

Ensuring children's online safety in Kazakhstan: balancing protection from harm with rights to information access

Kuanysh Zhumabekova

Doctoral Student, Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Makan Esbulatov, Almaty, Republic of Kazakhstan
kuanyshzhumabekova40@gmail.com

Zhanar Kegembayeva

Professor, Kazakh Ablai Khan University of International Relations and World Languages, Almaty, Republic of Kazakhstan
zhanarkegembayeva12@outlook.com

Azina Otarbayeva

Professor, Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Makan Esbulatov, Almaty, Republic of Kazakhstan
azina.otarbayeva20@proton.me

Abzal Yelubayev

Associate Professor, Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Makan Esbulatov, Almaty, Republic of Kazakhstan
A_Yelubayev97@hotmail.com

Syrym Abizhanov

Associate Professor, Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Makan Esbulatov, Almaty, Republic of Kazakhstan
AbizhanovSyrym@protonmail.com

DOI: 10.58866/FMY6192

Abstract

The relevance of scientific research is due to a number of problems that arise in the field of protecting children from the spread of harmful information on the Internet. An increase in the level of crimes against children of a sexual nature, a sharp jump in the level of suicides, the manifestation of various types of addiction, ranging from gambling and ending with drugs, is a consequence of such an influence. The purpose of this work is to study the current legislation of Kazakhstan in this area and to find gaps in its functioning, as well as to propose an effective mechanism for the legal regulation of protecting children from harmful information on the Internet, taking into account international legal experience. The basis of the methodological approach is the dialectical method, which was used to study the legal regulation in the sphere of the use of Internet resources by minors, the analysis method was used to study the legal acts in this area. The results of this study are a comparative analysis of the legal regulation of the protection of children from harmful content on the example of the legal experience of Australia, Britain, Germany in comparison with Kazakhstan. Also, the legislation on the protection of children from harmful information in Kazakhstan was analysed in detail and the main gaps in the existing acts were identified. The study outlines possible ways to develop national legislation through the adoption of new regulations, the purpose of which should be to increase control over the privacy of minors' data, restrict and block content that explicitly contains scenes of a sexual nature or violence, restrict advertising content, restrict access to information depending on from age. Also, it is going about the creation of special departments to regulate and control the issue of harassment and bullying, namely the Special Commissioner for Cyberbullying. The results obtained in this study can be used to protect children and prevent illegal actions against minors online at the legislative and local levels.

Keywords

Minors – sexual violence – the rights of the child – the right to access to information – social media

Introduction

Availability, openness of information, and limitless possibilities are not only the benefits of modern civilization, but also entail quite serious consequences for certain segments of the population, especially the most vulnerable among them – children. According to O. Ivanova¹ every child, whose consciousness has not yet been sufficiently formed, is vulnerable in the network and is influenced by any type of information. According to statistics, every third Internet user has not reached the age of majority, and the biggest problem in the network, which has become a global civilian security issue, is child sexual abuse on the Internet. According to Global Threat Assessment², among 54% of Internet users (aged 18-20), everyone has experienced at least one problem of online sexual violence. V.N. Strelka³ believes that the reason for this is content that denies family values, the purpose of which is the promotion of sexual relations, and coercion to acts of a sexual nature.

However, sexual abuse is not the only problem that minors face when using the Internet. Most often, it is also cyberbullying, which poses a direct threat to children's health, both psychological and physical, viewing inappropriate content that contains scenes of a sexual or violent nature, the emergence of gambling addiction, and as a result, problems at home, with learning and social adaptation⁴. Zh. Turmanova⁵ sees the reason in the very low digital competence of the younger generation. It is going about the fact that, in her opinion, the Internet is increasingly perceived as a way of entertainment, and not a tool for finding information, which leads to the massive use of gadgets around the clock. E.A. Skobina and E.S. Burdinskaya⁶ point out that in addition, the real problem is the latency of crimes against children on the Internet. The inability to hold the "virtual person" accountable creates more and more opportunities for the generation of various types of fraud, forms of exploitation and deception of children.

Ensuring information security is a vector of direction in the public policy of many countries. Republic of Kazakhstan (RK) confidently follows the trend towards protecting adolescents from dangerous information on the Internet, as well as their rights and freedoms, taking into account the safe use of digital technologies. The main confirmation of this was the adoption of the Law of the Republic of Kazakhstan No. 169-VI ZRK "On the protection of children from information harmful to their health and development"⁷, submitted for consideration by a group of deputies of the Parliament of the Republic of Kazakhstan. The purpose of the law was precisely to ensure the protection of the rights and interests of the child in accordance with international

1 Ivanova, O. (2021). Legal regulation of child protection regarding the negative impact of social networks and the Internet. *Knowledge of European Law*, 2:90-94.

2 Global Threat Assessment. (2021). <https://www.weprotect.org/wp-content/plugins/pdfjs-viewer-shortcode/pdfjs/web/viewer.php?file=/wp-content/uploads/Global-Threat-Assessment-2021.pdf&dButton=true&pButton=true&oButton=false&sButton=true#zoom=0&pagemode=none>.

3 Strelka, V.N. (2019). Human rights on the Internet: protecting of minors on the Internet. <https://goo.su/kaGUam>.

4 Zhanuzakova, L.T., Visarigova, A.Sh.-A. (2018). Legal framework for protecting children from information harmful to their health and development. <https://articlekz.com/article/20287>.

5 Turmanova, Z. 2019. Children in the information society: An information and methodological guide. Astana: IP Bika.

6 Skobina, E.A., Burdinskaya, E.S. (2018). Problems of protecting children in the Internet space. In: Proceedings of IV International Scientific Conference "Topical Issues of Legal Sciences" (pp. 58-62). Chita: Molodoy uchenyy.

