RELAÇÕES INTERNACIONAIS NO MUNDO ATUAL

CENTRO UNIVERSITÁRIO CURITIBA - UNICURITIBA - VOLUME 2 - NÚMERO 3/2021 CURITIBA/PARANÁ/BRASIL - PÁGINAS 01 A 16 - ISSN: 2316-2880

CYBERSTALKING AS A TYPE OF CYBERCRIME: COUNTERACTION OPPORTUNITIES IN RUSSIAN AND INTERNATIONAL LEGISLATION

CYBERSTALKING COMO TIPO DE CIBERCRIME: OPORTUNIDADES DE CONTRATAÇÃO NA LEGISLAÇÃO RUSSA E INTERNACIONAL

VITALII F. VASYUKOV
Associate Professor, Doctor of Law
Moscow State Institute of international relations (University) - Russia
Orel Law Institute of the Ministry of Internal
Affairs of Russia named after V.V. Lukyanov - Russia
https://orcid.org/0000-0003-0743-5616

ALEKSANDR VLADIMIROVICH BOCHAROV
Candidate of Legal Sciences, Associate Professor
Russian State University of Tourism and Service - Russia
https://orcid.org/0000-0001-7950-6052

EVGENIIA KASHINA
Deputy Development Director, ZAO “Promtechset’” - Russia
Lomonosov Moscow State University - Russia
https://orcid.org/0000-0002-6017-1069

DMITRIY ALEKSANDROVICH SINGILEVICH
International Law Institute, Moscow - Russia
https://orcid.org/0000-0002-2454-6898

RESUMO

Antecedentes: A Internet é caracterizada por um rápido crescimento, pois contribui para o progresso em quase todos os aspectos da sociedade e está disponível em quase todos os cantos do globo. Muitos recursos da tecnologia da Internet – baixo custo, facilidade de uso e anonimato – a tornam um ambiente atraente para fraudes, exploração sexual de crianças e um problema cada vez mais novo conhecido como cyberstalking ("assédio cibernético").

Objetivo: O objetivo do artigo é analisar as possibilidades de combate ao cyberstalking na legislação russa e internacional.

Resultados: Este artigo enfoca os principais aspectos do cyberstalking e esclarece o conceito e a essência do cyberstalking, define as etapas de preparação do cyberstalking e possíveis cenários de um ataque do cyberstalker, analisa as possibilidades de combate ao cyberstalking na legislação russa e internacional.

Revista Relações Internacionais do Mundo Atual Unicuritiba.
[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

Conclusão: Concluiu-se que o problema do cyberstalking é agravado no maior desenvolvimento ativo das redes informáticas e na integração ativa da tecnologia informática na vida pública e privada, o que exige a modernização da legislação no domínio da segurança da informação e dos dados pessoais, resultando numa necessidade de mais pesquisas sobre o tema visando o aprimoramento e desenvolvimento da legislação nacional, a criação de softwares especiais para a proteção dos direitos humanos e suporte metodológico adequado para a esfera do combate ao cibercrime.

Palavras-chave: assédio; vítima; cyberstalking; cibercrime; ataque de cyberstalker; chantagem; pressão; cyberbullying.

ABSTRACT

Background: The Internet is characterized by rapid growth, as it contributes to progress in almost all aspects of society and is available in almost all corners of the globe. Many features of Internet technology – low cost, ease of use, and anonymity – make it an attractive environment for fraud, sexual exploitation of children, and an increasingly new problem known as cyberstalking ("cyber harassment").

Objective: The purpose of the article is to analyze the possibilities of countering cyberstalking in Russian and international legislation.

Results: This article focuses on the main aspects of cyberstalking, and clarifies the concept and essence of cyberstalking, defines the stages of preparation of cyberstalking and possible scenarios of a cyberstalker attack, analyzes the possibilities of countering cyberstalking in Russian and international legislation.

Conclusion: It has been concluded that the problem of cyberstalking is exacerbated in further active development of computer networks and the active integration of computer technology in public and private life, which requires modernization legislation in the field of information security and personal data, resulting in a need for further research on the subject aimed at the improvement and development of national legislation, the creation of special software for the protection of human rights and appropriate methodological support for the sphere of combating cybercrime.

Keywords: harassment; victim; cyberstalking; cybercrime; cyberstalker attack; blackmail; pressure; cyberbullying.

