

LEGAL PROTECTION OF VULNERABLE GROUPS

Research Article

DOI: 10.17803/2713-0533.2023.1.23.157-178

The Need for the Development of a Constitutional and Legal Model for Ensuring the Information Security of Minors

Oleg Yu. Rybakov, Olga S. Rybakova

Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

Abstract: Based on the analysis of the main risks of the information environment for minors, the authors substantiate the need to form a constitutional and legal model for ensuring the information security of minors. The authors represent their understanding of the concepts of “threat,” “challenge,” “danger,” which are close in a categorical series with the concept of “risk,” is presented, and propose their definitions of the concepts of “information security,” “security worldview.” The main goals for ensuring the information security of minors are both security and the creation and maintenance of the most favorable conditions for the adaptation of a minor to the information environment of modern society, which contributes to his personal development, improvement of spiritual, moral, intellectual, creative abilities and self-realization, subject to minimization (and exclusion) of possible risks and threats to life, health and its comprehensive development. The elemental composition of the constitutional and legal model of information security of the child is presented, the formation of which is associated with the national model for the protection of the rights and freedoms of minors. The right to information security of minors comes from the meaning

and spirit of the Constitution, as it ensures the implementation of other constitutional rights and freedoms of minors.

Keywords: law; the right to safety; constitutional model; legal modeling; information security of a minor; constitutional rights and freedoms of minors

Cite as: Rybakov, O.Yu. and Rybakova, O.S., (2023). The Need for the Development of a Constitutional and Legal Model for Ensuring the Information Security of Minors. *Kutafin Law Review*, 10(1), pp. 157–178, doi: 10.17803/2713-0533.2023.1.23.157-178.

Contents

I. Introduction	158
II. Safety and Informational Security of Minors	160
III. Risk Classification of Information Security of Minors	161
IV. Discussion on the Necessity for the Constitutional and Legal Model Development for Ensuring the Information Security of Minors	170
V. Conclusion	175
References	176

I. Introduction

Minors are active participants of information relations. It is difficult to imagine a child's development outside of information that acts as a source of knowledge, a means of a mindset development, a condition for his socialization, intellectual, spiritual, psychological development, promotes various forms of communication. On the one hand, the information space carries a positive impulse for the development of minors, on the other, it can have a negative impact.

The global information space provides an opportunity for unlimited access to a wide range of information resources, thereby ensuring the realization of the human right to free access to information.

According to Illaria Bachilo, information is “a characteristic of the surrounding world perceived and understood by a person in all its diversity that arises in the process of cognition of the latter and allows, on the basis of cognition and measurement of the properties of objects,

phenomena, processes, facts and their reflection in various forms of perception, to distinguish their signs, elements, meanings and establish connections and the dependence of the whole variety of manifestations of the material, spiritual, ideological world” (Bachilo, 2016, p. 25).

Information, from the point of view of its essential characteristics, is a reflection of the existing reality in the human mind, expressed in symbolic form for the purpose of further orientation and adaptation in life (Kuznetsov et al., 2020, p. 37). In our opinion, information is the data about the surrounding reality, conditioned by human existence that changes in the process of human life. In other words, information is a collection of data about the surrounding reality, reflected in the mind of the individual. For an individual participant in information relations, only the information that is received and perceived (or not perceived) by his consciousness matters. Thus, the value of the information received is determined based on the characteristics of a particular subject of its consumption. The same information can be useful for one person and negative or even harmful for another.

The information that a minor receives is the overall data about the reality surrounding him, perceived by his consciousness matching his mental and intellectual capabilities, which, as a result, influences the further formation of his consciousness, mental state, development, and determines his models of behavior. It should be noted that, on the one hand, children adapt to the information space more easily than adults adapt, master it for various purposes. On the other hand, minors, due to their age characteristics, are the most vulnerable audience to the impact of a powerful information flow. Lacking the maturity of thinking skills, a child is not always able to differentiate the information received in a correct and adequate manner.

Plunging into the information space of modern communications, a child becomes an open target for all sorts of risks and threats (Rybakova, 2020, pp. 65–67; Bukalerova, Ostroushko, and Shagieva, 2021). Over the past year, we have noted with regret that many foreign media run a hybrid war against Russia, through the imposition of an alien ideology, the dissemination of false information, the distortion of historical truth, facts about the role of Russia in shaping the modern world order.

Children become unwitting targets of various kinds of information attacks. Due to the age and characteristics of the emerging personality, a child is not always able to objectively perceive such information, adequately respond to it, and establish its reliability. In this connection, the aim of ensuring the information security of minors is relevant.

