DOI 10.52468/2542-1514.2023.7(1).72-82

INTERNET SERVICE PROVIDERS AS SUBJECTS OF PREVENTION OF SEXUAL CRIME ON THE INTERNET

Anna K. Zharova
Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia

Article info
Received –
2022 January 15
Accepted –
2023 January 10
Available online –
2023 March 20

Keywords
Crime, Internet service provider (ISP), moderation, Internet, child pornography, software

The subject of the article is the provisions of the legislation of the Russian Federation aimed at ensuring the sexual inviolability of a minor.

The object of the research is the relations connected with ensuring the sexual inviolability of minors.

The Internet serves as an additional tool that facilitates access to minors, their social pages, the impact on the psyche of minors, and the involvement of children in destructive groups. However, not all articles establishing criminal liability for violation of the sexual inviolability of children contain a qualifying feature - this is the use of the Network in the implementa- tion of such activities. Thus, Art. 135 of the Criminal Code of the Russian Federation, which establishes criminal liability for committing indecent acts against minors, does not contain a qualifying feature - the commission of a crime through the use of the Internet.

The organization of Internet relations on the Web is carried out by various Internet provid- ers, whose activities are connected both with organizing the communications of network users and with ensuring the circulation of information on the Internet. Based on these the- ses, the article provides answers to such questions as can acts were committed with the help of Internet technologies to be qualified under Art. 135 of the Criminal Code of the Russian Federation, is the use of Internet technologies by ISPs effective as a tool to combat crimes against the sexual integrity of minors carried out using the Web, and what legal and technical instruments will ensure the sexual integrity of children?

The study showed that the norms of the Criminal Law aimed at preventing crimes related to the sexual inviolability of minors are also applicable to acts committed using the Internet. In accordance with the legislation of the Russian Federation, violence can take the form of physical or mental impact on a person, carried out through the Internet. Regarding the pos- sibility of committing indecent acts on the Web, it can also be concluded that such acts can be recognized as depraved, despite the absence of direct physical contact with the body of the victim.

States use various methods for determining the content, recognizing images distributed on the Web. The most commonly used technological tool is the information monitoring method. However, the obligation to use this method, both in Russia and in European coun- tries, is not provided for all types of hosting providers.

In connection with the analysis of Russian legislation, we can conclude that the possibilities of such hosting providers as the owners of audiovisual services and news aggregators in the field of information monitoring remained unused. Thus, the Federal Law "On Information, Information Technologies and Information Protection" does not contain requirements for the owners of audiovisual services and news aggregators to conduct mandatory monitoring of information distributed on Internet platforms.

The use of content filtering technology cannot be considered a panacea, but its mandatory use by various hosting providers will reduce the likelihood of distributing prohibited infor- mation.

The requirement for the owners of social networks to monitor content by their users, de- fined by the Federal Law "On Information, Information Technologies, and Information Pro- tection", is only the first step taken towards reducing the volume of prohibited content posted on the Web. However, the requirements for the use of image and text recognition technologies by Internet providers remained outside.

The article used the methods and techniques of formal logic - this is analysis and synthesis, analogy, comparison, hypothesis, proof in order to determine assumptions and find an- swers to the questions posed in the article.

The study and comparative analysis of the practice of ensuring the safety of children from information posted on the Web, reflected in foreign studies, demonstrating possible solu- tions, made it possible to compare Russian experience with the experience of foreign col- leagues and draw conclusions about approaches to solving the problems.

The methods of forecasting and modeling are used for formulating possible ways to develop regulation and eliminate gaps in Russian legislation.

1. Introduction

Crimes against the sexual integrity of minors are among the most serious crimes [1, p. 46]. The relevance of this problem is emphasized by Russian researchers [2, p. 81; 3, p.58; 4, p. 211; 5, p. 69] and foreign researchers [6, 7, 8]. The Organization for Economic Cooperation and Development has identified the following Internet risks for children such as: content risks it is risks associated with pornographic and racist content and contact risks associated with involving a child in sexual crimes [9, p.35].

