Juvenile Cybersecurity and Artificial Intelligence System

Erokhina E.V.[*], Letuta T.V.

Orenburg State University, Orenburg, Russia
[*]Corresponding author. Email: erohina.elena2020@gmail.com

ABSTRACT
Social networks and instant messengers have become so firmly established in everyday life that it becomes impossible to imagine your day without virtual space. Protecting children on the Internet is a relatively recent area of research and many countries are in the process of re-evaluating and developing new national legal policies. The relevance of the work stems from the fact that the transformation of public and private life into an increasingly digital, Internet-based model requires a rapid change in laws and regulations on privacy, data protection, and cybersecurity of minors. The scientific work outlines the main trends in the development of cyber threats against minors in the modern global information space; researched international and national legal regulation of the methods of cyber protection of minors; analyzed the controversial issues of the relationship between the rights of the child to freedom of expression and obtaining information from the responsibilities of the state and parents to ensure their safety The introduction of the artificial intelligence system "Internet-based family trust" is proposed, its technical elements are revealed, an algorithm is proposed for securing the legal status of the subjects of this system.

Keywords: *computer security, cyber threats, juvenile rights, harm, artificial intelligence system, information space, legal support of cyber security*

1. INTRODUCTION

The advances in computer technology and the development of the Internet have led to the fact that almost everyone lives in two worlds: real and virtual. Both worlds are interconnected with each other - the virtual world creates various Internet forms of real persons, establishes social and legal obligations. The main qualities of active Internet users (generation Z) are their openness, willingness to share information about themselves with an unlimited number of people. Minors independently put on public display part of their personal life, and sometimes all (bloggers). The individualization of the individual and the confirmation of his activities are transferred to the digital environment, which creates endless opportunities for abuse and the commission of crimes.

Proclaimed in the Declaration of Human Rights [1], the Convention for the Protection of Human Rights and Fundamental Freedoms [2], and in the basic laws of most states, the human rights (including the minor) to privacy, personal and family secrets, freedom of expression and information are fundamental, and their protection is entrusted to states and their associations. But at the same time, the UN Convention on the Rights of the Child[3] and other international acts impose an obligation on states to ensure the safety of minors. A dilemma arises when, on the one hand, the state and parents need to ensure the freedom of minors to use the Internet space, and on the other hand, it is necessary to protect them from the actions of cybercriminals.

Directly or indirectly, the issues of protecting children from harmful information on the Internet and finding the best means of such protection are given attention in legal and other specialized literature (A.V. Komarnitsky, A.S. Mosharova, D.A. Karabatova, M.S. Semikina, E.S. Akimysheva, A.A. Chesnokov M. Naarttijärvi, Justyna Wojniak, Marta Majorek, and other researchers). However, most of these studies focus on the role of good psychological work between parents and children, or investigate only certain aspects of this problem. We believe that the solution to the problem of the safety of minors in the Internet space should be based on interdisciplinary research, including research in the field of cultural and communicative fields of science, Internet research, information, pedagogical, psychological and sociological research, research on human-computer interaction, science and technologies, and, as one of the most basic types of research, it is necessary to recognize research in the field of jurisprudence aimed at determining the boundaries of what is permitted in the legal regulation of data personalization.

The purpose of the study is to identify the possibility of using an artificial intelligence system in order to prevent harm to minors.

2. METHODOLOGY OF THE STUDY

The civilizational approach will allow taking into account the assessment of modern cyber threats against minors, analyzing the problems and prospects for the development of legal support for the intellectual system "Internet environment of family trust" as the most optimal strategy for Russia in this area, taking into account cultural and national characteristics and technical development

The method of systems analysis will be used to study the legal support of cybersecurity of minors at the international and national levels, analyze the status of subjects of the intellectual system "Internet environment of family trust" and their interaction.

The formation method (dialectical-materialistic approach) will make it possible to come to the unification of the fundamental legal principles, norms and institutions in the field of international cooperation while ensuring the cybersecurity of minors.

3. ISSUES OF LEGAL REGULATION OF THE SAFETY OF MINORS IN CYBERSPACE

Protecting children on the Internet is a relatively recent area of concern for states, requiring a reassessment of existing government legal policies and the development of new legal policy responses.

