individual in the digital environment is sexting, which means the exchange of intimate content or messages

leading to threats, blackmail, bullying and even involvement in child pornography.

One of the threats to the informational security of minors is cyber grooming, that is the establishment of friendly relations and emotional connection with a child or adolescent in order to gain his/her trust for the purpose of sexual exploitation. In addition, according to researchers from the UK (Hoyle et al. 2015; Edwards, 2017.), cyber grooming was actively used to recruit girls in the so-called Islamic state (an organization banned in the Russian Federation).

Another tool of informational influence on the worldview of Internet users is fake news (although it is not a new phenomenon, it has reached unprecedented proportions due to new media (Galyashina and Nikishin, 2020). The Safe Internet League systematically registers the spread of fake news in Russia.

Fake news acts as a tool for manipulating the minds of Internet users and requires the development of organizational and legal mechanisms for filtering Internet content for fakes. It is worth noting that the self-regulation mechanisms proposed, for example, by Facebook raise concerns due to the already manifested politicization of the Facebook leadership.

3 DISCUSSION OF RESEARCH RESULTS

Based on the results of the study, we found that the most widespread destructive content in the Russian-speaking segment of the Internet is associated with the following information (worldview) security threats:

- propaganda of cult of cruelty and violence;
- popularization of extremist-terrorist ideology, especially Columbine-subculture (school shooting);
- humiliation of human dignity and discrimination on the basis of language, nationality, sex, religion and other socio-biographical grounds or grounds of physical disabilities;
- romanticizing of the underground culture (including prison culture);
- glorification of murderers;
- popularization of suicidal and other self-destructive behaviour, cybersuicide;
- cyberbullying, cyberbullicide;
- fake news.

In the Strategy for the Development of the Information Society in the Russian Federation for

2017 – 2030 (Ukaz Prezidenta RF ot 9 maia 2017 g. N 203), among the priorities in ensuring national interests, the primary importance is given to the formation of an 'information space, taking into account the *needs of citizens and society in obtaining high-quality and reliable information*' (p. 22). The goals of the formation of the information space of knowledge are defined as 'ensuring the *rights of citizens to objective, reliable, safe information* and creating conditions for meeting their needs for continuous development, obtaining *high-quality and reliable information*, new competencies, expanding horizons' (p. 24).

Thus, the information security of an individual is an integral part of the information security of the Russian Federation and can be considered in two aspects:

- as the security of the information itself (personal data, personal, state, commercial or family secrets, etc.) and
- as protection from (destructive) information.

Worldview cybersecurity is not reducible to any of these aspects. It covers, first of all, the second aspect and means the protection from information that destructively affects the worldview of an individual, his/her psychological and mental state, but also, partially coincides with the first aspect, since the dissemination of information constituting a personal or family secret may serve as a cause for bullying a person and even driving him/her to suicide (cyberbullicide).

It is traditionally accepted that integral components of personal security are such universal values as life, health, and freedom. They are subject to protection not only in the real (physical) but also in virtual (cyberspace) world. Life and health are under threat due to the dissemination of ideas of unmotivated violence, Satanism, mass murder and suicide, other self-destructive behaviour (self-harm, etc.), i.e. web users influenced by such ideas are ready to implement violence against themselves or others in the real (physical) world. In addition, it should be highlighted that the dissemination of such destructive propaganda affects the mental health of web users. Such values as honour, dignity, good name, business reputation, in conditions of freedom and anonymity of Internet communication are being marginalized. Defamation, insults, slander, bullying, outing have become integral attributes of modern web communication.

In today's new realities, the idea that the Internet is a space of absolute freedom and permissiveness has fewer and fewer supporters. Digital transformation influences all spheres of life and eradicates the

boundaries between the virtual world and the real world. The idea of 'electronic democracy' seems achievable. In 2001, K. Sunstein pointed out that the echo chamber effect makes cyberspace difficult to be compatible with the democratic communicative order (Sunstein, 2001b). Thus, informational relations that are being developed in cyber reality are subject to clear legal regulation, taking into account their nature, non-equivalence to 'real' relations.

4 CONCLUSIONS

In this article, the most widespread threats to the information (worldview) security of the Russian-speaking segment of Internet users were summarized and characterized. There are several recommendations aimed at improving the protection of information security:

- When considering the issue of improving Russian legislation regarding countering sexting, it is necessary to take into account the experience of foreign lawmakers who are paying special attention to sexting among minors (including the experience of Australia, the USA, Canada).
- Consideration should be given to criminalizing cyber grooming taking into account the legislative experience of the UK and Australia (the UK Sexual Offenses Act and the Australian Queensland Criminal Code).
- Information security also requires the development of legal and organizational (including forensic) models and methods to counter such phenomena of modern digital communication as cyberflashing (unsolicited sending of images or videos of the genitals), revenge porn (disclosure of intimate photos or videos without the consent of the person depicted in order to cause him/her anxiety or suffering), etc.
- Systemic changes to the Federal Law 'On Information, Information Technologies and Information Protection' dated July 27, 2006 N 149-FZ, the Federal Law 'On the Protection of Children from Information Harmful to Their Health and Development' dated December 29, 2010 N 436-FZ are required to expand and specify the types of information prohibited or restricted in distribution due to the emergence of new destructive trends in the digital environment. In addition, it is necessary to unify the categorical apparatus of these federal laws with the Criminal Code of the Russian

Federation and the Code of Administrative Offenses of the Russian Federation.