Analysis of statistical indicators of the number of crimes against sexual integrity and sexual freedom of minors shows an annual increase. In 2012, gaps in the definition of responsibility for acts against minors committed on the Internet and in social networks were partially eliminated. Despite the changes, there are still problems of committing crimes through the Web[10, p. 9], such as child trafficking, distribution of malicious content[11, p. 56], sexual harassment on the Internet[12, p. 20; 13, p.100], the formation of social networks of "death groups" [14, p. 8, 15, p. 55], conducting entertainment events of a pornographic nature on the Internet[16, p. 45, 17, p. 119], Internet exploitation of children[18, p. 3,4], evaluation of e-mail addresses, etc. evidence of acts committed online[19, p. 259; 20, p. 120].

Traumas of the child's psyche after sexual abuse [21, p. 1] make it necessary to study this problem[22; 23, p. 145; 24, p. 1-2]. Internet service providers, as information intermediaries, ensure the organization of emerging relationships. Understanding this encourages governments and legislators to develop a system for countering crime, giving Internet service providers additional legal tools.

The Art. attempts to answer the following questions: is the use of image and text recognition technologies by providers effective as tools for countering crimes against the sexual integrity of minors committed on the Internet, as well as whether indecent acts committed using Internet technologies fall within the scope of Art. 135 of the Criminal Code of the Russian Federation.

2. Indecent acts committed with the help of Internet technologies

The Web is preparing to commit a crime [25, p.180; 26, p. 2923; 27, p. 108] and there are more and more of them. Researchers disagree about negative Internet impacts[28, 29]. The features of committing sexual acts are discussed, such as the age of the child and the age difference between the child and the offender[30], touching the child or their absence[31] , only viewing pornography[32], whether the child knows the criminal[33; 34; 35; 36].

Analysis of court decisions allows us to conclude that such actions are qualified under Art. 135 of the Criminal Code of the Russian Federation, which establishes criminal liability for indecent sexual acts against minors without the use of violence, as well as under Art.242.1 of the Criminal Code of the Russian Federation, which provides for criminal liability for the production and trafficking of materials or objects with pornographic images of minors.

However, can violence be carried out online?

Since the Criminal Code of the Russian Federation does not disclose the concept of "violence", let us turn to the Plenum of the Supreme Court of the Russian Federation, which, under the threat of using violence in the commission of a crime under para "a" of Part 2 of Art. 282 of the Criminal Code, understands "statements or other actions expressing the intention of the perpetrator to use any physical violence against the victim" (para 9). "Violence in Art. 131 and Art. 132 of the Criminal Code of the Russian Federation should be understood as both dangerous and non-life-or health-threatening violence, including beatings or other violent acts related to causing physical pain to the victim or restricting his freedom".

The Decree of the President of the Russian Federation "On approval of the Charter of the Military Police of the Armed Forces of the Russian Federation and Amendments to Certain Acts of the President of the Russian Federation" defines violence as one of the forms of "cruel or degrading treatment" (item 201).

Thus, it can be concluded that in

ISSN 2542-1514 (Print)

accordance with the legislation of the Russian Federation, violence can take the form of physical or mental impact on a person. For the commission of mental violence, it does not matter whether the perpetrator is near the victim or not, especially if we are talking about a minor whose psyche is mobile. Thus, violence can also be implemented on the Internet.

Criminals are well versed in the technique of psychological influence [37], posting information both in social networks and sending it directly to minors, they use slogans and visualize them[38, p.13; 39]. The Plenum of the Supreme Court of the Russian Federation considers that indecent acts "can also be recognized as such actions in which there was no direct physical contact with the victim's body, including actions committed using the Internet or other information and telecommunications networks."

So, we can conclude that Art. 135 of the Criminal Code of the Russian Federation can be applied to a person who commits indecent acts on the Internet, despite the absence of direct mention of the Internet as a qualifying feature in Art. 135 of the Criminal Code of the Russian Federation. However, scientists propose to supplement Art. 135.1 of the Criminal Code of the Russian Federation, the composition of which is defined as "harassment of a minor for sexual purposes", which qualifies a sign as sexual harassment by an adult to a minor using the Internet [3, p.55].

Since the criminal has been conducting correspondence with a minor for several months, using certain terminology, videos, and photos, the question is natural – can Internet technologies prevent such a long communication, as well as recognize indecent actions and materials accompanying them?