1 INTRODUCTION

The Internet has generated a huge amount of anonymous online activity, both positive and negative (Savina, Tsvetkova, Galimova, Avezov, & Nazarov, 2020). On the

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

one hand, Internet anonymity promotes the open exchange of ideas and creative expression; on the other hand, it protects inappropriate and illegal behavior, such as cyberstalking, defamation, and copyright violations (Alexy, Burgess, & Baker, 2005; Zelenkov, Fedyakin, Zinkovsky, Nikitina, & Bikov, 2021).

Cyberstalking (cyber harassment) is increasingly recognized as a serious and widespread crime with the ubiquity of Internet-enabled devices and social networks. For example, an online survey of young people (from 10 to 15 years old) (Ybarra & Mitchell, 2008) showed that 15% were subjected to unwanted sexual harassment on the Internet, and 33% were subjected to online harassment. A survey of adult Internet users showed that 40% experienced various types of online harassment, including cyberstalking (Finn, 2004). Several other studies that have examined cyberstalking indicate that this is a widespread type of online offense (Baum, Catalano, & Rand, 2009).

Thus, the probability of cybercrime, especially cyberstalking, tends to increase. Indeed, existing trends and data indicate that cyberstalking is a serious problem, the scale, and complexity of which will grow as more and more people take advantage of the Internet and other telecommunications technologies.

Literature review

Harassment in general terms can be attributed to repeated acts directed against the victim, such as following the victim, making annoying phone calls, killing the victim's pet, vandalizing the victim's property, leaving written messages or objects (Cattaneo, Cho, & Botuck, 2011). Harassment can be accompanied by serious violent actions, such as physical harm to the victim, and this should be taken seriously. It all depends on how the pursuer behaves (Spitzberg, 2002).

The concept and essence of cyberstalking are described in various studies. The authors consider it necessary to cite some of them, reflecting the qualitative features in the approach to cyberstalking (Table 1).

Table 1. The concept and essence of cyberstalking

No.	Definitions	Source

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

1	obsessive harassment on the Internet by one person or a group of persons that carries a potential threat to the psychological, physical, or material condition of the victim	M.L. Pittaro (2007)
2	the use of electronic means of communication, including pagers, mobile phones, e-mail, and the Internet, to intimidate, threaten and harass the victim	L. McFarlane and P. Bocij (2003)
3	a type of offense in the information sphere that involves the harassment of a person on the network with aggressive or sexual overtones, the dissemination of false accusations on the Internet, gossip and slander	B. Spitzberg & G. Hoobler (2002)
4	refers to harassment activities carried out in "cyberspace" using information and communication technologies	N. Al-Mutawa, J. Bryce, V. N. L. Franqueira, & A. Marrington (2016)
5	repeated acts of harassment or threatening behavior of a cybercriminal towards a victim using Internet services	B.W. Reyns, B. Henson, & B.S. Fisher (2011)

Cyberstalking became possible due to the emergence and development of several factors, namely: digital technologies, computer networks, social networks (Bocij, 2005), and separate science-social engineering (Wykes, 2007). Cyberstalking manifests itself not only in the unauthorized use of personal data to smirch the honor of the victim or steal property (Bocij, Griffiths, & McFarlane, 2002) but also in psychological pressure, which implies contact with the pursuer (Beran & Li, 2005).

A cyberstalker is someone who uses the Internet as a kind of weapon or tool to hunt, stalk, threaten and cause fear and awe in their victims through sophisticated stalking tactics (Dennison & Thomson, 2002). Cyberstalkers can be both individuals and a group of those who do it for fun, but it is easy to perform certain actions when there is the necessary initial data (van der Aa, 2011).

Cyberstalking may include, but is not limited to, the transmission of threats and false accusations, damage to data or equipment, identity theft, data theft, computer monitoring, as well as harassment, including to minors, for sexual purposes and any form of aggression (Barak, 2005). Therewith, the "online harassment" and "cyberstalking"

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

terms are often used interchangeably (Southworth, Finn, Dawson, Fraser, & Tucker, 2007).

There is a similar type of cybercrime – cyberbullying, but these are completely different methods of influencing the victim and interacting with her. These two types of offenses are united by the use of the same hardware and software, such as a messenger, a social network, there is also a victim and an attacker (Henso, Reyns, & Fisher, 2011). Nature and the ultimate goal are quite different. If cyberstalking is a systematic, moral, and psychological pressure on the victim to obtain a certain result, then cyberbullying is harassment to meet certain moral and psychological needs of the attacker (Bocij & McFarlane, 2002; Lyndon, Bonds-Raacke, & Cratty, 2011).