7 Law of the Republic of Kazakhstan No. 169-VI ZRK "On the protection of children from information harmful to their health and development". (2018). <https://adilet.zan.kz/rus/docs/Z1800000169>

law⁸.

A number of scientists paid attention to the study of this topic. Zh. Turmanova⁹ studied the problem of developing the digital competence of children and parents, taking into account the identification of all the risks of the Internet. L.T. Zhanuzakova and A.Sh.-A. Visarigova¹⁰ studies the issues of protecting children from destructive information directly distributed in social networks. E. Pearl Ben-Joseph¹¹, who studied the issues of combating the manifestation of cyberbullying and ways to resolve the problem. Despite a fairly large array of information, the issue of real safety and protection of children on the Internet is still open. This is especially true with the spread of social networks such as YouTube, Instagram, TikTok. However, speaking about the regulation of the Internet sphere, authors agree with the opinion of L.A. Bukalerova and A.V. Ostroushko¹² that protection should take place precisely within the framework of international law, without violating the right of the child to access information and without depriving him of the right to freedom of speech, but creating for him a protective barrier against any malicious encroachment.

The purpose of the study is to analyse national legislation in the Internet sphere, as well as to create an effective mechanism for the legal regulation of protecting children from harmful information on the Internet by taking into account national legal experience while respecting the child's right to freedom of speech on the Internet. Also, it is worth outlining the directions for future research, including the issue of regulating the blocking of malicious content, protecting the right to freedom of speech and expression on the Internet, legal regulation for the distribution of harmful content for children, as well as the implementation of effective legislation regarding the protection of children from harmful information directly on the Internet.

Materials and Methods

The key research methods used include the dialectical method, comparative legal method, formal legal method, and the method of analysis. The dialectical method enabled a nuanced analysis of the various perspectives around children's internet use and online risks. The thesis of benefits was weighed against the antithesis of harms. Synthesizing these views allowed a balanced understanding of this complex issue. The comparative legal method facilitated a detailed comparison of Kazakhstan's legal framework to international models from Australia, the UK and Germany. Specific laws and regulations were analysed side-by-side to identify gaps in Kazakh law and potential improvements based on leading global approaches. The formal legal method supported a rigorous assessment of establishing legal norms around online content controls. The feasibility and implications of different regulatory mechanisms were examined, considering issues of scope, definitions, implementation, and enforcement.

8 Dossier on the draft law of the Republic of Kazakhstan "On the protection of children from information harmful to their health and development". (2015). https://online.zakon.kz/Document/?doc_id=31247960&doc_id2=31249501#activate_doc=2&pos=2_3;-100&pos2=0;0.

9 Turmanova, Z. (2019). Children in the information society: An information and methodological guide. Astana: IP Bika.

10 Zhanuzakova, L.T., Visarigova, A.Sh.-A. (2018). Legal framework for protecting children from information harmful to their health and development. <https://articlekz.com/article/20287>.

11 Pearl Ben-Joseph, E. (2022). Online Safety. <https://kidshealth.org/en/parents/net-safety.html>.

12 Bukalerova, L.A., Ostroushko, A.V. (2020). On the international legal and national regulation of relations to ensure the information security of children and minors. <https://lexed.ru/obrazovatelnoe-pravo/analitika/issledovaniya/o-mezhdunarodno-pravovom-internationalnom-regulirovanii-otnosheniy-po-obespecheniyu-informatsionnoy-be/>.

This study explores the problem of potentially dangerous information impacts on underage internet users in Kazakhstan and options for legal regulation. Attention is given to associated risks and consequences of malicious online content spread. Through the analytical method, the research analysed the national legislation of Kazakhstan, namely the Law of the Republic of Kazakhstan No. 169-VI ZRK “On the protection of children from information harmful to their health and development”¹³, the Law of the Republic of Kazakhstan No. 118-VII ZRK “On the introduction of amendments and additions to certain legislative acts of the Republic of Kazakhstan on the protection of the rights of the child, education, information, and informatization”¹⁴, the Law of the Republic of Kazakhstan No. 345 “On the rights of the child in the Republic of Kazakhstan”¹⁵. and also, partially Criminal Code of the Republic of Kazakhstan¹⁶. The precise language, provisions, definitions, and regulations were analysed to determine the current state of Kazakh law regarding online protections for minors.

In addition, the study utilized a rigorous legal methodology to examine the ways in which legal norms are established to communicate information online, both directly and through social media. The study carried out a comparative analysis of national legislation with the legislation of other countries, namely Australia, Britain, and Germany, in order to study the problem in the Republic of Kazakhstan and the world. These countries were chosen for comparative analysis because they have some of the most comprehensive and robust legal approaches globally when it comes to protecting minors online and regulating internet content¹⁷. Each country also has specialized agencies, codes, laws, or acts focused specifically on this issue. Comparing Kazakhstan legislation against models from world-leading countries allows identifying gaps and options to strengthen Kazakh laws and policies. The theoretical basis of the research is the research of scientists, as well as data and research of the United Nations International Children’s Emergency Fund (UNICEF), including sociological statistics of the Republic of Kazakhstan.

The desk research was carried out in three stages, the first of which encompassed the study of the theoretical base, including the regulatory legal acts of the Republic of Kazakhstan and other countries. Also, at this stage, the relevance of the stated topic, the main issues, the purpose of the work were formulated, and research methods were studied. The second stage is a process of studying the problem of protecting children from harmful information on the Internet, including sociological research on the territory of Kazakhstan. At this stage, the main risks that the minor faces, as well as the forms in which they manifest themselves, are formulated and deduced. In addition, the national legislation in the field of legal regulation of the protection of children’s rights and the legislation of other countries were studied and analysed. The third stage was the final one in this study, which formulated the problems faced by the national legislator of the Republic of Kazakhstan, proposed changes to the national legislation, and spelled out ways to develop this topic in the legal dimension.