Imagine seeing your ten-year-old son talking on the street with a stranger. At a minimum, you will try to find out who this person is, and what common topics of conversation your son and man may have. How will you feel when the child says that this is his friend, they communicate every day, they met in the park, and the child does not know who the man works and where he lives? This example is certainly scary. However, in terms of its prevalence, it is probably not as common in practice as dubious acquaintances in the Internet space. The problem of protecting children from such "suspicious, potentially dangerous persons" in the Internet space is becoming alarming. This is due to the fact that "early Internet growing up" is in dissonance with the legal capacity of minors. Minors, before reaching social maturity, are already skillfully mastering modern technologies, explaining their long work at the computer by the need to complete their homework. Almost 92% of minors are able to hide potentially dangerous active actions in the virtual space from their parents (watching content inappropriate by age, communicating with dangerous strangers or participating in online bullying) [4]. On the other hand, modern technologies open up wide opportunities for communication and realization of one's interests: trips to the store are being replaced by distance purchases, reading in the halls of the library is being replaced by online access to its funds and the possibility of distance learning. In conditions of infinitely expanding opportunities, a minor, as a subject that does not have full legal capacity, is not able to independently prioritize his communication and determine interests that are useful for his future.

We highlight the following types of cyber threats for a minor:

– disclosure of personal, family secrets – may adversely affect further education, professional activities of the minor and his family members;

– hobby for games in online casinos – can put the family of a minor in a difficult financial situation and harm the mental health of all family members;

– gaining access of a minor to illegal, harmful information (pornography or images promoting racism and violence);

– involvement of minors in activities dangerous to their life, health and moral foundations (promotion of suicide, self-harm, "courtship of pedophiles", "Internet theft of the identity of a minor", "online bullying"). A 2017 study by Julia Davidson Saqba Batool, Ciaran Haughton and Anulekha Nandi found that 6 to 25% of children in the UK are victims of cyberbullying [5].

At the same time, parents are not always able to represent and protect the interests of children and the interests of the family in the Internet space.

Cybersecurity consists of safeguards and actions that can be used to protect a cyber domain, in the public, government, military, and family areas, from threats that can harm or harm interdependent networks and information infrastructure.

Directly or indirectly, the issues of protecting children on the Internet and finding the best means of such protection are given attention in legal and other special literature. So M. Naarttijärvi in his work, assessing the relationship between the protection of personal data and the need to ensure supervision of messages, insists on the observance of the principles of legality and proportionality [6]. The work of Justyna Wojniak, Marta Majorek focuses on actors who can prevent harm from cybercriminals on the Internet, and the importance of educational programs, including information support of the program to protect children from cybercrime [7]. Charlotte Chang analyzes parent and school cybersecurity prevention efforts [8]. Various statistical reports [9] provide the results of an analysis of the performance of programs that block unwanted content [10].

Ensuring cybersecurity of minors is regulated by various regulatory legal acts and international acts, including: Declaration of Human Rights; Convention for the Protection of Human Rights and Fundamental Freedoms; UN Convention on the Rights of the Child;

the model law of the IPA CIS "On the protection of children from information harmful to their health and development" [11]; 2008 Declaration on the Protection of the Dignity, Safety and Privacy of Children on the Internet [12], EU Recommendation on Measures to Promote Respect for Freedom of Expression and Information with regard to Internet Filters [13]; EU Recommendation on the Empowerment of Children in a New Information and Communication Environment [14]; Recommendation of the EU Committee of Ministers "On measures to protect children from harmful content and behavior and to promote their active participation in the new information and communication environment" [15].

States also enact national legislation to protect children from cyberthreats: for example, Japan's Digital Security Strategy [16], US Children's Online Privacy Protection Act [17], Canada's Cybersecurity Strategy [18].

In Russia, the Doctrine of Information Security of the Russian Federation [19], the Decree of the President of the Russian Federation "On measures to ensure the information security of the Russian Federation when using information and telecommunication networks of international information exchange" [20], "Fundamentals of the state policy of the Russian Federation in the field of international information security for the period up to 2020". [21], Federal Law "On the Protection of Children from Information Harmful to Their Health and Development" [22]. There are many scattered articles and clauses in the laws, for example, Art. 64 in 126-FZ "On Communication" [23], Art. 15.2-15.8 in 149-FZ "On information, information technology and information protection" [24], etc. However, there is no single comprehensive regulatory legal act securing a single strategy for the Russian Federation to ensure the cybersecurity of minors.