3. Information technologies for crime prevention

Information posted on the Web stays there forever. Accordingly, pornographic materials sent by the criminal to the victim are stored by hosting providers, telecom operators and other information intermediaries. In accordance with clause 12 of the Rules of interaction between telecom operators and authorized state bodies engaged in operational search activities, a telecom operator must store information about subscribers and their switching within three years on the territory of the Russian Federation. According to Art. 64 Federal Law "On Communications" telecom operators are required to store information about messages from users of communication services for three years from the date of completion of such actions. Text messages of users of communication services and other messages should be stored by telecom operators for up to six months. Art. 10.1 of the Federal Law "On Information, Information Technologies and Information Protection "(hereinafter referred to as the Law "On Information") provides for similar obligations of the organizer of information dissemination on the Internet.

Since information on the Web remains forever and is stored by Internet service providers for six months to three years, the legislator should oblige Internet service providers to use image recognition technologies and filtering programs, working ahead of time, although it must be recognized that this is not possible in all cases [40, p.19]. Mandatory use of such technologies is provided only for educational organizations on school computers. For example, the Federal Law "On the Protection of Children from Information harmful to their health and Development" does not contain such requirements for Internet service providers. In order for filtering to be mandatory for all Internet service providers, it is necessary to fix this requirement at the legislative level.

The owner of a social network is required to use a different technology – information monitoring; other Internet service providers are not required to do so.

4. Can Internet intermediaries "intercept" illegal information?

On the one hand, the information transmitted from user to user over the Network is related to personal data, since it relates "directly or indirectly to a specific or identifiable individual" (Part 1 of Art. 3 of the Federal Law "On Personal Data"). For example, in compliance with confidentiality requirements, the hosting provider refused to disclose information about the person who placed the ad on the site. The ECHR confirmed the legality of these actions [41, p. 192]. On the other hand, no one has the right

to believe that the transmitted information is prohibited for distribution in advance. It is only possible to determine the essence of its content after obtaining access to the information on a legal basis.

It is impossible to ensure interception of transmitted information in the Web, since the TCP / IP protocol transmits information over the Internet in small data packets, in which it is impossible to recognize and evaluate the content of the transmitted information [42, p. 0472].

However, the same TCP / IP protocol collects information as a whole from the recipient of information, the content of which can already be evaluated. Various legal and technical tools are used to evaluate content without violating confidentiality requirements. Technical tools, for example, include artificial intelligence (AI) recognition technologies for images and symbols, which the People's Republic of China actively uses [43, p. 46]. AI, without identifying a person, recognizes the potential harmfulness of information that must be confirmed by a human AI operator. Only if this fact is confirmed, a link is established between the sender and users of this information in order to determine the identity of criminals. Since trafficking in pornographic materials is a crime if it is carried out for the purposes specified in Art. 242.1 of the Criminal Code of the Russian Federation.

Most states use such a tool to restrict the turnover of obscene materials as blocking the IP addresses of sites that host such material. Among them are Russia, Great Britain, France, and Germany [44, p. 35].

Russian judicial practice looks at downloading child pornography in a slightly different way. Thus, the Supreme Court of the Russian Federation determined that the fact that a citizen was aware that pornographic files were downloaded to his computer, which could have been available for download through a file exchange network to other users, cannot indicate that the convicted person intended to distribute them, since they were already distributed on the Internet and were freely available. Although the lower courts found the citizen guilty of committing a crime under Para "a", "d" of part 2 of Art. 242 of the Criminal Code of the Russian Federation, because he, using his personal computer, copied pornographic images of minors into a file-sharing program that allows downloading, sharing files, and providing access to them to an unlimited number of users[1].

In this example, the provider cannot track the information sent by the user, because the exchange is carried out through a file exchanger. Providers that store user information and provide access to it can monitor and filter the information. Although, scientists believe that these actions have drawbacks, for example, the lack of transparency in the operation of such technologies [45], guarantees that exclude the responsibility of Internet intermediaries in certain cases, and the risks of excessive removal of illegal content [46].

In addition, filtering algorithms can make mistakes when recognizing legitimate text as illegal, since existing algorithms have not yet developed to the level of human intelligence and cannot determine the essence of the text content.