13 Law of the Republic of Kazakhstan No. 169-VI ZRK “On the protection of children from information harmful to their health and development”. (2018). <https://adilet.zan.kz/rus/docs/Z1800000169>

14 Law of the Republic of Kazakhstan No. 118-VII ZRK “On the introduction of amendments and additions to certain legislative acts of the Republic of Kazakhstan on the protection of the rights of the child, education, information, and informatization”. (2022). <https://adilet.zan.kz/rus/docs/Z2200000118>

15 Law of the Republic of Kazakhstan No. 345 “On the rights of the child in the Republic of Kazakhstan”. (2002). https://adilet.zan.kz/eng/docs/Z020000345_.

16 Criminal Code of the Republic of Kazakhstan. (2014). https://online.zakon.kz/document/?doc_id=31575252#sub_id=0.

17 Lee, S., Chung, S., Lee, E. (2023). Globalization of the public relations agency industry: a country-level analysis of global public relations agencies and environmental factors. *Journal of Communication Management*, 27(1), 21-34.

Discussion of the impact of harmful internet content on children and adolescents

The Internet is clearly an achievement of modern society, which has brought unlimited opportunities for development and growth in all areas. However, despite this, one should not forget about the huge risks that modern humanity faces every day, using the benefits of information. The benefits and harms of the use of information technology have long been topic No. 1 for discussion in all spheres of life, from scientific discussions to plenary sessions of the highest legislative bodies of states¹⁸. However, despite such great popularity and a growing desire to find an effective way to resolve this issue, the problem is only gaining momentum every day, especially for the most vulnerable – children. The reason for this growth is due to the fact that children spend more of their time on the Internet. So, according to statistics, every half a second around the world at least one child accesses the Internet¹⁹.

According to UNICEF data²⁰, the frequency of using a computer and the Internet by children aged 6 to 15 in 2015 in Kazakhstan was 73.9% – at least once a day and 21.9% – at least once a week, but not every day. At the same time, 72.4% of users are children from 11 to 15 years old, and 38.3% are children from 6 to 10 years old²¹. Of course, the Internet allows children, but only with proper use, to open their horizons and express themselves, which contributes to better development and formation of a personality. Social networks open up new forms of communication and access to content, as well as the exercise of their rights to access information, but at the same time it can equally lead to loss of mental health, and in some cases even death, through the influence of malicious information, provoking issues such as cyberbullying, sexual violence, “trolling”, intimidation, or blackmail²².

E.A. Skobina and E.S. Burdinskaya²³ points to the need for legal regulation of such a concept as “trolling”, as well as its criminalization. Indeed, trolling, in fact, does not exist in national legislation and does not entail prosecution, although it is nothing more than a form of bullying. In fact, speaking in legal language, “trolling” can be qualified as an insult to the person, slander, which can harm both the psychological and physical health of the child, especially when it comes to insults on any social grounds. Often, among teenagers, trolling takes on a particular scale of cruelty and can even lead to acts such as suicide or mutilation. Thus, according to UNICEF statistics, more than a third of adolescents worldwide are subjected to cyberbullying on an ongoing basis, and one in five of them do not attend educational institutions for this reason. And most often, a similar problem occurs in social networks or forums, as well as in the exchange of messages and comments, which in consequence leads to self-harm, and sometimes even to suicide²⁴. The legal regulation of such actions on the Internet, as well as the establishment of criminal liability for them in the event of damage to the health or growth of a child, would definitely contribute to a decline in the spread trend. As for the question of actually

18 Tarasenko, O. (2018). The Concept of Illegal Content on the Internet. Law Journal of the National Academy of Internal Affairs, 8(1), 61-70.

19 Protecting children online. (2022). <https://www.unicef.org/protection/violence-against-children-online>.

20 Ibid.

21 Oksamitnyi, Yu.V., Aidapkelov, N.S. (2017). Children of Kazakhstan: Statistical compendium. Astana: Statistics Committee of the Ministry of National Economy of the Republic of Kazakhstan.

22 Turmanova, Z. (2019). Children in the information society: An information and methodological guide. Astana: IP Bika.

23 Skobina, E.A., Burdinskaya, E.S. (2018). Problems of protecting children in the Internet space. In: Proceedings of IV International Scientific Conference “Topical Issues of Legal Sciences” (pp. 58-62). Chita: Molodoy uchenyy.

24 Protecting children online. (2022). <https://www.unicef.org/protection/violence-against-children-online>.

identifying such situations and bringing them to justice, it is worth talking about the creation of such a body as the Special Commissioner for Cyberbullying, whose functions would be to identify such incidents and eliminate them.

The greatest resonance is caused by the problem of sexual violence on the Internet, the root cause of which is precisely malicious information. The inability of children to filter information allows criminals to easily find their victims, forcing them to have sexual contacts, distribute sexual content, or commit sexual crimes against third individuals. In addition, such actions can take place live. According to O. Ivanova²⁵, the category of children most susceptible to sexual exploitation is those who grow up in dysfunctional families, on the verge of poverty, as well as in conditions of social inequality. Of course, external factors such as the social environment, upbringing, family relationships have a huge impact on the growth and formation of the child's personality. And most often, problems in real life are transformed into the "online life" of a teenager. It is going about sexual attacks, threats, and lack of sexual education, which become harbingers and concomitant factors of problems on the Internet.