- Consideration should be given to the possibility of strengthening the institution of self-regulation in information relations in the Internet environment. It is required to tighten the responsibility of the administrations of social networks for failing to take measures to counter the dissemination of destructive content.

In addition, it is necessary to develop organizational (including forensic) and legal models and methods for countering destructive propaganda and recruiting activities not only on the Internet but also in networks such as Darknet, VPN, Tor, I2P, Freenet.

ACKNOWLEDGEMENTS

The reported study was funded by RFBR, project number 20-011-00190.

REFERENCES

- Gurov, F. N. (2019). Informatizatsiia obshchestva i transformatsiia subekta kommunikativnykh praktik. *Gumanitarnyi vestnik*, 4: 1–16. https://gurovpr.ru/netcat_files/userfiles/gurov-article2.pdf
- Chubina, E. A. (2020). Professionalnaia deiatelnost eksperta glazami sovremennykh media. *Vestnik kriminalistiki*, 3(75): 105.
- Nikishin, V. D. (2020). Tsifrovye i rechevye sledy v aspekte obespecheniia informatsionnoi (mirovozzrencheskoi) bezopasnosti v internet-srede. *Sudebnaia ekspertiza*, 1(61): 131–139.
- Sunstein, C. R. (2001). *Echo chambers*. Princeton: Princeton University Press.
- Potseluev, S. P. and Podshibiakina, T. A. (2018). O faktorakh politicheskoi radikalizatsii v setevoi kommunikatsii posredstvom «ekhhokamer». *Nauchnaia mysl kavkaza*. 2(94): 29–33.
- Sunstein, C. R., 2007. *Republic.com 2*. Princeton–Oxford: Princeton University Press.
- MacKay, W. (2012). Respectful and Responsible Relationships: There's No App for That. *The Report of the Nova Scotia Task Force on Bullying and Cyberbullying*. February 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2123494&download=yes
- Golovanova, N. A. (2019). Novye formy onlain-prestupnosti za rubezhom. *Zhurnal zarubezhnogo zakonodatelstva i sravnitel'nogo pravovedeniia*. 3: 42–57.

- Filippov, V. M., Bukalero, L. A., Ostroushko, A. V. and Karpukhin D. V. (2019). *Pravovye mery protivodeistviia vrednomu informatsionnomu vozdeistviu na nesovershennoletnikh v informatsionno-telekommunikatsionnykh setiakh: monografiia*. Moscow: RUDN Publ.
- Golovanova, N. A. (2018). Problemy borby s bullingom: zakonodatelnoe reshenie. *Zhurnal rossiiskogo prava*, 8(260): 113–123.
- Amelina, Ia. A. (2019). Benefis nenavisti. Kak «kolumbainery» i kerchenskii ubiitsa Vladislav Rosliakov stali «geroiami» rossiiskoi destruktivnoi molodezhi (18+). In *Kavkazskii geopoliticheskii klub*. pages 6–7. Moscow: Izdatel Vorobev A.V. Publ.
- Amelina, Ia. A. (2018). Transformatsiia destruktivnykh praktik posle razgroma t.n. «Islamskogo gosudarstva»: poslednie tendentsii. «Kolumbain» v rossiiskikh shkolakh – dalee vezde?.. (18+). In *Kavkazskii geopoliticheskii klub*. page 23. Moscow: Izdatel Vorobev A.V. Publ.
- Bychkova, A. M. and Radnaeva, E. L. (2018). Dovedenie do samoubiistva posredstvom ispolzovaniia internet-tekhnologii: sotsialno-psikhologicheskie, kriminologicheskie i ugovno-pravovye aspekty. *Vserossiiskii kriminologicheskii zhurnal*. 1: 101 – 115.
- Hoyle, C., Bradford, A., and Frenett R. (2015). Becoming Mulan? Female Western Migrants to ISIS. Report of the Institute for Strategic Dialogue. Available at: <http://www.strategicdialogue.org/>
- Edwards, S. (2017). Cyber-Grooming Young Women for Terrorist Activity: Dominant and Subjugated Explanatory Narratives. In Viano E. (eds) *Cybercrime, Organized Crime, and Societal Responses*, pages 23 – 46. Springer.
- Galyashina, E. and Nikishin, V. (2020). Media security of megascience projects: legal experts training. In J. Phys.: Conf. Ser.1685 012004 doi:10.1088/1742-6596/1685/1/012004.
- Ukaz Prezidenta RF ot 9 maia 2017 g. N 203 «O strategii razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017 - 2030 gody». SPS Garant.
- Sunstein, C.R. (2001). *Republic.com*. Princeton: Princeton University Press.