Konovalov N. N. believes that "Russian judicial practice recognizes materials or objects containing nude minors as pornographic only in cases where the delinquent's sexual interest is established" [47, p. 16]. It is difficult to agree with the author's opinion, Art. 242.1 of the Criminal Code of the Russian Federation refers to crimes "manufacturing, acquiring, storing and (or) moving across the State Border of the Russian Federation for the purpose of distributing, publicly demonstrating or advertising, or distributing, publicly demonstrating or advertising materials or objects with pornographic images of minors". In other words, the Art. of the Criminal Law clearly

[1] Cassation ruling of the Judicial Board for Criminal Cases of the Supreme Court of the Russian Federation dated 10.07.2019 No. 16-UD19-7 Verdict: According to paragraphs "a", "d", Part 2 of Art. 242.1 of the Criminal Code of the Russian Federation for possession for the purpose of distributing materials with pornographic images of minors. Definition of the Supreme Court of the Russian Federation: Judicial acts have been canceled, the criminal case has been terminated due to the absence of corpus delict in the act, the right to rehabilitation has been recognized. *Bulletin of the Supreme Court of the Russian Federation*. 2020. № 6.

ISSN 2542-1514 (Print)

identifies the purpose of the criminal's actions. As noted by Makarov A.V. and Zhukova M.V., in the absence of a goal, a person cannot be brought to criminal responsibility for this crime [45, p. 44].

All these examples once again prove the complexity of automating the assessment of the content of information distributed on the Internet.

Under such circumstances, social networks that are hosting providers should have legal tools for self-regulation of information distributed in their networks. To solve this problem, in 2020 the Law "On Information" includes Art. 10.6, which contains the obligation of the owner of a social network to moderate content in order to identify, among other things, materials with pornographic images of minors or ads about attracting minors as performers of pornographic activities (Para “a”and “e” of Part 5 of Art. 10.6 of the Law "On Information").

For other hosting providers, for example, the owner of an audio-visual service, a news aggregator, or an organizer of information distribution on the Web, the obligation to monitor information is not provided. Roskomnadzor independently monitors information on the Internet sites of these providers.

The requirement to monitor information, for example, is provided for by the legislation of Florida and Georgia [48, p. 79].

5. Conclusion

The study showed that the norms of criminal law aimed at preventing crimes related to the sexual integrity of minors are also applicable to acts committed on the Internet. Violence on the Internet can take the form of physical or mental impact on a person. Committing indecent acts is also possible online, despite the lack of direct physical contact with the victim's body.

The capabilities of hosting providers, such as owners of an audio-visual service, news aggregators and organizers of information distribution on the Web in the field of information monitoring remained unused. The requirement set by the Law "On Information" for owners of social networks to monitor the information disseminated by their users is the first step taken towards reducing the volume of prohibited content posted on the Web. However, the requirements for the use of image and text recognition technologies by Internet service providers remain outside the limits. Having formed a system of requirements for providers of various levels on the use of information filtering and monitoring technologies, taking into account that the responsibility for monitoring information is already assigned to Roskomnazdor, you can significantly complicate the distribution of information harmful to children over the Web and thereby protect them on the Internet.

REFERENCES

1. Engelgardt A.A., Zemskaya E.V. A qualification of the aggregate of crimes against sexual immunity and sexual freedom of minors (in the meaning of a note to article 131 of the Criminal code of the Russian Federation). *Rossiiskii sledovatel' = Russian Investigator*, 2018, no. 5, pp. 44–47. (In Russ.).

2. Esakov G.A. (ed.). *Commentary on the Criminal Code of the Russian Federation*, article by article, 9th ed. Moscow, Prospekt Publ., 2021. 816 p. (In Russ.).

3. Donchenko A.G., Tokareva A.A. Responsibility for crimes related to sexual exploitation and sexual abuse of minors in modern legal systems. *Lex russica*, 2018, no. 6, pp. 54–62. (In Russ.).

4. Karagodin V.N. *Investigation of intentional crimes against life, sexual freedom and inviolability of minors*, Monograph. Moscow, Prospekt Publ., 2018. 320 p. (In Russ.).

5. Dolgova S.I. Some aspects of organization of operations of internal affairs agencies of the CIS member states aimed at prevention of the involvement of minors in destructive groups on the Internet. *Administrativnoe pravo i protsess = Administrative Law and Procedure*, 2021, no. 6, pp. 68–73. (In Russ.).