However, when it comes to children's exposure to harmful information on the Internet, including sexual content, it is not worth considering only socially disadvantaged families. According to social studies, the most common victims of sexual exploitation are minors between the ages of 14 and 17, the reason for which is their propensity for risks and dangerous behaviour due to the formation of personality in adolescence. In addition, studies show that there is no clear trend in the division into the conditions in which the child was brought up. Adolescents who became victims consciously made contact with the perpetrator, understanding the consequences of their actions²⁶. Y. Godyk²⁷ explains this trend through the peculiarities of behaviour depending on the age group. V.N. Strelka²⁸ adheres to a similar idea, pointing out that minors are exposed to harmful content not depending on external factors, but due to their psychological immaturity. They are not capable of recognizing and separating information into positive, harmful, or neutral, and therefore cannot refuse it.

One of the most common issues faced by children is the issue of privacy. Often, 90% of young users do not even think about the risks of posting private information and the consequences that may arise²⁹. While agreeing with the author's statement, it is important to note that such actions often remain in the shadow of parents and law enforcement agencies, and therefore do not have legal regulation in most of their cases³⁰. Data theft is one of the most common crimes on the Internet and is popular among both young and older users. Thus, the case of KU against Finland in 2008 can be an example of this. It was about the fact that on a dating site, on the account of a 12-year-old boy, an ad with sexual content was posted. According to the decision of the European Court of Human Rights, a violation of the right to privacy of the plaintiff was recognized in the context of the absence of a requirement from the state to the Internet provider regarding the

25 Ivanova, O. (2021). Legal regulation of child protection regarding the negative impact of social networks and the Internet. *Knowledge of European Law*, 2, 90-94.

26 Palfrey, J., Boyd, D., Sacco, D. (2010). *Enhancing child safety and online technologies. Final report of the Internet safety*. Durham: Carolina Academies Press.

27 Godyk, Y. (2011). Threats and risks to the safety of the children's and teenage Internet audience. *Vestnik Moscow*, 6, 115-129.

28 Strelka, V.N. (2019). Human rights on the Internet: protecting of minors on the Internet. <https://goo.su/kaGUam>.

29 Protecting children's rights in the digital world: an ever-growing challenge. (2014). <https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1>.

30 Kobzeva, S. (2017). Protection of the rights of minors from threats on the Internet. *Information Law*, 2:33-39.

person responsible for placing the advertisement³¹.

In addition, the problem of a global nature, the primary source of which is precisely the availability of confidential information, is human trafficking. The Internet is the most effective way to find victims for recruitment in the field of human trafficking for the purpose of sexual or labour exploitation of children. As E.A. Skobina and E.S. Burdinskaya³² points out, the lion's share of the problems lies precisely in the inability of the state to control the content that reaches teenagers. Unwanted pages with pornographic, exploitative, drug dealer content remain hidden from all but the "target audience" itself, and virtuality only contributes to the flourishing of such crimes without being held accountable for what they have done. The solution should not be exclusively legislative consolidation of restrictions on the dissemination of information, because not only the state is responsible for the growth and upbringing of a child. It is worth talking about comprehensive cooperation at all stages, from interaction in the family and school, ending with the settlement of situations by a special commissioner. Only with comprehensive work at all levels, proper parental control, high-quality digital education in educational institutions, preventive measures by law enforcement agencies, as well as an effective way of legal regulation of this issue, including the inevitability of criminal liability for the perpetrator of disseminating malicious content (including sexual exploitation, data theft, bullying), it will be possible to talk about the protection of the rights of the child from harmful information, while respecting his right to freedom.

It is worth noting, however, that while supervision and some content control may be necessary to protect minors, full cooperation at all levels should focus on education and empowerment rather than unsupervised monitoring and coercion. Parents are responsible for their children's Internet use, but schools also play a key role in providing digital literacy programs to teach youth how to make responsible online decisions and identify manipulation³³. Any legal regulations or special commissioners should only focus on serious crimes such as sexual exploitation, not over-regulation of broad swaths of speech and relationships. And the consequences of distributing genuinely harmful content should catch up with the perpetrators, not infringe on children's freedom to responsibly navigate the expanding digital world as they grow up.

D. Aikenova³⁴, in her studies of the state policy for the protection of children's rights in the Republic of Kazakhstan, often raises the issue of an increase in crimes against children, as well as the issue of social orphanhood with living parents. It is worth noting that the Internet is often the fuelling factor for such phenomena. The child's lack of ability to filter information and separate negative, neutral and positive opens the door for him to a stream of illegal or harmful content, like pornographic materials, materials calling for cruelty, racist accents, and provokes anti-social attitudes, the formation of anti-moral and anti-legal behaviour, and can also lead to the use of narcotic or other psychotropic substances, cause addiction or provoke an early sexual life, which brings irreparable harm to children's health and life. The authors would propose a multi-faceted approach to strike the right balance between these interests. First, parents/guardians

31 Protecting children's rights in the digital world: an ever-growing challenge. (2014). <https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1>.

32 Skobina, E.A., Burdinskaya, E.S. (2018). Problems of protecting children in the Internet space. In: Proceedings of IV International Scientific Conference "Topical Issues of Legal Sciences" (pp. 58-62). Chita: Molodoy uchenyy.

33 Maksymenko, O. (2021). Methodological foundations of the cognition of children's rights. Law Journal of the National Academy of Internal Affairs, 11(2), 13-17.

34 Aikenova, D. (2014). State policy for the protection of children's rights in Kazakhstan. Astana: L.N. Gumilyov Eurasian National University.

bear responsibility for reasonable supervision of younger minors while also allowing age-appropriate independence online and room to learn. Second, digital literacy education can help equip children to think critically about content and develop personal guidelines for evaluating risks/reliability as their judgment matures. This empowers their decision-making. Third, regulation should focus narrowly on restricting access to illegal, dangerous materials like those you listed, not wider censorship. As kids grow into teens able to better analyse content themselves, access could expand with more training on ethical digital citizenship. Additionally, specialized agencies and reporting channels can facilitate removing harmful content without over-policing legal speech. And enforcement should target distributors, not minor viewers lacking intent. This balanced framework allows nurturing children's critical thinking skills and self-directed exploration online, while sheltering from the most clearly damaging materials their developing judgment is unprepared to handle. It's a nuanced approach respecting both protection and healthy development into digital adulthood. There are certainly challenges, but with care and safeguards for all rights, positive solutions should be possible.