II. Safety and Informational Security of Minors

Safety is a general social value. Security, as a quality of life, as the state of social and personal environment for a minor, where there are threats, dangers, risks, should have cumulative indicators.

Security is commonly understood through the idea “protection.” At the same time, security is a subjectively perceived assessment of the position of the subject, who, according to his assumption, is out of danger. Security may or may not be the same as safety. Security integrates both objective indicators (presence of normative, procedural, organizational, etc.) conditions, as well as subjective ones, involving, in particular, the person’s own assessment of his state as safe and contributing to the preservation of such a state. In our opinion, *security* is the quality and state of social environment, relevant and desirable for a person due to the absence of signs of threats, dangers, and risks. The *worldview of security* is a system of views on the interaction of a person and the surrounding world, the social environment regarding the provision of conditions for preserving his life, health, and dignity.

Information security is of particular importance in the conditions of information and technological society. Anna Chebotareva defines information security of a person as the state of safety determined by mitigation of external and internal risks and challenges for an individual in the global information society. Safety implies the ability to resist these risks and challenges through the information security culture development, as well as through the formation of state policy aimed at creating conditions for the realization of information rights and freedoms provided that information security is ensured (Chebotareva, 2017).

The study of the information security of minors becomes topical due to the peculiarities of age, psychological characteristics, the state of

consciousness, the nature of interaction with society. Sergey Budanov proposes one of the first definitions of information security of minors in his dissertation research. There it is defined as “a set of organizational and legal means regulating the rights of minors in the information environment, ensuring their protection from the influence of harmful (negative) information that entails a danger to their life and health, or that can harm normal moral spiritual, mental and physical health” (Budanov, 2006). Sergey Ivanov defines the information security of a minor as “a state of protection for children, which guarantees the exercise of their constitutional rights to search, receive, store, produce, disseminate information, to the inviolability of information about private life, and the absence of a risk associated with causing harm to their health and (or) physical, mental, spiritual, moral, intellectual development” (Ivanov, 2011, p. 66). In this definition, the scientist considers the category of security through the protection of a minor from the negative impact in the information space. Exploring the problems of legal regulation of information security of minors Larisa Efimova announces the formation of a new institution of information law--the institution of legal support of information security for children (Efimova, 2019, p. 134). We suppose that the main goal of ensuring the information security of minors is not only security, but also the creation and maintenance of the most favorable conditions for the adaptation of a minor in the information environment of modern society. This contributes to his personal development, improvement of spiritual, moral, intellectual, creative abilities and self-realization, subject to minimization (and exclusion) of possible risks and threats to life, health and its comprehensive development.

III. Risk Classification of Information Security of Minors

It is necessary to distinguish between the concepts of “risk,” “threat,” “challenges,” “danger,” “probability of danger.” Risk is an ontologically expressed component of human activity. It can be realized in a variety of forms and scales, being one of the components and factors of human life, accompanying its evolution. Risk is inherent in man as a generic being, is invariably present in various types of his activities and is associated with uncertainty. The presence of risk does not mean the

presence of an immediate threat and danger. It is danger that appears as a quality that can manifest itself in a situation of risk.

Risk as a result of human activity is associated with ontological risk, expressed as potential and completely unpredictable consequences, which have a mostly negative result. Risk implies a possible discrepancy between the goal and the result and the presence of danger. Danger is the qualitative side of risk, its refinement, assessed by a person based on any criteria, signs, measurements. The probability of danger is the sum of conditions, factors that transform the risk into a specifically expressed danger.

Threat is a negative directed action or inaction of any subject who has the goal of achieving the desired results with the help of his action. Challenges are factors, conditions, circumstances that are signs, characteristics of a particular stage in the development of a society, state, person. The challenges today are the consequences and results of scientific and technological transformations. The concept of “challenge” means an assessment by a thinking, rationally developing person of new factors that change, correct the existing way of life. Thus, historical challenges were transitions from an archaic, traditional society to an industrial and post-industrial one, the invention of weapons of mass destruction, environmental and technological disasters, and so on.

The challenge generates a situation of the necessary solution of emerging globally expressed problems. Mankind, armed with a stock of social systematized experience, scientific theories, changes in their paradigms, creates many challenges itself, believing that it is following the correct general path of development. Not all challenges are generated by intentional human activity. But people should respond to all challenges, both preventively and upon the manifestation of the initial stage of the challenge. We would like to correlate this conceptual series in connection with the realization of the rights and freedoms of minors.

