Modeling problems legal regulation of the field of artificial intelligence

V.V. Antonov 1, Z.I. Kharisova 2, N.R. Kalimullin 2, A.I. Abdulnagimov 1

1 Ufa State Aviation Technical University, Ufa, K. Marks str., 12, 450008, Russia
2 Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Muksinov str., 2, 450103, Russia

E-mail Zarinaid@mail.ru

Abstract. The analysis of the current state of regulation issues at various levels of the development and application of artificial intelligence systems is presented. Key issues in the field of regulation of robotic systems are considered. Possible threats are described, a model for the formation of artificial intelligence systems, including the ones for high-risk facilities is proposed.

Keywords: Artificial intelligence; Law; Neural networks; Robot ethics

1. Introduction
The active development of artificial intelligence (AI)-based systems creates new challenges for society, the discussion of which is necessary, moreover, with the participation of representatives of completely different spheres of public life: from developers and technical specialists to legislators, law enforcement bodies [1,2] and art workers. The issues of regulation of both the activities of developers of AI systems and the results of AI activities require vigorous discussion. Today, there is no clear understanding of the legal status of AI and the results of its activities, i.e. it is unclear who will own this result, who will be responsible for socially dangerous consequences and violations of the law. The introduction of self-learning systems into various systems [3,4] creates new sources of increased danger, for example, transport with an AI-based control system. The issue of legal regulation of such systems is relevant primarily in connection with industry-specific legal problems that cannot be resolved within the framework of current legislation (which hinders the development of technologies). In addition, the introduction of new technologies is intensifying within the digital economy, which requires appropriate regulatory mechanisms.

The regulation of AI should not hinder the development of technologies both in our country and around the world. The importance of AI development has been repeatedly emphasized at the political level as well. Today, there are elaborations of national strategies for the development of artificial intelligence in many countries [5,6], the goals of which are to maintain leadership positions in this field at the international level, to develop safe and comfortable cities, to provide affordable and high-quality medical, logistics and educational services, to create a developed transport system in the country, as well as the exploration of outer space and the oceans.
Due to the emerging opportunities for solving many problems in the economic and social spheres, it becomes necessary to determine the legal status of artificial intelligence, taking into account the general trends in the regulation of robotics in the world.

2. AI terminology
Participants in different discussions do not always mean the same thing when discussing AI. Thus, an important step is the development of a generally accepted conceptual apparatus. This article discusses the concept of “artificial intelligence” as a complex of technological solutions that allows you to simulate human cognitive functions (including self-learning and search for solutions without a predetermined algorithm) and obtain specific tasks results comparable at least with the results of human intellectual activity. The complex of technological solutions includes information and communication infrastructure, software (including those employing machine learning methods), processes and services for data processing and finding solutions. Thus, AI is a system, for the creation of which a complex technological chain is required: from the creation of specific processors and computing centers (if we talk about AI for mass or industrial use), other hardware, algorithms to databases for training, etc. So, it becomes apparent that many parties are involved in the creation of AI.

Promising methods of artificial intelligence are the methods aimed at creating fundamentally new scientific and technical products, including those for the development of universal (strong) artificial intelligence (autonomous solution of various problems, automatic design of physical objects, automatic machine learning, algorithms for solving problems based on data with partial markup and (or) insignificant amounts of data, information processing based on new types of computing systems, interpreted data processing and other methods) [7,8]. The AI development strategy assumes the emergence of the so-called strong artificial intelligence, which becomes more likely with the development of quantum computers, removing the limitations of the architectures with binary logic used today.

Thus, the term “artificial intelligence” is suitable for two types of intelligent systems, which have one common property - learning and self-learning, but which have an incomparably different level of capabilities and consequences, including legal ones.

3. Ethical aspects of artificial intelligence regulation
The formation of man and society took place over millennia, while the human psyche was formed with the ability to distinguish between good and evil, to sympathize, to predict implicit consequences, etc. Artificial intelligence (if we talk about “strong” AI) without going through such a long evolutionary path will possess the properties obtained during training and self-learning. Thus, those behavioral models, which seem to be “disadvantageous” at first glance, should be considered as a mandatory element of learning, otherwise AI behavior will be sociopathic in nature.

Despite the lack of the ability to create “strong” AI in the near future, the existence of existential risks of such a rapid development of technologies is quite obvious [9]. In these conditions, the adoption of the Asilomar AI Principles in January 2017 at the conference in Asilomar, USA (2017 Asilomar conference) was the first and very significant step to the responsible approach of humanity to the development of AI and robotics. The Asilomar AI Principles were developed and adopted following the conference of AI developers and researchers. To date, over 4,000 scientists, developers, entrepreneurs and experts have signed them. Among them are Elon Musk, Stephen Hawking and Ray Kurzweil, representatives from Google, Apple, Facebook, IBM, Microsoft, etc. The first paragraph of these principles proclaims the goal of AI research: the goal should be to create useful intelligence rather than uncontrollable intelligence. In total, 23 principles are presented, each of which emphasizes the responsibility of developers, politicians, businessmen towards humanity in the field of AI development.