Research hypothesis: the problem of cyberstalking is becoming more acute in the conditions of further active development of computer networks and active integration of computer technologies into public and private life, which requires the modernization of legislation in the field of information and personal data protection.

Research objectives:

1. to determine the stages of preparation for cyberstalking and possible scenarios of a cyberstalker attack based on an expert survey;

2. to analyze the possibilities of countering cyberstalking in Russian and international legislation.

The article consists of an introduction, a literature review, methods, results, discussion, and conclusion.

2 METHODS

2.1 RESEARCH DESIGN

A mixed type of research design was used to prove the hypothesis based on a combination of requirements for data collection and analysis necessary for the

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

implementation of the research goal. Therefore, the following methods were chosen to obtain information:

- analysis of legislation, scientific and legal literature using methods of analysis, synthesis, comparison, and generalization – to study the state of the research problem;

- the expert survey method was used to determine the stages of cyberstalking preparation, as well as possible scenarios of a cyberstalker attack.

- ranking method – to determine the rank of a possible cyberstalker attack scenario.

The procedure, research tools

The sources of information necessary for the implementation of the research goal were selected at the first stage of the research: legislative acts; articles published in journals indexed by Scopus and Web of Science (20 sources), collective monographs (2 sources) containing information regarding cyberstalking as a type of cybercrime.

At the second stage of the study, based on an expert survey in the video conference mode (Skype), the stages of cyberstalking preparation, possible scenarios of a cyberstalker attack, as well as the possibilities of countering cyberstalking in Russian and international legislation have been determined. The criteria for selecting experts (20 people) were the presence of articles on this topic published in journals included in the Scopus or Web of Science citation databases in the amount of at least 3 or at least 12 years of experience in law enforcement agencies.

At the third stage of the study, the analysis of the collected information was carried out, with the interpretation of the results obtained.

Statistical analysis

The study used numerical calculation methods using the Microsoft Excel software product, which was used to calculate the percentage of expert mentions of possible cyberstalker attack scenarios.

3 RESULTS

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

Experts argue that it is necessary to go through several stages of preparing an offense to commit cyberstalking (Table 2).

Table 2. Stages of cyberstalking preparation

No.	Stage	Characteristics
1	Choosing a victim	Provided that the victim is already familiar, this stage moves on to the next one. If the victim is not familiar, it is selected from social networks according to a certain criterion, which has already been determined by the cyberstalker
2	Exploration stage	All information that can be obtained from social networks is collected and classified: email address, other contact information, place of residence, contacts in social networks, the degree of relationships, the role in relationships. The greatest priority is given to relatives and those with whom a person interacts constantly, the place of work, and information about hobbies. Information about the financial situation is collected
3	Tracking stage	The main tracking is carried out in social networks. The scope of interests includes personal data, private life, frequently visited places, movable property, information about account numbers and banks whose client is the victim, etc.
4	Quiet (deep) pursuit	A social network profile and an electronic mailbox are being hacked. Access to the victim's card and current accounts, if such an action exists in the cyberstalker plan
5	Active phase	The beginning of a cyberstalker attack on the victim. Receiving the first threats.

Note: compiled based on the expert survey

According to the results of the expert survey, the mechanism of a cyberstalker attack is possible in several scenarios (Table 3).

Table 3. Cyberstalker attack scenarios.

No.	Mechanism	%*	Rank
1	Interaction directly with the victim for blackmail		1
2	Interaction directly with the victim to gain control over the victim's social life in a computer network		2
3	Hard pressure of the victim		3
4	Using the contact information of the social network		4
5	Interaction with real-life acquaintances		5
6	Mass pressure		6

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

Note: compiled based on the expert survey; * – percentage of expert mentions

4 DISCUSSION

Let us take a closer look at the cyberstalker attack scenarios presented by experts (Table 3).

Interaction directly with the victim for blackmail is carried out when the victim begins to be blackmailed and forced to commit certain actions, or to obtain certain benefits, both material and non-material, for himself/herself or a third person. The result is achieved by threats to publish certain personal information about the victim, thanks to which the latter will be in a vulnerable position, especially young people with weak psychological stability and aged 16-20 years suffer from this (Vinichenko, Rybakova, Chulanova, & Makushkin, 2020). The tools of such interaction are threatening emails from anonymous sources, threatening emails from newly created accounts in social networks, phone calls, and SMS messages (Beran & Li, 2005). This option, according to experts, is possible provided that the cyberstalker is not sure of the victim's resilience, or there is no certain information that can be made public. This method is usually used by novice cyberstalkers because they can be quickly identified by email addresses and phone numbers (Wykes, 2007).