This contributes to the formation of anti-family foundations, the depreciation of socially important institutions, and the formation of an aggressive personality in a teenager. Such forms as stalking, encouraging self-harm, spreading hatred, phishing, and cyberbullying are also popular. An example of this is the case of a 10-year-old boy in Italy who, wanting to repeat a life-threatening "challenge" on TikTok, died while doing it, leading to tighter control of users whose age cannot be verified by the state³⁵. More and more recently there has been a trend towards the formation of digital literacy, thanks to which the child will be able to properly manage his right to access information. Many texts adopted by the European Council and other international organizations precisely imply this aspect of the use of the Internet by a minor user. That is, it is going about strict legislative regulation of a child's visits to certain resources, but about the ability of children to determine the type of information, understand negative content, as well as the ability to handle information of this kind.

Z. Turmanova³⁶ also speaks about the need to form digital competence in her writings. In her opinion, due to the growth of the child in a hyper-information society, it is required to ensure a "safe Internet", limiting it literally to parental control, and also instilling in the child a system of certain knowledge and views that contribute to critical thinking and the ability to filter, select, and compare information that is freely available on the web. Agreeing with the opinion of the researcher, it is worth adding that such programs should be fixed in the form of preventive mechanisms to combat the impact of harmful information on the child, both at the national and local levels. UNICEF adheres to a similar idea in its programs to protect children from harmful information³⁷. Such a strategy, of course, is correct to achieve the goal, because, with the interaction at all levels, it is really possible to create a safe space for children on the Internet. However, in addition to preventive programs, an important aspect is the legal regulation of the issue at the national level.

Gaps in legal protection and potential solutions to the threat of harmful online content to children in Kazakhstan

The Internet has ceased to be a tool for learning, but gradually moved into the risk zone, every day acquiring shades of danger for the child. So, this is confirmed by the statistics on the facts of cyberbullying

35 de Franssu, L.-V. (2022). Online dangers for children are rife. We must both pre-empt them and treat the consequences. <https://www.weforum.org/agenda/2022/06/child-safety-protection-internet/>.

36 Turmanova, Z. (2019). Children in the information society: An information and methodological guide. Astana: IP Bika.

37 Protecting children online. (2022). <https://www.unicef.org/protection/violence-against-children-online>.

in Kazakhstan, according to which about 80 thousand calls were recorded in 2021 alone³⁸. Cyberbullying, as well as the problem of child sexual abuse, as well as the manifestation of antisocial attitudes and anti-moral behaviour, are generated by the lack of control over the information that teenagers and children absorb on the Internet. Kazakhstan is a country with one of the highest rates of crime against children. Thus, according to the data of the Committee on Legal Statistics and Special Accounts of the Republic of Kazakhstan, since 2018 there has been an increase in the number of criminal offences against minors. If analysing the data for the first quarter, starting from 2018, it is possible to see a rapid growth trend, so in 2018, the number of offences was 773 (5.8%), in 2019 – 857 (10.9%), in 2020 – 672 (-21.6%, which indicates a significant drop, which is associated with the COVID-19 pandemic), in 2021 – 897 (33.5%)³⁹. The first positions are occupied by crimes directed against the person, as well as those directly motivated by the influence of harmful content on the Internet – sexual acts, including violent acts, incitement to suicide, and corruption of minors⁴⁰.

The problem is that Internet security regulation is one of the most controversial and complex in terms of legal regulation. The first and main problem is the lack of appropriate legislation that would regulate this particular sphere of legal relations in the Republic of Kazakhstan. The second factor is the almost incommensurable amount of information and the high coefficient of anonymity, which allows acting absolutely freely both within the legal and outside the legal framework, while not always bearing responsibility for one's actions. The fact is that it is possible to hold accountable for statements or acts on the Internet only if it contains a specific corpus delicti and is criminalized. However, even under such conditions, it is quite difficult to do this at a time of high latency of the crime, as well as the anonymity of the offender himself. A similar situation is typical for almost all countries, even such developed ones as the USA, Canada, Germany, France⁴¹.

As for countries that have just embarked on the path of development in the information sphere, the situation is much worse. In 2018 the Law of the Republic of Kazakhstan No. 169-VI ZRK “On the protection of children from information harmful to their health and development”⁴², was adopted which made significant adjustments in the field of protecting children from harmful information. The purpose of this law is to comprehensively regulate legal relations in the sphere of protecting children from harmful information disseminated by any media resources, including electronic ones. That is, the main task is to reduce the impact of any negative content that contains psycho-traumatic scenes, information with scenes of severe violence or sexuality, and also contributes to the formation of antisocial attitudes and behavioural parameters in society. This law is a new milestone in the history of Kazakhstani legislation and contains elements of the best foreign practices assimilated from the Model Law “On the protection of children from information that is harmful to their health and development”⁴³, adopted by the CIS (Commonwealth of Independent States) member states. It is going about such principles as the definition of understanding the age category of information products, the child's access to information, information products for children, age classification, the protection of children from information that is harmful to their health and development. The definition of these concepts at the legislative level gave impetus to the development of a real mechanism for protecting children from

38 Statistics of criminal offenses. 2022. https://data.egov.kz/datasets/govagencies?govAgencyId=AVPHItpZ1KT8iE_U7zeS.

39 Ibid

40 Ibid

41 Steshenko, V. (2019). Legal protection of the rights of children and adolescents and a safe information space. Kharkiv: Pravo.