Among the aspects of this document that deserve special attention are:
the provision on "useful financing", which implies additional investments for research in the field of AI in order to increase the effectiveness of implementing AI in the field of the most pressing problems;

- the provision on "scientific and political communication", which implies close cooperation between developers of AI systems and persons responsible for the legal regulation of AI;

- the provision on "security and transparency of errors", as well as the application of restrictions in software implementations of AI related to the principles of universal morality.

Software developers based on AI principles are one of the key "players" and are responsible for erroneous decisions based on AI, as well as the formation of moral costs from the use of AI software systems [10, 11]; moreover, these developers can influence such consequences. At the same time, the Asilomar principles of research in the field of AI declare the so-called anthropocentric path, which says that everyone should be able to choose in what capacity to use AI-based software systems for what purpose. It is possible for a number of purposes – do not apply at all. At the same time, the emerging problem of using personal data in AI-based solutions is, also given special attention, since this is, directly related to ensuring basic human rights and society as a whole. In the long term, the development of the theory of strong AI, when software systems in the field of AI begin to acquire the ability to recognize "themselves "as" individuals", is declared with significant restrictions - supervision, compliance with ethical standards and minimizing the above risks, and even at the stages of forecasting[12].

The proposals put forward by the experts are essentially the example of the first attempts at self-regulation, when organizations or individuals are developing rules before the state has developed binding laws. One of the characteristic attributes of self-regulation is an association. Its rules become binding on all its members. An example of such association is the Partnership on AI, the partnership that includes Amazon, Apple, Google, IBM, Facebook, Microsoft and others. It was created in 2017 and it is too early to talk about specific rules, but we see one of the unique examples of association of the largest companies in the world (by the way, competitors in a number of areas) around the problem of artificial intelligence development.

4. Possible threats and legal regulation of systems based on artificial intelligence

The civil liability system, especially in European countries, covers most of the future scenarios for the development of new technologies, including those based on artificial intelligence, however, in some countries, especially in developing ones, there are a number of unsolved problems. In general, the problems are associated not with the proliferation of systems based on AI, but with the problem of identifying the actions of such systems and correlating them with deliberately inherent errors or, in the worst case, the development and additional training of such systems, including, for unknown reasons, according to an unlawful scenario.

At the same time, it is important to regulate this industry not in separate countries or exclusively on the territory of the European Union [13], but at the international level.

Since artificial intelligence algorithms can process large amounts of data with great precision and speed, often significantly exceeding human potential, AI applications are becoming more common today. However, the dependence on AI carries risks, especially when a decision-making process is totally automated. Problems arise when the available algorithms reflect the prejudgement, for example, of the developer company in relation to any category of people, race or even gender, as a result of which, just as in the case of “mechanical” solution of problems by the person himself, one may encounter “human” as well as a “robotic” factor. For this reason, the openness of a particular development is important, as well as its evaluation and recognition as a safe, impartial and effective system by an independent group of experts in this industry. Thus, the regulations are needed to recognize the development as objective, effective and qualitative with the possibility of continuous training, adaptation and data protection with encryption [14].
The accuracy and reliability of AI algorithms and automated decision-making primarily depends on the operator (trainer), at the same time, the level of responsibility is often assigned to him in proportion to the contribution to the system, since it is too early to talk about establishing responsibility for a robot. In this case, there is an obvious need for insurance of AI systems as a guarantor of compensation for damages.

However, in the case of full assignment of responsibility for the actions of the robot to the developer or operator, the factor of stimulating the development of modern systems based on AI is lost. An alternative solution is to establish a separate category of law for robotic systems with the status of an electronic person, making him responsible for all actions [15].

Thus, it can be noted the need to consider the following issues in the field of legal regulation of robotic systems:

- formation of an insurance fund to compensate for damage caused by AI systems;
- introduction of a licensing system for AI developments;
- establishing legal entity status for AI-based systems;
- establishing uniform international legal norms for neural network developments;
- imposition of responsibility for damages (violation of production technology, operation and information security) on the operator, developer or owner.

5. AI information security threat model

The widespread use of AI generates many potential threats. However, already today information systems used in certain areas are regulated by law, for example, in Russia, the “Requirements for ensuring the protection of information in automated control systems for production and technological processes at critical facilities, potentially hazardous facilities, as well as the facilities posing an increased danger to life and health of people and to the environment” and the “Requirements for ensuring the safety of significant objects of the critical information infrastructure of the Russian Federation” have been approved. AI systems introduced in these areas, or forming high-risk facilities, naturally fall under such requirements.

One of the requirements for such information systems is the availability of the Information Security Threat Model. A threat model is a fundamental document in building an information system. It takes into account the peculiarities of the information system: software, hardware, software and hardware tools and information processing [16, 17]. A threat model is a document that regulates threats to an information system and the security of information in it. The formation of threats by the information system itself is not reflected in the threat model. However, an established and proven control system can be a reliable basis for the formation of a basic methodology and standards in designing AI systems from the standpoint of safety.