6. Anh P., Kathryn S.S., Kim-Kwang R.Ch. Threaten me softly: A review of potential dating app risks. *Computers in Human Behavior Reports*, 2021, vol. 3, art. 100055. DOI: 10.1016/j.chbr.2021.100055.

7. Zhong L.R., Kebbell M.R., Webster J.L. An exploratory study of Technology-Facilitated Sexual Violence in online romantic interactions: Can the Internet's toxic disinhibition exacerbate sexual aggression? *Computers in Human Behavior*, 2020, vol. 108, art. 106314. DOI: 10.1016/j.chb.2020.106314.

8. Tantum M., Ross T. Legal responsibility of Internet service providers: Part 1. *Network Security*, 1999, vol. 1999, iss. 1, pp. 10–15. DOI: 10.1016/S1353-4858(99)80002-6.

9. Kobzeva S.V. Juvenile Right Protection from Internet Threats. *Informatsionnoe pravo = Information Law*, 2017, no. 2, pp. 33–39. (In Russ.).

10.Turkulets V.A. Sexting with regards to minors: criminal legal and victimological aspect. *Yuridicheskie issledovaniya = Legal Studies*, 2020, no. 5, pp. 1–11. DOI: 10.25136/2409-7136.2020.5.33125. (In Russ.).

11. Zharova A.K. Legal tools of protection of internet users from cyberbullying. Experience of Great Britain. *Yuridicheskii mir = Juridical World*, 2021, no. 7, pp. 52–57. (In Russ.).

12. Dacka M. Child sexual abuse – issues and prevention. *Psychologia Wychowawcza*, 2022, vol. 65, no. 23, pp. 5–22. DOI: 10.5604/01.3001.0015.9114.

13. Tereshchenko L.K. Regulation and deregulation of communications by state. *Zhurnal rossiiskogo prava = Journal of Russian Law*, 2019, no. 10, pp. 98–108. DOI: 10.12737/jrl.2019.10.8. (In Russ.).

14. Maslov A.A., Babushkin A.A., Belykh-Silaev D.V. The main areas of joint research of the Ministry of Internal Affairs of Russia and the Federal Penitentiary Service of Russia in the sphere of criminal intelligence and surveillance operations. *Ugolovno-ispolnitel'naya sistema: pravo, ekonomika, upravlenie = Criminal-Executory System: Law, Economics, Management*, 2021, no. 5, pp. 3–9. DOI: 10.18572/2072-4438-2021-5-3-9. (In Russ.).

15. Kiryukhin V.V. On building up administrative law measures aimed at combating activities on the Internet provoking suicidal behavior in minors. *Administrativnoe pravo i protsess = Administrative Law and Procedure*, 2020, no. 6, pp. 53–56. (In Russ.).

16. Sharapov R.D. Qualification of crimes related to illegal trafficking of pornographic materials and objects. *Zakonnost',* 2021, no. 8, pp. 43–48. (In Russ.).

17. Dvoryanchikov N.V., Antonov O.Yu., Shulga T.I., Korchagin N.Yu. Specifics of Psychological Impact Strategies for Persons Committing Sexual Crimes Against Minors through the Internet. *Psychology and Law*, 2020, vol. 10, no. 2, pp. 111–126.

18. Morteza D., Maliheh A., Moghanibashi-Mansourieh A., Ostadhashemi L. Facilitators and Barriers to Child Sexual Abuse Interventions: A Qualitative Study of Interventions in Iran. *Iranian Journal of Psychiatry and Behavioral Sciences*, 2022, vol. 16, iss. 4, art. e129326. DOI: 10.5812/ijpbs-129326.

19. Zharova A. Ensuring the Information Security of Information Communication Technology Users in Russia. *International journal of Cyber Criminology*, 2019, vol. 13, no. 2, pp. 255–269. DOI: 10.5281/zenodo.3698141.

20. Voronin M.I. Characteristics of Electronic (Digital) Evidence Assessment. *Aktual'nye problemy rossiiskogo prava = Actual Problems of Russian Law*, 2021, no. 8, pp. 118–128. DOI: 10.17803/1994-1471.2021.129.8.118-128. (In Russ.).