42 Law of the Republic of Kazakhstan No. 169-VI ZRK “On the protection of children from information harmful to their health and development”. (2018). <https://adilet.zan.kz/rus/docs/Z1800000169>

43 Model Law “On the protection of children from information that is harmful to their health and development”. (2009). https://base.spinform.ru/show_doc.fwx?rgn=62134.

harmful information and contributed to the emergence of laws to protect against cyberbullying and other types of risks that the World Wide Web brings with it.

Thus, one of the positive aspects of this Law is the restriction of content for children according to their age group. It concerns about such information content as scenes of cruelty, violence, or a sexual nature that can provoke in the mind of a child potentially dangerous actions for his life and health, as well as form anti-social behaviour and anti-moral principles⁴⁴. The key moment is also defining age categories according to the Model Law “On the protection of children from information that is harmful to their health and development”⁴⁵. It is going about the literal categorization of the age of children and their access to a particular type of content. 6 categories of information products are distinguished, starting from universal – which is allowed for children of any age, followed by the category “up to 6 years old”, the category “from 6 years old”, the category “from 12 years old”, the category “from 16 years old” and category “from 18 years old” (which is prohibited for distribution to children). However, it is worth noting that such labelling of information content has a greater impact in areas such as television, print media, electronic and computer games, while almost completely leaving the Internet sector out of regulation. The fact is that web platforms, social networks, and other sites are practically not amenable to this legal regulation, except for some sites with sexual content, as well as a select number of social networks that require verification of the user’s age, thereby allowing adolescents to have access to any type of information without restriction⁴⁶.

Another gap in this law is the direct permission of the national legislator to distribute information products without an age category sign. So, according to Article 15 of the Law of the Republic of Kazakhstan No. 169-VI ZRK “On the protection of children from information harmful to their health and development”⁴⁷, the distribution of information products without an age category sign is not allowed on the territory of the Republic of Kazakhstan, except for Internet resources. Thus, the legislator, introducing into the field of legal regulation such important aspects as the age category for the dissemination of information, automatically eliminates the need for its control in the global network. The only aspect that affects the concept of the age category is the introduction of online games among children that contain the following plots:

- stories with content that provokes a child to a negative attitude towards the shortcomings of other people;
- stories that contain violent scenes or provoke aggressive actions; plots that are associated with virtual murders or any other mutilation of virtual characters;
- plots related to the infliction of psychological violence on a person, as well as severe moral and mental suffering; plots of a sexual nature, in which the genitals or sexual intercourse are naturalistically imitated;
- stories that can cause panic attacks, fear, or horror in children.

44 Zhyvko, Z., Rudyi, T.V., Senyk V. (2018). Technologies of Criminal Analysis in the Practice of Countering Cybercrime. Social and Legal Studios, 1(2), 40-47.

45 Ibid

46 Law of the Republic of Kazakhstan No. 169-VI ZRK “On the protection of children from information harmful to their health and development”. (2018). <https://adilet.zan.kz/rus/docs/Z1800000169>

47 Ibid

Thus, despite efforts to protect children's rights to safety and to protect them from harmful information, in accordance with the Convention on the Rights of the Child⁴⁸, as well as Law of the Republic of Kazakhstan No. 345 "On the rights of the child in the Republic of Kazakhstan"⁴⁹, this law does not provide for real mechanisms of protection against the spread of malicious information (pornographic materials, content inciting violence or cruelty, information promoting antisocial/dangerous behaviours, materials that could encourage suicide or self-harm etc.) on the Internet. It is worth talking about the introduction of a real preventive mechanism at the legislative level, which would limit children's access to this type of content and secure their growth and development, in addition, it is worth thinking about changes in the direction of social policy, which could be guided by UNICEF policy in this direction. The solution could be social programs aimed at creating a digitally literate society, the purpose of which is to use the Internet and media resources in order to solve vital issues, which UNICEF mentions in its programs to protect children from harmful information⁵⁰.

Thus, according to the organization, the reaction should be coordinated and simultaneously go both at the national and global levels. The topic concerns about government investment programs, the purpose of which is to form a media-literate society, to increase the level of knowledge and awareness of the child about the risks on the Internet, and the ability to distinguish between harmful information and ways to deal with it. And at the same time, simultaneously strengthen legal control over the dissemination of information for minors on all media resources, including print media, television, digital resources, cooperating with technology companies in the direction of creating safe digital products⁵¹. Such a strategy, of course, is correct to achieve the goal, because with interaction at all levels, it is really possible to create a safe space for children on the Internet. However, in addition to preventive programs, an important aspect is the legal regulation of the issue at the national level⁵². It is logical to comparison the national practice of legal regulation in comparison with international experience.

It is important to note the experience of Australia, which created the world's first independent government agency "eSafety" in 2015, which acts as the Children's Electronic Safety Commissioner, especially working through all the risks and harms that they face in the digital world⁵³. The agency's priority in its functioning is to direct efforts to ensure that social networks, messaging services, games, videos, and various applications adhere to measures to ensure Internet safety for all categories of the population. But the main aspect is the fact that "eSafety" has the power under the law to require providers and suppliers of information to report on the dissemination of information in order to increase the level of transparency of activities in the information space⁵⁴.

The United Kingdom is also paying quite a lot of attention to this aspect, as well as adopting a special

48 Convention on the Rights of the Child. (1989). https://www.un.org/ru/documents/decl_conv/conventions/childcon.shtml.

49 Law of the Republic of Kazakhstan No. 118-VII ZRK "On the introduction of amendments and additions to certain legislative acts of the Republic of Kazakhstan on the protection of the rights of the child, education, information, and informatization". (2022). <https://adilet.zan.kz/rus/docs/Z2200000118>

50 Protecting children online. (2022). <https://www.unicef.org/protection/violence-against-children-online>.

51 Ibid

52 Demydenko, V. (2018). The Principles of Application of Legislation by Local Government in the Field of Cybersecurity. Law Journal of the National Academy of Internal Affairs, 8(1), 141-153.