Interaction directly with the victim to gain control over the victim's social life in a computer network is a modified version of blackmail. This type of offense, according to experts, is carried out provided that the cyberstalker has certain technological skills, the consequence of which is, in particular, hacking a profile in social networks, anonymous calls, gaining control over all possible devices of the victim, and performing certain programs for intimidation. For example, printing out any phrases or "playing" with the light on a printer, provided that it is possible to get access to the smart home system (McFarlane & Bocij, 2003). The use of this option is possible to receive funds from the victim in exchange for leaving alone or to encourage certain actions.

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

The option *of hard pressure* on the victim is possible provided that the cyberstalker has a certain team of professionals in this field or has ordered the execution of certain actions to "external" professionals (Reyns et al., 2011). In this case, the information that can be made public if a certain goal is not achieved really exists. It was obtained from the victim himself/herself or in another way – from registries, data banks, or even this is information with limited access. There is a possibility that the victim has valuable information or has to do something that is of serious importance to the customer of the cyberstalker attack. Every step of a person in the digital network is tracked. Attackers will gain access and steal not only social network profiles and passwords to electronic mailboxes, but also the phase of tracking and interaction in reality begins. The victim's money disappears from his/her current accounts, the victim is delivered certain types of items, and quite often a car is stolen. Sometimes the victim's phone is hacked and outgoing calls are blocked or pursuers create a DDOS attack using SMS messages or anonymous phone calls (van der Aa, 2011).

When *using the contact information of a social network*, certain accounts spread deliberately false information designed to cause disgust to the victim. In this variant, the cyberstalker creates a large number of profiles in the social network, certain websites with fictitious information about the victim (and the payment for hosting and the name of the site is made by an anonymous method or by carding) (Spitzberg, 2002). The victim is sent their demands to social networks and e-mail to stop the intimidation campaign. In this case, as experts note, there is never any contact in the real world between the cyberstalker and the victim.

A rather cynical kind of cyberstalker is *interaction with real-life acquaintances* when the victim does not receive threats directly. Interaction directly with the victim does not occur, but only through relatives and friends, who begin to be terrorized by phone spam calls from anonymous numbers and slander the victim (Spitzberg & Hoobler, 2002). In social networks, spam messages from newly created accounts will appear on the page of each friend or relative (Lyndon et al., 2011). Sometimes, as an option, SMS spam is used

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

instead of calls. The attackers provide all the requirements in SMS messages or on the pages in social networks of all friends and relatives (McFarlane & Bocij, 2003).

Experts call *mass pressure a variant of hard pressure on the victim*, but there is a rather serious difference – absolutely all friends from social networks and real life will be under attack by a cyberstalker. The closest relatives may also lose funds from their current accounts (Bocij et al., 2002).

Unfortunately, Russian legislation still does not consider cyberstalking as a separate type of offense. There are no mechanisms for recording, confirming, and collecting evidence, as well as protecting the victim. It should be borne in mind that cyberstalking is a cybercrime, that is, a complex offense consisting of several actions that have a specific scenario and use hardware and software (Spitzberg, 2002). It should also be taken into account that certain laws have not yet been adapted to modern realities, so they do not indicate legal responsibility for committing such acts (Cattaneo et al., 2011). Therefore, it is quite difficult to determine the degree of guilt of the organizer of the act, but such a crime must be considered in parts because it is performed depending on the scenario.

The main idea of cyberstalking is interference in the life of a certain individual using a computer network to create conditions for moral, material impact, and psychological suffering of the victim.

The first state law on stalking was passed in 1990 when California passed a law making stalking a criminal offense. To date, all 50 states and the District of Columbia have enacted prosecution laws (Dennison & Thomson, 2002), with 44 states enacting cyber-stalking laws as part of existing harassment laws (2006 National Conference of State Legislatures), making it a federal offense to transmit any threatening information that is intended to harm another person. The penalty for violating the law provides for a prison sentence of up to five years and may include a fine of up to 250,000 US dollars (Dennison & Thomson, 2002).