There is a risk of formation and global development of information and communication technologies with a focus on the “values” of artificial intelligence that has become a factor of the general social level and is a challenge. It is able to weaken the traditional value bases of respect for a person, ensuring his dignity, the loss of control by adults over the

state of a favorable environment for a child, which creates a threat of universal social discrimination and the presence in the life of a child of a constantly reproducing danger of his degradation. The risk in the current projections of technological development is unavoidable, since it requires a change in the paradigms of the value-theoretical plan and the approval of the same standards for different states of ideals and ideas of goodness, justice, dignity, philanthropy, implemented mainly as natural rights in the state-legal life in the world level.

Technological risks for the first time in the history of humankind become social for the modern information society. Today, there is a possibility that the main risk of a futurological nature will be the departure of a natural person into the development of a partially artificial person, which is facilitated by modern robotic technologies. With the advent of new digital forms of interaction within the information space, the likelihood of new risk situations for a minor as a participant in information relations increases.

Earlier in our works, we have given classifications of the most probable risk situations that may arise in connection with the uncontrolled immersion of a minor child in the information environment, proposed by domestic and foreign scientists, have already been presented (Rybakova, 2020, p. 68; Rybakov and Rybakova, 2019).

The classification proposed in 2012 by the Organization for Economic Cooperation and Development still deserves some interest (OECD):¹

1. *Internet-technology risks* that include content-risks, involving viewing prohibited information (pornography, racism, aggression, hatred, including harmful advice (suicide) and contact-risks, cybergrooming, cyberbullying, online harassment, cyberstalking.

2. *Consumer-related risks* that include online marketing, over spending risks and fraudulent transactions.

3. *Information privacy and security risks*. Russian experts offer five groups of on-line risks for minors (Soldatova et al., 2012):

¹ Recommendation on the OECD Council Report on risks faced on children online and policies to protect them. Pp. 24–30. Available at: https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf [Accessed 03.09.2022].

1) *content risks* arising from the use of materials located on the Web (texts, pictures, audio and video files, links to various resources), and containing “illegal, unethical and harmful information (violence, aggression, erotica or pornography, hateful content, obscene language, information inciting racial hatred, propaganda of anorexia and bulimia, suicide, gambling, drugs, etc.);”

2) *communication risks* that arise in the process of communication and interpersonal interaction of users on the Web (among the examples, scientists name cyberbullying, illegal contacts (for example, online grooming, sexual harassment), online dating and subsequent meetings with online acquaintances in real life);

3) *consumer risks* arising from the abuse of consumer rights on the Internet (among the risks of this group, scientists name: the risk of purchasing low-quality goods, various fakes, counterfeit and counterfeit products; loss of funds without purchasing a product or service; theft of personal information for the purpose of fraud);

4) *technical risks*, which are determined by the possibility of implementing threats of damage to computer software, information stored on it, violation of its confidentiality or theft of personal information through malicious programs (viruses, worms, Trojan horses, spyware, bots, etc.);

5) *the risks of acquiring Internet addiction* or an irresistible craving for excessive use of the Internet, which in minors manifests itself in the form of passion for video games, an obsessive need to communicate through instant messengers, social networks and forums, online watching videos, movies and series. Among the main symptoms of Internet addiction, among scientists mention loss of control over the time spent on the network, withdrawal syndrome, replacement for reality.

The analysis of the above studies allows us to conclude that the main group of risks for the development of a minor are risks that have a direct impact on the formation of the worldview of a minor (worldview risks) — *the first group of risks*.

These risks can be attributed to the so-called primary threats, the meeting with which has a direct impact on the further formation and development of the minor. The emergence of risks in this group is

associated with the minor's access to excessive information that they are not ready to adequately perceive due to objective reasons: peculiarities of age psychology, an unformed system of personal values, the influence of various motivations on the child's consciousness, the immaturity of thinking as an insufficient result of experience and knowledge, an imperfect system goal setting, etc.

According to the classification proposed by Aleksey Chesnokov and Elena Akimysheva, all information that is redundant for children's perception could be divided into the following categories:

1) information harmful to health (high-frequency radiation, increased noise level and fire hazard, damage to eyesight, arthritis of the wrist joints, etc.);

2) information promoting ideas prohibited in society (terrorism, fascism, racial intolerance, sectarianism, drugs, cruelty to people, etc.);

3) information that causes sexual deviations (pornography, homosexuality, various perversions);

4) games that immerse in the virtual world, promote violence, develop gambling addiction, and do not contribute to the development of intelligence;

5) social networks that contribute to the creation of computer addiction, the risk of access by adults with criminal intent, conditions for the acquisition of prohibited goods (spice, other narcotic and psychotropic substances, stolen goods, weapons);

6) various kinds of fraud, online casinos, theft, inducement to purchase expensive information products (Chesnokov and Akimysheva, 2015).