21. Fanslow J., Hashemi L., Gulliver P., Mcintosh T. A century of sexual abuse victimisation: A birth cohort anal-

ysis. *Social Science & Medicine*, 2021, vol. 270, iss. 12, art. 113574. DOI: 10.1016/j.socscimed.2020.113574.

22. Hayward D., Cheit R.E. Child sexual abuse, in: Sanders T. (ed.). *The Oxford Handbook of Sex Offences and Sex Offenders*, Oxford University Press, 2017, pp. 123–142. DOI: 10.1093/oxfordhb/9780190213633.013.15.

23. Aswadi Aswadi, Suriah Suriah, Stang Stang, Nurhaedar Jafar, Erniwati Ibrahim, Ridwan Amiruddin, Sukfitrianty Syahrir. Edutainment as A Strategy of Child Sexual Abuse Prevention: Literature Review. *Open Access Macedonian Journal of Medical Sciences*, 2022, vol. 10, no. F, pp. 141–145. DOI: 10.3889/oamjms.2022.7670.

24. González-Prendes A.A., Hicks L.M., Matthews Th., Domke S. Cognitive-Behavioral Therapy, in: *Oxford Bibliographies*, Last modified: 27 June 2018. DOI: 10.1093/OBO/9780195389678-0149.

25. Alieva E.A. Internet as a means of performance sexual abuse. *Probely v rossiiskom zakonodatel'stve = Gaps in Russian Legislation*, 2017, no. 4, pp. 180–182. (In Russ.).

26. Singh R., Koushal V., Bharti B. A descriptive study on child sexual abuse act in India. *Journal of Family Medicine and Primary Care*, 2022, vol. 11, iss. 6, pp. 2923–2932. DOI: 10.4103/jfmpc.jfmpc_1071_21.

27. Ngo N. Child sexual abuse violence against human dignity of children Child sexual abuse violence against human dignity of children. *International Journal of Research Studies in Education*, 2021, vol. 10, no. 15, pp. 97–108.

28. Sabine K. Witting, Transnational by Default: Online Child Sexual Abuse Respects No Borders. *The International Journal of Children's Rights*, 2021, vol. 29, iss. 3, pp. 731–764.

29. Ali S., Paash A.S. A systematic review of the technology enabled child sexual abuse (OCSA) &it's impacts. *Journal of Legal, Ethical and Regulatory Issues*, 2022, vol. 25, special iss. 5, pp. 1–18.

30. Amirova D.K., Gilmutdinov D.D. Criminal Liability for Lecherous Acts Committed Against Minors Using the Information and Communication Network Internet. *Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii = Scientific Notes of the Kazan Law Institute of MIA of Russia*, 2021, vol. 6, no. 2 (12), pp. 122–125. (In Russ.).

31. Mamedyarov A.A. Depraved actions using the Internet. *Colloquium-Journal*, 2019, no. 8–9 (32). pp. 51–52. DOI: 10.24411/2520-6990-2019-10211. (In Russ.).

32. Jud A., König E., Liebhardt H., Fegert J.M. How to find help in the Internet? Internet researches aiming at service support in cases of child sexual abuse. *Nervenheilkunde*, 2013, vol. 32, iss. 11, pp. 841–847.

33. Skvortsova O.V., Makarenko D.D. Acts of sexual abuse through the use of Internet. *Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. Yuridicheskie nauki = Scientific Notes of V.I. Vernadsky Crimean Federal University. Juridical Science*, 2021, vol. 7, no. 1, pp. 146–153. DOI: 10.37279/2413-1733-2021-7-1-146-153. (In Russ.).

34. Ali S., Haykal H.A., Youssef E. Child Sexual Abuse and the Internet – A Systematic Review. *Human Arenas*, 2021, vol. 4, iss. 1. DOI: 10.1007/s42087-021-00228-9.

35. Mitchell K.J., Jones L.M., Finkelhor D., Wolak J. Internet-facilitated commercial sexual exploitation of children: Findings from a nationally representative sample of law enforcement agencies in the United States. *Sexual Abuse: A Journal of Research and Treatment*, 2011, vol. 23, iss. 1, pp. 43–71.

36. Kloess J.A., Hamilton-Giachritsis C.E., Beech A.R. Ofense processes of online sexual grooming and abuse of children via Internet communication platforms. *Sexual Abuse: Journal of Research and Treatment*, 2019, vol. 31, iss. 1, pp. 73–96.