As with federal laws, most state stalking laws require that the perpetrator directly threatens to harm the victims in any way (Pittaro, 2007). Since most state laws require a

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

direct threat to harm the victim, many criminals can avoid arrest and prosecution in the absence of a direct threat. In other words, the harassment can continue as long as the stalker does not directly threaten the victim or the victim's family with bodily harm (Southworth et al., 2007). In addition to criminal sanctions, some states allow victims to file a civil lawsuit against the harasser for harm, including defamation, libel, pain, and suffering, or loss of income (Spitzberg & Hoobler, 2002).

Researchers (Al-Mutawa et al., 2016) note that the following elements are required for the commission of a crime in American criminal law: that there is a certain behavior, the intention to cause harm, the presence of a victim. Establishing a certain behavior is not as difficult as establishing the intention to cause harm, according to which the state (the prosecution) must prove that the criminal intended to cause harm, especially if the victim and the cyberstalker were previously strangers.

The criminal legislation of the Russian Federation (State Duma of the Federal Assembly of the Russian Federation, 1996) may define these actions (cyberstalking) in cases of defamation, i.e. the Dissemination of Deliberately False Information (Article 128.1, Part 2), Extortion (Article 163).

However, if a person is not threatened to give out certain materials about him/her or is not ordered to transfer funds to stop cyberstalking, there are no requirements to perform certain actions – only harassment and a constant life in fear, then such a case is unfortunately not defined by the legislator, except if cyberstalking led to a tragic outcome for the victim – Incitement to Suicide (Article 110, part 2, paragraph "d").

There is no clear understanding in the legislation of what a DDOS attack on a communication device of a potential or real victim with the help of a large number of phone calls is (Zelenkov, 2021). At its core, such a violation as the intimidation of a person through means of communication is not defined by any law.

In the context of the development of digitalization, the concept of "personal data" and its perception, which exists in the current Russian legislation (State Duma of the Federal Assembly of the Russian Federation, 2006), is becoming increasingly "blurred" and ambiguous. Moreover, there is no clear boundary between the concepts of "personal

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

data" and "confidential information", and there is also no clear legal liability for negligent handling of personal data at all stages of working with them, collecting, processing, distributing, storing and destroying.

One of the experts (R. Vladimir, 8 years of experience in law enforcement agencies) asked a question during the discussion and answered it himself: "What kind of information about a person should be considered confidential information? If the information is taken from social networks, that is, the one that the person has personally stated, then such information is public and publicly available. If a person is persecuted by threatening to spread erotic information or by spreading information and evidence about his/her private life that he/she would like to hide, then we will get a situation that provokes criminals to cyberstalker activity". The expert cites evidence of a person's participation in a criminal offense that was not received by law enforcement officers, materials of an erotic nature, certain compromising evidence, and others as an example of information with which this person will not voluntarily turn to law enforcement agencies.

An individual who represents the injured party puts both the legislator and law enforcement officers in a losing position in advance because there is no mechanism for legal protection against criminal actions of this kind. Quite often, information is used as a product (which is also not defined in the legislation) as a means of manipulation, and there is no option to ban and seize information from the offender.

5. CONCLUSION

Modern legal problems in the field of electronic information communication are associated with the fact that technical and technological interaction with the real world is carried out through a virtual space using a certain software and hardware complex. Due to the rapid development of IT technologies and the slow development of legislation in the field of computer technologies, we have a situation where criminals act with impunity in conditions of imperfect legislation.

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

The complexity of detecting a criminal and getting help from the police, the lack of a legislative definition of the "cyberstalking" concept together with the definition of counteraction mechanisms, provides criminals with the opportunity to carry out actions that they choose according to a certain scenario with impunity. It is a large number of variations of the criminal's actions that make it impossible to determine the degree of his/her guilt, and the injured party – protection from the attacker.

Thus, the results of the study confirmed the hypothesis that the problem of cyberstalking is becoming more acute in the conditions of further active development of computer networks and active integration of computer technologies into public and private life, which requires the modernization of legislation in the field of information and personal data protection. Otherwise, with the subsequent integration of computer technologies into private and social life, we will see an increase in the number of cybercriminals who will be able to freely terrorize the population, feeling their impunity.

As a result, the scale and appearance of new methods of cybercrime determine the need for further research on this topic, aimed at improving and developing legislation, creating special software tools for protecting human rights, and appropriate methodological support for countering cybercrime.

REFERENCES

Al-Mutawa, N., Bryce, J., Franqueira, V. N. L., & Marrington, A. (2016). Forensic investigation of cyberstalking cases using. *Behavioural Evidence Analysis Digital Investigation, 16*, 96-103.

Alexy, E. M., Burgess, A. W., & Baker, T. (2005). Internet offenders. *Journal of Interpersonal Violence, 20*(7), 804-812.