53 eSafety's purpose is to help safeguard Australians at risk of online harms and to promote safer, more positive online experiences. (2022). <https://www.esafety.gov.au/about-us/who-we-are/regulatory-schemes>.

54 Ibid

“Age-Appropriate Design Code”⁵⁵. This is a kind of code, which is aimed at regulating the dissemination of information for children on the Internet. It is going about such aspects as privacy, inappropriate advertising, as well as ways to keep children online for a long period of time. By adopting the Code in 2021, the United Kingdom government has set aside 1 year for companies to implement all the rules. Thus, according to it, companies that are providers of any information services for children undertake to create design services in accordance with their age and interests; maintain a high level of confidentiality of personal data by default; protect underage users from any information, including advertising, that could induce them to sexual exploitation; turn off location services that can track their location; file reports with the British High Commissioner on the data companies collect from children. This Code has had the most impact on major information service companies such as YouTube, TikTok, and Instagram. For example, YouTube has blocked the ability to target advertising services to children, TikTok has limited the sending of notifications after 9 p.m., and Instagram prohibits messaging between adults and minors that the latter are not subscribed to on the social network. Subsequently, these restrictions affected not only Britain, but users in around the world. It is important to note that non-compliance with the rules of the Code entails potential liability in the form of fines of up to 4% of the company’s profits, which is a deterrent to fulfilling all conditions⁵⁶.

The German government has also placed great emphasis on protecting children online, obliging providers to protect them from sexual exploitation, cyberbullying, financial fraud, and data theft. In 2020, the Bundestag adopted amendments to the Youth Protection Act, amending the regulation of protecting children from harmful information on the Internet⁵⁷. The newly adopted law aims to counter the risks for children and adolescents online, including social platforms, in order to protect them from potentially inappropriate content and to protect personal data⁵⁸. The change directly affected:

- Internet services undertake to apply appropriate preventive measures to prevent the dissemination of harmful information to minors;
- age restrictions for computer games and films are being modernized;
- suppliers are required to monitor and control and remove any information that indicates cyberbullying;
- provides for the application of legal liability for evasion of the law.

A similar form of legal regulation can be introduced into the national legislation of Kazakhstan. Thus, the existing law on the protection of children should be supplemented by a separate legal act, the purpose of which is precisely to regulate the issue of protecting children on the Internet from harmful information. The law should include a list of restrictions:

55 Introduction to the Age-Appropriate Design Code. (2021). <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>.

56 Protecting children’s rights in the digital world: an ever-growing challenge. (2014). <https://www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1>.

57 Giffey, F. (Ed.). (2020). *Jugendschutz – verständlich erklärt*. Berlin: Bundesministerium für Familie, Senioren, Frauen und Jugend. [in German].

58 Mentukh, N., Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*, 1(1), 4-17.

The use of exclusively children’s design, taking into account the age categories prescribed in the Law of the Republic of Kazakhstan No. 169-VI ZRK “On the protection of children from information harmful to their health and development”⁵⁹, completely excluding images of a sexual nature, violent death, as well as images that can provoke attacks of fear or panic in children.

- Increased control over sensitive data that all users under the age of 18 leave online.
- Age control when accessing content that could potentially be dangerous to children.
- Blocking children’s access to web resources that contain explicit content of a sexual nature, scenes of violence, or extreme cruelty.
- Automatic blocking of advertising content in the segment of the children’s audience.

Such a normative legal act should provide for liability for evasion of compliance with the norms, as well as administrative punishment if such actions did not cause damage to the life and health of the child. Otherwise, it is worth discussing criminal liability.

According to L.-V. de Franssu⁶⁰, an integral element of the mechanism for protecting children from harmful information on the Internet is the presence of a government hotline that can remove content that violates the rights and interests of the child from any websites, social networks, or other platforms. Examples of such bodies are Telefono Azurro in Italy, the Internet Watch Foundation in Britain, or the National Centre for Missing and Exploited Children in the United States. This is a kind of trust or safety line that every child who has become a victim of an online crime caused by malicious information can turn to. This practice can be implemented in the legislative plane of Kazakhstan, because after the adoption of the law “On the Protection of Children’s Rights”, there is an opportunity to work out various programs at all levels. Also, the formation of a special department under law enforcement agencies, whose functions will include monitoring the observance of the rights of the child on the Internet and protection from malicious information, may become a kind of version of the British and American “Hot Lines” in Kazakhstan. However, in addition to preventive programs, it is worth considering such formats of legal regulation as the removal or blocking of potentially unwanted material. Internet service providers, social media platforms, website administrators and a specialized government agency should be legally required to remove or block inappropriate, dangerous material for children from any digitally accessible spaces, including websites, forums, apps, and message boards hosting such content. Companies enabling digital access should take responsibility for content takedowns, complemented by public oversight and enforcement from a dedicated government body monitoring online platforms for inappropriately accessible materials⁶¹.

Considering international experience, it is important for Kazakhstan to borrow legal regulation in the field of cyberbullying. Cyberbullying among teenagers ranks first in Kazakhstan. According to the sociological data

59 Law of the Republic of Kazakhstan No. 169-VI ZRK “On the protection of children from information harmful to their health and development”. (2018). <https://adilet.zan.kz/rus/docs/Z1800000169>

60 de Franssu, L.-V. (2022). Online dangers for children are rife. We must both pre-empt them and treat the consequences. <https://www.weforum.org/agenda/2022/06/child-safety-protection-internet/>.