The above classification names information that is essentially destructive for the child's consciousness, which, according to psychologists, can cause psychological or mental trauma for the child, which refers to disturbances in the normal functioning of the psyche, including cognitive processes (memory, attention, thinking, speech). Scenes of cruelty, violence, pornographic images, information of an extremist, terrorist nature, other illegal acts distributed through television, on the Internet, including in computer games, lead to an unconscious desire by a minor child to imitate what they see.

Exploring the influence of media, television and Internet content on the psychological characteristics of a minor, Olga Makhovskaya and Fedor Marchenko propose the term “screen homeless children.” Thus, they refer to such cases of uncontrolled immersion of a child in the media space, “when the child is alone with the screen, and there is no adult nearby who could comment on the content and warn of danger, they put in a vulnerable position not individual children or groups, but entire populations of young viewers and users” (Makhovskaya and Marchenko, 2017). Of course, viewing such information content, in the absence of an adult “guide” nearby (parent, educator, teacher, etc.) who is able to competently present the seen stories to the minor and evaluate the behavior of the characters, the child may believe that the behavior patterns seen are acceptable and in real life.

Plunging into the information environment, minors perceive information through the reflection in mind, differentiate the received information into interesting (uninteresting), useful (useless), positive (negative), reliable (unreliable), etc. according to their intellectual, moral, cognitive capabilities.

There is an opinion of teachers, psychologists that in order to normalize the child’s socialization and adequate perception of negative information, a minor child, in accordance with his age and level of development, should receive a certain amount of “negative information.” Thus, they become aware of the existence of antisocial behavior, aggression and evil, but such information should not be presented as encouraged behavior, but on the contrary, it is required to express censure of such behavior, to speak of it as deviant from the norm (Ambalova, 2019; Golubeva, 1985; Saltykova-Volkovich, 2016).

We believe that such information should be presented only when children are together with adults. In this case, the role of a “guide” in the information flow is assigned to parents, teachers, educators who are able to set the right moral guidelines, thereby contributing to the formation of a positive model of behavior of a minor. In the absence of competent support, due to their age, psychological, physiological characteristics of personality development, a child is not able to independently adapt to the modern information and communication society. This leads to the transformation of the moral and moral attitudes of the child, which can

further lead to the formation of an aggressive behavior model, and, as a result, an increase in the number of children with various forms of social maladaptation and deviant behavior.

The *second group of risks* is the risks associated with the involvement of a minor in illegal activities through the Internet. It should be emphasized that the risks of this and subsequent (third) groups are secondary in relation to the first group of risks, derived from them.

Taking into account the age characteristics, the child gradually expands the volume of interaction with the information Internet environment, the search queries for information are supplemented by the possibility of establishing new contacts with virtual interlocutors, including through social networks (*Vkontakte*, *Odnoklassniki*, etc.). Communication of minors with each other and the outside world takes place in virtual reality. Psychologists confirm that the space of social networks for a teenager is simultaneously associated with autonomy from adults and with a sense of the possibility of manifesting one's own activity and freedom in choosing the content and forms of communication (Sobkin and Fedotova, 2019). In other words, the Internet is an alternative communication platform for minors, where, in the absence of visualization of the interlocutor, they have the opportunity to communicate, exchange information, express an opinion, count on the support of the virtual community (interlocutor), and therefore, feel full, confident and comfortable.

In itself, virtual communication on the network does not pose a danger, if the rights of a minor are not violated, and neglect of the norms of what is permitted is not allowed. On the one hand, virtual communication is convenient for minors themselves. Features of the child's and adolescent psyche are characterized by the presence, to one degree or another, of certain complexes and phobias, low self-esteem, self-doubt (appearance, knowledge, social status, etc.), which often prevents full communication with peers outside the virtual space. Thus, virtual communication is preferable to offline interaction. According to the study "Children of Russia Online," almost a third of the children and adolescents surveyed admitted that they introduced themselves online as another person at least once (Soldatova et al., 2012). Thus,

a minor prefers virtual self-realization rather than traditional ways of interacting with peers.

Virtual communication becomes dangerous in cases where it goes beyond ordinary communication, contains elements of behavior unacceptable in society (aggression, illegal mental and (or) emotional pressure on a minor, blackmail, etc.). We must agree with Illaria Bachilo that all the complexity of regulating relations in this area is explained by the fact that the so-called “virtual subject” operates in the Internet space, which is “poorly tangible” (its signs and characteristics are unstable), but it is capable of action and participates in relations on a par with others” (Bachilo, 2016). This statement is still relevant today. The anonymity of social network participants complicates the manageability of this type of legal regulation.