37. Pestereva Yu.S., Ragozina I.G., Chekmezova E.I. Role of the Plenum of Russian Supreme Court in the judicial practice formation. *Pravoprimenenie = Law Enforcement Review*, 2021, vol. 5, no. 4, pp. 209–225. DOI: 10.52468/2542-1514.2021.5(4).209-225. (In Russ.).

38. Dvoryanskov I.V., Panfilov E.E. The state and issues of prevention of delinquent behavior of minors. *Ugolovno-ispolnitel'naya sistema: pravo, ekonomika, upravlenie = Criminal-Executory System: Law, Economics, Management*, 2018, no. 5, pp. 11–15. DOI: 10.18572/2072-4438-2018-5-11-15. (In Russ.).

39. Dolgikh T.N. *The concept and signs of the subject of the crime. Features of the special subject of the crime*. 2021. Available at ConsultantPlus. (In Russ.).

40. Elin V.M. Criminal-legal protection of information in the GAS «Vybory» as a development of the provisions of the doctrine of information security. *Pravovye voprosy svyazi*, 2009, no. 2, pp. 17–21. (In Russ.).

41. Noel G. Muridzo, Chikadzi V., Kaseke E. Challenges Encountered by Children with Disabilities Accessing Child Sexual Abuse Interventions in Zimbabwe. *Journal of Human Rights and Social Work*, 2018, vol. 3, iss. 1, pp. 191–201.

42. Zharova A., Elin V., Panfilov P. Technological and legal issues of identifying a person on the internet to ensure information security, in: Katalinic B. (ed.). *Proceedings of the 29th International DAAAM Symposium ''Intelligent Manufacturing & Automation'' (24-27th October 2018, Zadar, Croatia)*, Vienna, DAAAM International Publ., 2018, pp. 0471–0478. DOI: 10.2507/29th.daaam.proceedings.069.

43. Troshchinsky P.V. Digital China before and during the coronavirus period: specifics of normative legal regulation. *Law and Digital Economy*, 2021, no. 1, pp. 44–58. DOI: 10.17803/2618-8198.2021.11.1.044-058.

44. Elin V.M. *Comparative analysis of the legal support of information security in Russia and abroad*, Monograph. Moscow, 2016. 165 p. (In Russ.).

45. Makarov A.V., Zhukova M.V. Relevant issues of criminal liability for manufacture of pornographic materials featuring juveniles for circulation purposes. *Rossiiskii sledovatel' = Russian Investigator*, 2017, no. 15, pp. 43–47. (In Russ.).

46. Zharova A., Elin V. State regulation of the IoT in the Russian Federation: Fundamentals and challenges. *International Journal of Electrical and Computer Engineering*, 2021, vol. 11, iss. 5, pp. 4542–4549. DOI: 10.11591/ijece.v11i5.pp4542-4549.

47. Konovalov N.N. Liability for the manufacture and circulation of files or objects with pornographic images of minors in international, foreign and Russian criminal law. *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yustitsiya = International Criminal Law and International Justice*, 2021, no. 2, pp. 15–18. DOI: 10.18572/2071-1190-2021-2-15-18. (In Russ.).

48. Fedorov A.V. The criminal liability of legal entities in Georgia. *Rossiiskii sledovatel' = Russian Investigator*, 2021, no. 10, pp. 73–80. (In Russ.).

INFORMATION ABOUT AUTHOR

Anna K. Zharova – Doctor of Law, Associate Professor; Senior Researcher
Institute of State and Law of the Russian Academy of Sciences
10, Znamenka ul., Moscow, 119019, Russia E-mail: anna_jarova@mail.ru
ORCID: 0000-0002-2981-3369
ResearcherID: H-4012-2015
Scopus AuthorID: 56964137900
RSCI SPIN-code: 2240-1467

BIBLIOGRAPHIC DESCRIPTION

Zharova A.K. Internet service providers as subjects of prevention of sexual crime on the Internet. *Pravoprimenenie = Law Enforcement Review*, 2023, vol. 7, no. 1, pp. 72–82. DOI: 10.52468/2542-1514.2023.7(1).72-82. (In Russ.).