4. ARTIFICIAL INTELLIGENCE SYSTEMS AS A SOLUTION TO MINOR SAFETY PROBLEM

In most countries, parents and their substitutes are responsible for the care and protection of their children. Parents are the main actors with the rights and responsibilities to educate, care for, represent, and protect the interests of the child. We believe that such protection also includes protecting the child from the threats of the digital world because in most cases the harmful consequences of such threats are realized in the real world. But it is impossible to require parents to effectively perform their duties or to impose responsibility on them in cases where, for objective reasons, they cannot. Parents cannot know all the dangerous content that appears, changes, etc., they do not have professional skills in identifying fake pages or programming bookmarks [25]. They cannot independently master all gadgets, hack into the accounts of their children, both due to lack of knowledge and due to fear of undermining the trusting relationship that should be between family members (family trust).

For parents who are concerned about the safety of their children on the Internet, such tools are offered as: setting the function of "parental control" on the computer, programming certain bookmarks on the website or social network of service providers, etc. But let's be honest - in most cases it doesn't work [11].

We believe that such a virtual island in the digital space is needed, which would allow parents to: effectively take care of their children without violating the boundaries of their personal space; be confident in the preservation of information that constitutes personal and family secrets of family members; and gave children the opportunity to exercise their rights. In this case, we are talking about artificial intelligence as a real tool that can be effective, since they imitate aspects of intellectual behavior that have a high degree of self-determination (autonomy) and independence from the will of the developer or user [26].

We propose to create a technical and legal basis for such a tool as "Artificial Intelligence "Internet Environment of Family Trust". The subjects of which will be:

– Law enforcement agencies, which constantly update black and white lists of sites, form a list of keywords, generate information on undesirable areas in social networks, etc. and transmit this information to AI "Internet environment of family trust"

– Parents who, through their will and will, define unwanted content, set keywords and form basic prohibitions. Note that definitions of illegal and unacceptable content for children fall under national interpretation and reflect cultural and social values.

AI "Internet environment of family trust" when it detects that a minor communicates with a fake page, when recording messages of pornographic content or Internet terror, transfers information to parents and law enforcement agencies, which take appropriate response measures against operators.

Parents and the state cannot foresee in advance all types of cyber threats to a minor. AI "Internet environment of family trust" as a self-learning program, within the framework of the given criteria, will make a decision to block new sites, prohibit transactions, etc. Although, undoubtedly, the subsequent approval of the actions of the AI by the parents will be critical.

Also, the AI "Internet environment of family trust" will inform the parents about the presence of a threat to the child in general, without giving them the opportunity to read messages, watch the page on social networks, etc. If there is a relationship of trust between the parents and the child, they have authority, then the parents will be able to convey the danger to the minor.

If, based on the results of the inspection, the law enforcement authorities establish the danger or unlawfulness of actions against a minor child, then they can initiate a case and inform the parents that their child is in danger, but more specific.

Developing artificial intelligence "Internet environment of family trust" can be used: white and black lists of sites, phrases - a widely used method. The disadvantages are the lack of a real assessment of the content and fairly simple workarounds. DNS protection can also be used, which is much more difficult to circumvent. Combined systems for analyzing audio-visual information are of particular interest, but at the moment they can only be installed on powerful computers. Within the framework of creating an effective system, it is permissible to use both semantic analysis of content and intellectual classification of text.

5. CONCLUSION

In the modern world, the "early Internet growing up" of minors is in dissonance with their legal capacity.

On the one hand, the state and parents are obliged to ensure the safety of a minor child, including cybersecurity, on the one hand, and on the other, they are obliged to ensure the realization of such rights of minors as the right to: expression of their own opinion, the right to receive information, personal and family life, confidentiality.

We believe that modern legal support for the safety of minors in cyberspace is insufficiently developed in terms of its scope and content and does not provide protection against cyber threats. We believe that to ensure the safety of minors in the digital world, states should adopt state and interstate cybersecurity strategies for minors, combining legislative, technical, educational and educational measures. The most responsive to the modern challenges of the information space is the European Strategy for Improving the Internet for Children.