61 Rafalskyi, M. (2023). Offences in the sphere of virtual assets turnover and analysis of their qualification. Law Journal of the National Academy of Internal Affairs, 13(3), 65-76.

of the National Centre for Public Health of Kazakhstan, 11% of children aged 10 to 15 have been cyberbullied at least once online, directly on social platforms. In 2021 alone, about 80,000 reports of cyberbullying were recorded⁶². It is worth noting that after acceptance on May 3, 2022, of the Law of the Republic of Kazakhstan No. 118-VII ZRK “On the introduction of amendments and additions to certain legislative acts of the Republic of Kazakhstan on the protection of the rights of the child, education, information, and informatization”⁶³, the solution of the problem moved from the dead point. Thus, the bill defines such concepts as bullying and cyberbullying. In addition, at the level of the Ministry of Information and Social Development, negotiations are underway with large technology companies, namely Facebook, Instagram, to apply preventive measures and protect children from online bullying. The idea is that a social network and electronic communications services whose audience has more than 100,000 users should appoint a representative who will cooperate with the Ministry of Information on identifying cyberbullying incidents and counteracting them. Thus, in case of detection of a case of cyberbullying, a representative of a particular social network, together with the Ministry of Information, must take appropriate measures within three days⁶⁴. A logical continuation of this reform would also be the appointment of a Special Commissioner for Cyberbullying, who could coordinate the activities of all representatives with the right to demand accountability.

It is worth noting that there are quite a lot of discussions regarding the mentioned Law. Some human rights activists say that such a regulation is only a way to tighten censorship on the Internet, limiting the right to freedom of speech and expression, replacing the notion of protecting children from harmful information with the desire to remove disadvantageous content⁶⁵. However, before the adoption of this law, the national law of Kazakhstan did not at all provide for such concepts as “bullying”, intimidation, harassment, and, accordingly, responsibility for such acts was not applied. The only similar crimes are such acts as driving to suicide, threatening to kill and slander. The application of the law led to amendments to the Criminal Code of the Republic of Kazakhstan⁶⁶, introducing the paragraph in Part 2 of Art. 105: through the use of telecommunications networks, including the Internet. Thus, providing for direct criminal liability for incitement to suicide by harassment or intimidation online, enabling law enforcement agencies to apply not only preventive measures, but also bring the perpetrators to criminal responsibility.

So, in summary, while historically Kazakh law lacked clear frameworks for classifying and prosecuting abusive behaviours online against children, the latest reforms have:

- Codified definitions covering bullying and cyberbullying
- Set punishments for online provocation/incitement to suicide
- Enabled law enforcement agencies to apply criminal charges to perpetrators of severe cases of youth cyber harassment and its tragic consequences.

62 Every fifth Kazakhstan teenager becomes a victims or participants of bullying. (2020). <https://hls.kz/archives/20567>.

63 Law of the Republic of Kazakhstan No. 118-VII ZRK “On the introduction of amendments and additions to certain legislative acts of the Republic of Kazakhstan on the protection of the rights of the child, education, information, and informatization”. (2022). <https://adilet.zan.kz/rus/docs/Z2200000118>

64 Titova, A. (2022). Cyberbullying is a real problem or a reason for tightening censorship. <https://goo.su/XTwd486>.

65 Aikenova, D. (2014). State policy for the protection of children’s rights in Kazakhstan. Astana: L.N. Gumilyov Eurasian National University.

66 Criminal Code of the Republic of Kazakhstan. (2014). https://online.zakon.kz/document/?doc_id=31575252#sub_id=0.


This signifies key progress in providing legal accountability regarding online bullying and related attacks against young people in Kazakhstan.

Conclusions

While the Internet undoubtedly provides significant opportunities for children, including enhancing their creativity and access to information, it simultaneously exposes them to risks such as cyberbullying, sexual exploitation, and exposure to inappropriate content. This dual nature of the Internet necessitates a balanced approach that acknowledges both its benefits and dangers. It's crucial to recognize that children vary in their ability to discern information online. This variation often stems from differing educational backgrounds and personal experiences. Therefore, a one-size-fits-all approach to online safety may not be effective. Tailored strategies that take into account these differences are essential.

The role of national legislators is pivotal in navigating the balance between protecting children online and preserving democratic values like freedom of speech and access to information. The challenge lies in implementing regulations that safeguard children without overstepping into censorship or infringing upon democratic freedoms. The United Nations Convention on the Rights of the Child should be the guiding framework for any legislation. However, the specifics of which convention or provisions are being referred to must be clearly stated for clarity and accuracy. Alongside the issues of content and access, the right to privacy and data protection, especially for minors, is a critical area that needs emphasis. Legislation should address how children's data is collected, used, and protected online.

Developing an effective legal framework requires a thorough understanding of the digital landscape and its impact on children. The legislation should be precise, enforceable, and adaptable to the rapidly evolving nature of the Internet. Additionally, it should be complemented by educational and preventive programs to build an information-competent society, empowering children to understand their rights and responsibilities online. While recognizing the myriad benefits of the Internet for children, it's imperative to develop nuanced and effective strategies to protect them from its potential harms. This requires a collaborative effort involving legislators, educators, parents, and the children themselves, underpinned by the principles of democracy, education, and respect for children's rights.



This article was published by the Security and Human Rights Monitor (SHRM).
www.shrmonitor.org

Security and Human Rights (formerly Helsinki Monitor) is a journal devoted to issues inspired by the work and principles of the Organization for Security and Cooperation in Europe (OSCE). It looks at the challenge of building security through cooperation across the northern hemisphere, from Vancouver to Vladivostok, as well as how this experience can be applied to other parts of the world. It aims to stimulate thinking on the question of protecting and promoting human rights in a world faced with serious threats to security.

Netherlands Helsinki Committee
Het Nutshuis
Riviermarkt 4
2513 AM The Hague
The Netherlands

© Netherlands Helsinki Committee. All rights reserved.

www.nhc.nl