New forms of interaction and ways of building relationships with a virtual community (interlocutor) determine the emergence of communicative skills on the network, which together determine the rules, values, and ultimately the subculture of the virtual community. In this case, there is a risk of deviation from the moral values generally accepted in society, which can manifest themselves in various forms of antisocial behavior. Modern forms of asocial behavior of minors are characterized by their diversity, ranging from deviant and addictive behavior to delinquent, manifested in the commission of offenses. As a rule, antisocial behavior is manifested not only externally, but is also accompanied by a change in the internal moral and value attitudes of the minor. The antisocial behavior of minors is one of the most significant among the problems of modern society that need to be addressed.

Taking into account the fact that juveniles are characterized by immaturity of thinking as a result of insufficient experience and knowledge (Feldshtein, 2004; Golubeva, 1985), a tendency to imitate (Rean, 2012), a certain susceptibility to the negative influences of the microenvironment, the desire for extreme behavior, then getting into the Internet space, the child finds himself in a zone of special risk. Uncontrolled unlimited presence in the network has a traumatic and sometimes corrupting effect on minors, facilitates their involvement in illegal activities.

Indeed, through immersion in virtual reality, a minor, without suspecting it, can be involved in illegal activities (including extremist, terrorist activities), any other direction, for example, dissemination of prohibited information, violation of public order and public safety, etc. Not all children in adolescence know that such activities are punishable, and punishment may be applicable to them (or legal representatives). Many of the minors believe that “hiding behind a nickname” and being in virtual reality can go unnoticed and unidentified. At the same time, minor children, without suspecting it, bear responsibility (administrative and criminal) starting from the age established by law.

The *third group of risks* presents the risk to become a victim of unlawful (including criminal) actions. It should be noted that the following list of possible illegal actions against minors is not exhaustive. Let us name the most common cases of violation of the rights of underage users of various Internet search engines.

Internet information deception, which manifests itself in the risk of obtaining “inaccurate information” due to the fact that a minor, in the absence of filters, has access to an unlimited number of information resources. Modern schoolchildren and students get most of the information from the network by entering an appropriate search query, where, along with reliable official sources (reference search engines, library resources, etc.), there are so-called unreliable *Yandex-Google* sources. Receiving a *Yandex-Google* answer to a question asked, a minor is not able to critically evaluate the information received, he accepts it as the truth.

We agree with Aleksey Minbaleev, that ensuring information security always involves ensuring the integrity, reliability and accuracy of information, respectively, the implementation and protection of the right to reliable information, scientists are invited to consider as a factor in ensuring information security (Minbaleev, 2019). In this case, we are talking about information as an object of consumption.

Minors may be victims of Internet crimes. Due to their inexperience, a minor child may face other types of violation of his rights as a consumer of various products, goods and services, if they are provided in poor quality, or if they are not provided at all after the on-line payment is made. A much greater danger for minors is the possibility of becoming a

victim of various crimes, including those committed using the Internet, the variety of which is increasing every year, starting with account hacking, e-mail, cyber fraud, etc. The minor does not have the special knowledge and sufficient experience to resist this.

In the past few years, one of the most common types of destructive behavior among minors has become Internet harassment of peers using threats, an expression of aggression. Aggressive behavior of minors towards peers occurs in the form of intimidation, usually using personal information about the victim.

The suggested classification of information risks is certainly not exhaustive. The overloading of the modern information environment raises the question of the need to protect minors from excessive information that is negative for perception and not intended for the child's psyche.

New forms and methods of illegal interaction of the criminal community with minors, which are implemented through the Internet, unfortunately, are constantly "improved" and modified, which requires the development of new approaches to solving the problems of ensuring the information security of minors. We are talking about the need to form a national model for ensuring the information security of a minor that best meets the challenges and threats of the modern information space, providing optimal conditions for the upbringing and development of a minor.

IV. Discussion on the Necessity for the Constitutional and Legal Model Development for Ensuring the Information Security of Minors

The information security of minors should be considered in the system of building a national model of the constitutional and legal maintenance of their rights and freedoms. We are talking about such inalienable constitutional rights of the child as the right to full development (physical, spiritual, moral, intellectual), the right to health protection (mental, physical), the right to information, the right to education, the right to access cultural values and to join in culture, etc.