Barak, A. (2005). Sexual harassment on the Internet. *Social Science Computer Review, 23*, 77-92.

Baum, K., Catalano, S., & Rand, M. (2009). *Stalking victimization in the United States*. Washington DC: U.S. Department of Justice, pp. 1-16.

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research, 32*, 265-277.

Bocij, P. (2005). Reactive stalking: A new perspective on victimization. *The British Journal of Forensic Practice, 7*(1), 23-45.

Bocij, P., Griffiths, M., & McFarlane, L. (2002). Cyberstalking a new challenge for criminal law. *Criminal Lawyer, 122*, 3-5.

Bocij, P., & McFarlane, L. (2002). Cyberstalking: Genuine problem or public hysteria? *Prison Services Journal, 140*(1), 32-35.

Cattaneo, L., Cho, S., & Botuck, S. (2011). Describing intimate partner stalking overtime. *Journal of Interpersonal Violence, 26*(17), 3428-3454.

Dennison, S. M., & Thomson, D. M. (2002). Identifying stalking: The relevance of intent in commonsense reasoning. *Law and Human Behavior, 26*(5), 543-558.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*(4), 468-483.

Henso, B., Reyns, B. W., & Fisher, B. S. (2011). Security in the 21st century. *Criminal Justice Review, 36*(3), 253-268.

Lyndon, A., Bonds-Raacke, J., & Cratty, A. D. (2011). College students' Facebook stalking of ex-partners. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 711-716.

McFarlane, L., & Bocij, P. (2003). Cyberstalking: Defining the invasion of cyberspace. *Forensic Update, 1*(72), 18-22

Pittaro, M. L. (2007). Cyberstalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology, 1*(2), 180–197.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle – Routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

Savina, S. V., Tsvetkova, O. N., Galimova, L. I., Avezov, A. H., & Nazarov, A. A. (2020). Application of telecommunications technologies in the management of territories. *Journal of Environmental Management and Tourism, 11*(5), 1143-1151. doi: 10.14505//jemt.v11.5(45).12

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. *Violence against Women, 13*(8), 842-856.

Spitzberg, B., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media Society, 4*(1), 71-92.

Spitzberg, B. H. (2002). The tactical topography of stalking victimization and management. *Trauma, Violence, and Abuse, 3*(4), 261-288.

State Duma of the Federal Assembly of the Russian Federation. (1996). *Criminal Code of the Russian Federation of June 13, 1996, No. 63-FZ (as amended on April 5, 2021, as amended on April 8, 2021)*. Sobranie Zakonodatel'stva Rossiiskoi Federatsii [SZ RF] [Collection of Legislation of the RF] 17.06.1996, No. 25, Item 2954.

State Duma of the Federal Assembly of the Russian Federation. (2006). *Federal Law of July 27, 2006, No. 152-FZ (as amended on December 30, 2020) "On Personal Data" (as amended and supplemented, entered into force on March 1, 2021).* Retrieved from http://www.kremlin.ru/acts/bank/24154

van der Aa, S. (2011). International (cyber)stalking: Impediments to investigation and prosecution. In R. M. Letschert, J. J. M. van Dijk (Eds.), *The new faces of victimhood: Globalization, transnational crimes and victim rights* (pp. 191-213). Dordrecht, Netherlands: Springer.

Vinichenko, M. V., Rybakova, M. V., Chulanova, O. L., & Makushkin, S. A. (2020). The social environment change under the influence of artificial intelligence: The views of orthodox clergy and parishioners. *European Journal of Science and Theology, 16*(5), 57-67.

Wykes, M. (2007). Constructing crime: Culture, stalking, celebrity and cyber. *Crime, Media, Culture, 3*(2), 158-174.

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]

Ybarra, M. L., & Mitchell, K. J. (2008). How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics, 121*(2), 350-357.

Zelenkov, M. Y. (2021). How to lower the possibility of terrorism development in democratic society? *Justica, 26*(39), 57-78. doi: 10.17081/just.26.39.4909

Zelenkov, M. Y., Fedyakin, I. V., Zinkovsky, S. B., Nikitina, V. S., & Bikov, M. Y. (2021). Religion-state relations as a source of modern terrorism. *Laplage Em Revista*, *7*(2), 463-472. doi: 10.24115/S2446-6220202172769p.463-472

[Received/Recebido: Março 11, 2021; Accepted/Aceito Abril 01, 2022]