When building a threat model of information systems, a certain methodology is used, which includes the following stages:

- description of the information system;
- structural and functional characteristics;
- description of security threats;
- violator model;
- possible vulnerabilities;
- ways of implementing threats;
- consequences of violation of information security properties.
To adapt the methodology for describing AI systems, the description of security threats and the threat bank, presented on the relevant information Internet resources of the regulators, should be supplemented accordingly.

The compliance of the information system with the developed threat model will require constant or periodic monitoring. For this, it is necessary to develop a verification concept, including the following methods:

- expertise;
- statistical analysis;
- formal verification methods;
- dynamic verification methods;
- synthetic verification methods.

6. Conclusion

Thus, it can be noted that it is necessary to consider the following issues in the field of regulation of robotic systems:

- development of the concept of ethical and legal regulation of AI-based systems;
- establishing the status of a legal entity for AI-based systems and uniform international legal norms for neural network developments;
- introduction of a licensing system for AI developments;
- imposition of responsibility for damages (violation of production technology, operation and information security) on the operator, developer or owner;
- development of a security threat model of AI-based systems in accordance with the proposed methodology;
- formation of a specialized bank of threats to AI-based security systems, as well as the descriptions of typical security threats;
- development of a threat model verification concept.

The proposed measures will make it possible to establish the fundamental basis of legal regulation of AI-based systems, as well as to ensure compliance with the safety requirements of functioning based on the proposed methodology.

7. Acknowledgment

The study is carried out with the financial support of the Ministry of Education and Science of the Russian Federation within the framework of the main part of the state assignment to higher educational institutions No. FEUE-2020-0007.

References

[1] Cerka P, Grigiene J and Sirbikyte G 2017 Is it possible to grant legal personality to artificial intelligence software systems. Computer Law & Security Review 33 685.- DOI: 10.1016/j.clsr.2017.03.022

[2] Carrillo M 2020 Artificial intelligence: From ethics to law Telecommunications Policy 44.- DOI: 10.1016/j.telpol.2020.101937

[3] Fetisov V, Kharisova Z, Dmitriyev O and Melnichuk O 2017 Rapid particle size analysis of suspensions based on video technology and artificial neural network with additional training during operation International Journal of Applied Engineering Research 12(7) 1271.

[4] Peng Y, Li S and Hu Z 2019 A self-learning dynamic path planning method for evacuation in large public buildings based on neural networks Neurocomputing 365 71.- DOI: 10.1016/j.neucom.2019.06.099
[5] Borges F, Laurindo J, Spinola M, Gonçalves R and Mattos C 2020 The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions *International Journal of Information Management*. DOI: 10.1016/j.ijinformat.2020.102225

[6] Trappey A, Lupu M and Stjepandic J Embrace artificial intelligence technologies for advanced analytics and management of intellectual properties *World Patent Information* 61.- DOI: 10.1016/j.wpi.2020.101970

[7] Noriega M. 2020 The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions *Futures* 117.- DOI: 10.1016/j.futures.2019.102510

[8] Gasimova R and Abbasli R 2020 Advancement of the search process for digital heritage by utilizing artificial intelligence algorithms *Expert Systems with Applications* 158.- DOI: 10.1016/j.eswa.2020.113559

[9] Sergievskii V 2020 Super Strong Artificial Intelligence and Human Mind *Procédia Computer Science* 169 458.- DOI: 10.1016/j.procs.2020.02.225

[10] Samsonovich A 2020 Socially emotional brain-inspired cognitive architecture framework for artificial intelligence *Cognitive Systems Research* 60 57.- DOI: 10.1016/j.cogsys.2019.12.002

[11] Shank D and Desanti A 2018 Attributions of morality and mind to artificial intelligence after real-world moral violations *Computers in Human Behavior* 86 401.- DOI: 10.1016/j.chb.2018.05.014

[12] Kouziokas G 2017 The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment *Transportation Research Procedia* 24 467.- DOI: 10.1016/j.trpro.2017.05.083

[13] Cohen G Evgeniou T, Gerke S and Minssen T 2020 The European artificial intelligence strategy: implications and challenges for digital health *The Lancet Digital Health* 2 376.- DOI:10.1016/S2589-7500(20)30112-6

[14] Rahman S, Khalil I, Atiquzzaman M and Yi X 2020 Towards privacy preserving AI based composition framework in edge networks using fully homomorphic encryption *Engineering Applications of Artificial Intelligence* 94.- DOI: 10.1016/j.engappai.2020.103737

[15] Villaronga E and Golia 2019 A Robots, standards and the law: Rivalries between private standards and public policymaking for robot governance *Computer Law & Security Review* 35 129.- DOI: 10.1016/j.clsr.2018.12.009

[16] Figueira P, Bravo C and Lopez J 2020 Improving information security risk analysis by including threat-occurrence predictive models *Computers & Security* 88.- DOI: 10.1016/j.cose.2019.101609

[17] Kulikov G, Antonov V, Kharisova Z and Rodionova L 2020 The set-theoretic approach to the construction of the dual system model of the pack for the studied area of activity with mixed real and virtual objects *Vestnik SUSU. Computer Technologies, Management, Radio Electronics* 20(1) 5–15.- DOI: 10.14529/ctcr200101