The information security of the child is part of his personal security, which, according to Madlena Vorontsova, is an objective (natural-legal) level of security, which is initial and allows the child to exist as a living organism (Vorontsova, 2017, p. 40). Thus, the child's right to information security includes a whole range of rights and freedoms, primarily the right to life and health, full development. The rights of every child are constitutional values, embody the interests of future generations, the entire nation, and form the basis of the national security of our state. The implementation of the indicated rights ensures the comprehensive spiritual, moral, physical, intellectual development of the minor, his social integration, contributes to his self-expression, and provides an opportunity to exercise other constitutional rights.

The information security of children should be considered as a complex category that takes into account all the risk groups listed above. The child is integral as a person, specific as an individual, and valuable in itself as a person and must be protected from possible negative influences on him in the information space. The Constitution of the Russian Federation establishes a special status for a child (a person under the age of 18) as a subject in need of special protection. This approach is due, first of all, to the age, emotional-volitional, psychological characteristics of the child's personality, which justifies the need for special protection measures from society and the state. Ensuring the safety of the child in the context of constitutional and legal values involves the creation of a favorable environment for the life of the child.

There is a special information security regime in place for minors. Federal Law No. 124-FZ "On the basic guarantees of the rights of the child in the Russian Federation" establishes the basis for ensuring the basic constitutional guarantees of the rights and legitimate interests of the child, based on the principles of prioritizing the preparation of children for a full life in society, the development of socially significant and creative activity in them, the education of high moral qualities in them, assigns the state authorities are obliged to take measures to protect the child from information, propaganda and agitation that harm his health, moral and spiritual development (Para. 1 of Art. 14). It should be emphasized that the assignment of this duty to the state

does not exclude, but complements the duty of parents to protect and educate their children, taking measures aimed at the healthy spiritual and moral development of the child. It should be noted that there have been positive developments in the development of federal legislation to ensure the information security of children and adolescents, including on the Internet, since 2010 (Federal Law No. 436-FZ of 29.12.2010 “On the protection of children from information harmful to their health” were adopted; The Concept of Information Security of Children, 2015; Strategies for the development of the Information Society in the Russian Federation, 2008 and 2017).

The model of constitutional and legal regulation of relations in the field of ensuring the information security of a child assumes the presence of the following main elements: goals, objectives, principles of functioning, a system of subjects that provide this model, a system of guarantees, criteria and forms for fixing its effectiveness. The latter is necessary, since the goals cannot be absolutely identical to the result, and it is necessary to diagnose the success of the model. It should be taken into consideration that the legal modeling of the information security of minors is an activity scheme for achieving goals, which expresses its social significance.

As the Constitutional Court of the Russian Federation pointed out in its Judgment that “legal regulation in the field of state protection of the rights of minors implies, in particular, the existence of legislative measures aimed at ensuring the safety of each child both directly from criminal encroachments and from an adverse effect on his morality and psyche, which can significantly affect the development of his personality, even without being expressed in specific illegal acts.”² The same goals, according to another Judgment of the Constitutional Court of the Russian Federation, necessitate the use of optimal legal tools in legal regulation, which, taking into account the requirements of Articles 17 (Part 3) and 55 (Part 3) of the Russian Constitution, “to protect child from exposure to information that can harm his health and development, in particular information associated with the aggressive

² Judgment of the Constitutional Court of the Russian Federation No. 19-P dated July 18, 2013. Available at: <http://doc.ksrf.ru/decision/KSRFDecision135892.pdf>. (In Russ.). [Accessed 13.10.2022].

imposition of specific models of sexual behavior, the formation of distorted ideas about socially recognized models of family relations that correspond to moral values generally accepted in Russian society in their constitutional and legal expression.”³

Based on constitutional principles and priorities, the legislator, forming the main directions of legal policy, sets himself the task of ensuring the safety of minors in the information sphere, which are aimed at minimizing and eliminating the risks of the information space, at preventing the commission of illegal acts against minors through the use of Internet technologies. The safety of minors in the information space is ensured by the norms of various branches of law — constitutional, informational, civil, criminal, administrative, etc., which together form the legislative framework for legal regulation in this area.

The dynamics of the development of public relations in the digital environment in the Russian space has necessitated the adoption of a whole array of regulatory legal acts and policy documents in the field of ensuring human security as a participant and the main subject of information relations. For twenty years, Russian legislation has formed a fairly large array of legal acts aimed at ensuring the security of technological information systems, information itself as an object, as well as subjects of information legal relations as the main participants in these relations.

Despite the measures taken in the field of ensuring the safety of minors in the information environment, at present it cannot be argued that the situation in this area has been fully resolved and the problems have been exhausted. With the advent of new digital forms of interaction within the information space, the likelihood of new risk situations for a minor as a participant in information relations increases.

It should be noted that the model of constitutional and legal regulation of information security of minors is at the stage of its formation. National Security Strategy of the Russian Federation (hereinafter — the Strategy), approved by the President of the Russian Federation on July 2, 2021, Decree No. 400, calls information security one of the priorities of

³ Judgment of the Constitutional Court of the Russian Federation No. 24-P dated September 23, 2014. Available at: <http://doc.ksrf.ru/decision/KSRFDecision173469.pdf>. (In Russ.). [Accessed 27.10.2022].

the national security of our state. The Strategy defines national security threats as “external cultural and informational expansion (including the distribution of low-quality mass culture products), propaganda of permissiveness and violence...” This approach is fully consistent with the constitutional principle of ensuring the information security of an individual, society, state and is dominant.

Today we should talk about the creation of the Russian model of information security of minors. It is necessary to implement the domestic model since the relationship of the safe life of the child fits into the conditions of a specific socio-cultural environment of a society built on domestic traditions, historical, spiritual and cultural values. The condition for creating a national model is the existence of constitutional provisions that determine the vectors for the development of legislation in the field of ensuring the information security of children.

The main principles of ensuring the information security of minors are:

1) *principle of the most complete provision of the rights and freedoms of a minor in the information space*, which involves the creation of favorable conditions for the development of the personality of a minor, which is implemented by recognizing a minor as an equal participant in the information space, which corresponds to international standards in this area and constitutional principles for ensuring information and related rights of a minor;

2) *principle of systematic state-legal regulation*, which involves legislative, law enforcement, executive-administrative and control activities of the state to ensure the safe implementation of the rights and legitimate interests of minors in the information environment, by pursuing a unified state policy in the field of information security;

3) *principle of complexity*, which implies the interaction of legal, organizational, economic, preventive, educational, educational and other measures to create an optimal mechanism for protecting a child in the information space;

4) *principle of continuity*, which implies the implementation of the mechanism for the protection of minors in the information space on an ongoing basis.

We believe that it is on the above principles that the constitutional and legal model for ensuring the information security of minors should be built.

V. Conclusion

The complex of existing problems in the field of ensuring the information security of minors leads to the need to form a legal model based on constitutional values. It is necessary to talk about the constitutional and legal model, which is proposed in this article and which fits into the national model of ensuring the constitutional rights and freedoms of a minor. A minor, proceeding from the spirit and meaning of the Constitution, has a constitutional right to security in the information environment, which directly affects the implementation of his other constitutional rights. The information security of a child should be considered in the national security system. We are talking about generations of young people who are able to assess the quality, reliability, integrity of information from a humanistic legal standpoint, have the ability and ability to correlate the information received with other arrays of it.

The trinity of law, governance and organization forms the basis for ensuring the information security of minors. Regulatory prescriptions presuppose public administration in the field of information management and the existence of organizational efforts by both the state and civil society institutions to achieve the goals of information security of minors. It is advisable to implement the constitutional and legal model of information security of minors taking into account the following priorities:

- legislative consolidation of the system of guarantees for the realization of the rights and freedoms of minors in the information society;
- legislative and organizational provision of protection against risks and threats to the information environment in the following areas: 1) protection of children from access to unfavorable (destructive) information; 2) protection of information about a minor from unlawful dissemination and use by third parties; 3) protection of minors from

crimes and other illegal actions committed against them with the help (through) information and communication technologies; 4) protection of minors from offenses committed by them through information and communication technologies;

- legislative and organizational support for the formation of the information culture of children and adolescents, which is the most important element of ensuring information security;

- control and supervisory provision of information security of minors.

References

Ambalova, S.A., (2019). Psychological causes of deviant behavior of adolescents: prevention and correction. *Azimut nauchnykh issledovaniy: pedagogika i psikhologiya*, 8(3)(28), pp. 317–319. (In Russ.).

Bachilo, I.L., (2016). *Information law: A textbook for academic undergraduate studies*. 5th ed., rev. and suppl. Moscow: Prospect Publ. (In Russ.).

Budanov, S.A., (2006). *Legal support of information security of minors*. Cand. Sci. (Law) Diss. Voronezh Institute of the Ministry of Internal Affairs. Voronezh. (In Russ.).

Bukalero, L.A., Ostroushko, A.V., and Shagieva, R.V., (2021). Counteraction to Dangerous Infringements on Children's Rights and Interests in the Information Sphere in the Context of the Digital Transformation of Management in Russia. In: *Socio-economic Systems: Paradigms for the Future*. Collection of Articles, 314, pp. 1239–1247.

Chebotareva, A.A., (2017). *Legal support of personal information security in the global information society*. Dr. Sci. (Law) Diss. Institute of State and Law of the Russian Academy of Sciences. Moscow. (In Russ.).

Chesnokov, A.A. and Akimysheva, E.S., (2015). The role of the internal affairs bodies in the mechanism of ensuring the information security of the child. *Altaiskiy yuridicheskii vestnik*, 3(11), pp. 139–142. (In Russ.).

Efimova, L.L., (2019). Legal regulation of information security of children in the UK. *Pravo i gosudarstvo: teoriya i praktika* [Law and State: Theory and Practice], 11(179), pp. 121–131. (In Russ.).

Feldshtein, D.I., (2004). *Psychology of growing up: Structural and content characteristics of personality development*. Selected Works: 2nd ed. Moscow: Moscow Psychological and Social Institute: Flint Publ. 672 p. (In Russ.).

Golubeva, L.M., (1985). Causes of offenses among youth and measures to eliminate them. In: Golubeva, L.M. *Offenses among youth and measures to prevent them*. Kirgiz SSR Case. Frunze: Ilim Publ. Pp. 42–60. (In Russ.).

Ivanov, S.V., (2011). Information security of children (theoretical and legal aspect). *Vestnik Ekaterininskogo instituta* [Bulletin of the Catherine Institute], 2(14), pp. 62–66. (In Russ.).

Kuznetsov, P.U., et al., (2020). Information technologies in legal activity. 3rd ed., rev. and suppl. Moscow: Urayt Publ. (In Russ.).

Makhovskaya, O.I. and Marchenko, F.O., (2017). The influence of educational media on the development and viability of children. *Institut psikhologii Rossiiskoy Akademii nauk. Organizatsionnaya psikhologiya i psikhologiya truda*. [Institute of Psychology of the Russian Academy of Sciences. Organizational psychology and psychology of work], 2(2), pp. 201–224. (In Russ.).

Minbaleev, A.V., (2019). The impact of constitutional rights and freedoms of man and citizen on the development of information law in the context of the digitalization of modern society. In: *Legal education and legal science in Russia: Current trends and development prospects (To the 15th Anniversary of the Faculty of Law of Kursk State University)*, pp. 204–212. (In Russ.).

Rean, A.A., (2012). Teen subculture is a zone of potential risks. *Psikhologicheskaya nauka i obrazovanie* [Psychological science and education], 17(4), pp. 5–10. (In Russ.).

Rybakov, O.Yu. and Rybakova, O.S., (2019). Principles of information security of a child on the Internet. *Studies in Computational Intelligence*, Vol. 826, pp. 427–433.

Rybakova, O.S., (2020). Safety of minors in the information society: analysis of cyber risks and threats. *Monitoring pravoprimeneniya* [Monitoring of Law], (35), pp. 65–73. (In Russ.).

Saltykova-Volkovich, M.V., (2016). Causes and features of deviant behavior. *Vestnik Polotskogo gosudarstvennogo universiteta. Seriya E. Pedagogicheskie nauki*, 15, pp. 24–28. (In Russ.).

Sobkin, V.S. and Fedotova, A.V., (2019). Adolescent aggression in social media: Perception and personal experience. *Psikhologicheskaya nauka i obrazovanie [Psychological science and education]*, 24(2), pp. 5–18, <https://doi.org/10.17759/pse.2019240201>. (In Russ.).

Soldatova, G., Rasskazova, E., Zotova, E., Lebesheva, M., and Roggendorf, P., (2012). *Children of Russia Online: risks and safety. Results of the international project EU Kids Online in Russia*. Available at: <http://psypublic.com/assets/files/EU-Kids-Online-II-inRussia.pdf> [Accessed 12.10.2022].

Vorontsova, M.A., (2017). Personal safety of minors as a constitutional value. *Probely v rossiyskom zakonodatelstve [Gaps in Russian Legislation]*, 5, pp. 40–43. (In Russ.).

Information about the Authors

Oleg Yu. Rybakov, Dr. Sci. (Law), Dc. Sci. (Philosophy), Professor, Head of Philosophy and Sociology Department, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

9 Sadovaya-Kudrinskaya Str., Moscow 125993, Russian Federation

ryb.oleg13@yandex.ru

ORCID: 0000-0003-4805-3083

Olga S. Rybakova, Cand. Sci. (Law), Associate Professor, Department of Constitutional and Municipal Law, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

9 Sadovaya-Kudrinskaya Str., Moscow 125993, Russian Federation

orro21@yandex.ru

ORCID: 0000-0003-2870-4355