Effective cybersecurity of minors is only possible with the cooperation of parents, society, the state and the private sector (in the field of IT technologies). Using in the digital space, the proposed artificial intelligence "Internet environment of family trust" would allow parents to: effectively take care of their children, without violating the boundaries of their personal space; be confident in the preservation of information that constitutes personal and family secrets of family members; and for children to ensure the child's right to privacy and confidentiality.

AI "Internet environment of family trust" will represent one of the most effective, efficient ways to solve the problem of realizing the rights of minors to access information and to express their opinion, the effectiveness of the exercise of parental rights and responsibilities for caring for the child's personality and safety, the implementation of the state of public interests in the field of family and child protection.

REFERENCES

[1] 1 Universal Declaration of Human Rights. Adopted by Resolution 217 A (III) of the UN General Assembly on December 10, 1948. https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

[2] Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4. XI. 1950. URL: https://www.echr.coe.int/documents/convention_rus.pdf https://www.echr.coe.int/documents/convention_rus.pdf

[3] Convention on the Rights of the Child. Adopted by General Assembly resolution 44/25 of 20 November 1989. URL: https://www.un.org/ru/documents/decl_conv/conventions/childcon.shtml

[4] R. Siciliano? What the child is hiding. URL: https://www.mcafee.com/blogs/consumer/family-safety/digital-divide/

[5] I. Zych, R. Ortega-Ruiz, R. Del Ray, Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention, and intervention. Aggression and Violent Behavior, 23 (2015) 1-21. DOI: 10.1016 / j.avb.2015.10.001

[6] S. Livingstone, J. Davidson, J. Bryce, C. Haughton, A. Nandi. Children's online activities, risks and safety: a literature review by the UKCCIS Evidence Group, 2007. p. 32-33.

[7] Del Rey, R., J.A. Casas, R. Ortega. Impact of the ConRed program on different cyberbulling roles. Aggressive Behavior. 42 (2) 2016.123-35. DOI: 10.1002 / ab.21608;

[8] S. Hinduja, J. W. Patchin. Bullying, cyberbullying, and suicide. Archives of Suicide Research, 14 (3) (2010) 206-21. DOI: 10.1080 / 13811118.2010.494133.

[9] M. Naarttijärvi, Balancing data protection and privacy - The case of information security sensor systems, Computer law & Security review, volume 34 (5) (2018) 1019-1038. DOI: https://doi.org/10.1016/j.clsr.2018.04.006

[10] J. Wojniak, M. Majorek, Children and ICT European initiatives and policies on protecting children online // Universal journal of educational research, 4 (1) 2016 131-136, DOI: 10.13189 / ujer.2016.040116.

[11] C. Chang. Internet safety survey: who will protect the children? Berkeley technology law journal. Annual review of law and technology, 25 (1) (2010) 501-527. Published by: University of California, Berkeley, school of law. DOI: 10.15779 / Z38HQ3D

[12] S. Livingstone, J. Davidson, J. Bryce, C. Haughton, A. Nandi. Children's online activities, risks and safety: a literature review by the UKCCIS Evidence Group, pp. 41-42, 2007ю

[13] E. Magkos, E. Kleisiari, P. Chanias, V. Giannakouris-Salalidis. Parental control and children's internet safety: the good, the bad and the ugly, 2014, 18 p.

[14] Model Law on the Protection of Children from Information Harmful to Their Health and Development ". Adopted in St. Petersburg on 03.12.2009 by Resolution 33-15 at the 33rd plenary session of the Interparliamentary Assembly of CIS Member States. Newsletter. Interparliamentary Assembly of States - members of the Commonwealth of Independent States, 46 (2010) 190 - 228

[15] Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet (Adopted by the Committee of Ministers of the Council of Europe on 20 February 2008 at the 1018th meeting of the Ministers' Deputies. http: //childcentre.info/public/protecting_children_on_the_internet.pdf

[16] Recommendation CM / Rec, 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, 2007.

[17] Cybersecurity strategy. The Government of Japan, 2015. https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

[18] Children's online privacy protection rule ("COPPA"). Children's Online Privacy Protection Act of 1998, 15 U.S., paras. 6501-6505. https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim