Artificial Intelligence and Problems of Ensuring Cyber Security

Zarina I., Khisamova[1]
Krasnodar University of the Ministry of Internal Affairs of the Russian Federation

Ildar R., Begishev[2]
Kazan Innovative University, Russian Federation

Elina L., Sidorenko[3]
Moscow State Institute of International Relations (University), Russian Federation

Abstract
The active use of artificial intelligence leads to the need to resolve a number of ethical and legal problems. The ethical framework for the application and use of data today is highly blurred, which poses great risks in ensuring data confidentiality. In the article, the authors analyzed in detail the main problems in the field of cybersecurity in connection with the active use of AI. The study identified the main types of criminological risks associated with the active implementation of AI. By a separate question, the authors investigated the issues of bringing to responsibility and compensation for damage caused by AI. The authors argue the position about the need to recognize AI as a source of increased danger. It is proposed to use the legal fictitious as a method in which a particular legal personality of AI can be perceived as a non-standard legal position, different from reality.

Keywords: Artificial Intelligence, Machine Learning, Criminological Risks, The risks of the use of Artificial Intelligence, Threat of Use of Artificial Intelligence, Ethical Issues, Cyber Security.

[1] Head of the Department of planning and coordination of scientific activities of the Research Department of Krasnodar University of the Ministry of Internal Affairs of the Russian Federation; Candidate of Legal Sciences, Krasnodar, Russian Federation. Email: alise89@inbox.ru.
[2] Senior researcher of Kazan Innovative University named after V.G. Timiryasov (IEML), candidate of Legal Sciences; Merited Lawyer of the Republic of Tatarstan, Kazan, Russian Federation. Email: begishev@mail.ru.
[3] Professor of the Department of Criminal Law, Criminal Procedure and Criminalistics, Director of Center for Digital Economy and Financial Innovation, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs; (Miep Mgimo); Head of the Working Group on Cryptocurrency Turnover Risk Assessment at the State Duma of the Russian Federation, doctor of Juridical Sciences. Email: 12011979@list.ru.

Introduction

Since ancient times, mankind has tirelessly sought to alleviate hard work. After the mechanization of physical labor, people thought about the automation of mental processes, which for a long time was a purely human prerogative.

In the early 40s of the 20th century, due to the development of computer technology, it became possible to use the resources of its memory and processor power to create intelligent programs. With the help of computers, formal reasoning systems were implemented, and tests were carried out to ensure that they are somewhat sufficient to demonstrate reasonableness in practice. The founder of AI theory is considered an outstanding English mathematician, cryptographer, member of the Royal Society of London A. Turing. He considered that machines as well as people are possible to use the available information, as well as the mind to solve problems and make decisions, in addition, he described the test (later named after the author), which allows to determine when the machines will be able to compare with human mind. In his opinion, successful passing the test by any artificial system allows us to call it the "Artificial intelligence system" (Turing, 1950, pp. 433-460).

The term "Artificial Intelligence" (AI) was first proposed by an American computer scientist, member of the United States National Academy of Sciences, A. Turing Prize winner, John McCarthy at a seminar at the University of Dartmouth in 1956. McCarthy & Minsky proved the possibility of creating AI. The Dartmouth conference was the starting point for AI research, which has been going up and down for 70 years (McCarthy, 2006, pp.12-14.).

Artificial intelligence is widely used in education, medical care (AI will replace doctors from the disease diagnosis and prescribing treatment); pensions, logistics, retail, environmental protection (Statista, 2017), transport (by 2025, the volume of supply of AI-based systems for Autonomous vehicles will exceed $ 150 million); financial services and technology (hedge funds that use AI demonstrate much better results than those driven by people), public administration and law enforcement (Reiff, 2017). Artificial intelligence technology can accurately perceive, predict and anticipate key trends in infrastructure and social security operations. The use of artificial intelligence is becoming an important factor in the development of the digital economy of any state.

According to analysts, by 2020, the artificial intelligence market will grow to $ 5 billion due to the use of machine learning technologies and intelligent language recognition (Markets and Markets Research, 2017), and the global GDP in 2030 due to the active use of AI will grow by 14%, or 15 $ 7 trillion (PwC, 2017).

However, the average person doesn't even realize that he is using AI. So, 77% actually use a service or device with AI, while only 33% know about it (Pega, 2017).

The undoubted advantages of the introduction of AI can be seen not only by large corporations, but also by ordinary people: 61 % of the 6,000 people surveyed said that they believe that AI will make the world a better place (Arm Limited, 2017). However, the ongoing growth of investment and expand the areas of implementation of AI has led to humanity's awareness of the "reverse side" of the coin called "artificial intelligence".

The scientific and expert community has long pondered over the still unsolvable issues for humanity. Do we, modern society, understand what AI is, and what risks does its creation and turnover entail? The European Union introduces new rules for developers

and suppliers of automated computer systems solutions. Representatives of such companies will be required to explain to users how the system works, and by what principle decisions are made. The problem is that this may not be possible. Yes, it is possible to explain the basic principles of neural networks without problems, but few people can tell exactly what happens there during the processing of complex information. Even the creators of such systems cannot explain everything "from and to," because the processes that occur in the neural network during information processing are very complex.

Never before has a man created machines whose principle of operation is not completely understood by the creators themselves and is sharply different from the method of processing information used by the person himself. So, can we expect normal interaction with machines that are unpredictable? Will we be able to extract the benefits of using AI, avoiding negative consequences? Are there regulatory mechanisms for controlling AI? Is global legislation ready to regulate situations when AI will participate in the infringement of legally protected relationship? And would the title of the book "Our final invention: artificial intelligence and the end of human era" (Barrat, 2013) be prophetic?

The present study attempts to find answers to such ambiguous, and at the same time topical issues.

Methods

The study is based on a systematic analysis of the role and associated threats to cybersecurity. the Authors actively used scenario analysis to model risk-related situations. To make their expert assessments more objective, the authors used methods of analogy and prediction. The research tasks required the use of several groups of primary and secondary sources. Primary sources included official publications of Federal agencies, including security reports, statistics, public opinion polls, and media reports. Secondary sources included mainly monographs and scientific articles evaluating processes and phenomena in the field under study.

The Terminology of Artificial Intelligence

AI has been the subject of various scientific fields quite recently, which is why there is a lack of definition of its structure, as well as the range of issues that are associated with it: so, although the preconditions for the study of AI took place already at the beginning of the XVIII century, the formation of the direction refers only to the middle 40 50s XX century.

As a scientific field, AI gained weight after the end of World War II. This was due to the merits of such scientists as A. Turing (1950), W. McCulloch (1965) and W. Pitts (1943).

In 2007, in an interview to the question "What is Artificial Intelligence?" J. McCarthy replied that it was the science and development of intelligent machines and systems, especially intelligent computer programs designed to understand human intelligence. The methods used are not necessarily biologically plausible (McCarthy, 2007).

Bernard Marr rightly points out that the definitions of artificial intelligence begin to change depending on the goals that are being attempted by using the artificial intelligence system. Typically, people invest in the development of artificial intelligence for one of

these three purposes: creating systems that think exactly like people ("strong artificial intelligence"); creating systems that will work without understanding how human thinking works ("weak artificial intelligence"); the use of human thinking as a model, but not necessarily the ultimate goal (2018).

In this study, we have understood AI as a collective term for intelligent computer software (AI systems, AI technologies) that can analyze the environment, think, learn, and respond to what it "feels".

AI is a kind of intelligent system capable of making decisions on its own. This system represents the direction of the development of computer functions related to human intelligence, such as: reasoning, training, and problem solving. In other words, AI is the transfer of human capabilities of mental activity to the plane of computer and information technologies, but without inherent human vices (Afanasyev, 2018, pp. 28-34.). Scientists dealing with this issue are intensively studying the prospects for recognizing an e-face and the place of a person in such a world (Carriço, 2018, pp. 29-36.).

Kurzweil (1990) argues that AI is the prerogative of machines that require intellectual abilities when implemented by humans. However, in this case, the textual construction causes a state of uncertainty (it requires the presence of intellectual abilities), since any action, even the most elementary in its essence, can be regarded as a manifestation of intelligence. Winston (1980) in turn, considers AI a computing machine that has the ability to "do things that seem reasonable to people"(p. 11). Bellman (1978) supposes that AI is automation of actions, the group of which includes decision-making, problem solving, training (p. 57). According to Smolin (2004), "artificial intelligence" can be interpreted as a system that has the ability to purposefully change (taking into account the state of information inputs) some parameters of functioning, as well as the way of its own behavior (pp. 15-17).

We agree with Ponkin and Redkina (2018) that AI is an artificial complex cybernetic computer-software-hardware system (electronic, including virtual, electronic-mechanical, bio-electronic –mechanical or hybrid) with cognitive-functional architecture and own or relevant available (attached) computing power of the required capacities and speed (pp. 91-109). The same conclusion had been reached by Morkhat (2017, p. 138).

In modern scientific and technical literature provides a lot of different classifications of AI systems and applications. However, taking into account the methodology of this study, we adhered to the classification of AI, taking into account the applied aspects of modern information and telecommunications technology (Amores, 2013, pp. 81-105).

In the PwC study (2017) all types of AI are divided into two groups depending on the interaction with the person in their activities. Thus, AI interacting with people is usually referred to special stable systems, such as auxiliary intelligence, which helps people accomplish tasks faster and better. Stable systems are not able to learn from their interactions. This group also includes adaptive (augmented intelligence), which helps people make the right decisions and is able to self-train during interaction with a person.

The second group, which does not interact with humans, includes automated intelligence, designed to automate mechanical/cognitive and routine tasks. Its activity is not related to the implementation of new tasks and is in the field of automation of existing tasks. This group also includes "Autonomous intelligence", which in its functionality and

capabilities surpasses all previous ones, and can pose a threat to humanity and society. Such AI is able to adapt to different situations and act independently without human intervention, committing, for example, identity theft (Marron, 2008, pp. 20-38.).

Data Ethics and the Problem of Moral Choice of AI

Data ethics is developing and becoming more relevant, as evidenced by the relevant documents of states, corporations and social institutions. Defining the boundaries of ethical access to data is a complex problem that affects various stakeholders: citizens, the state, corporations, public institutions, etc., and requires a comprehensive solution.

Data ethics, as a kind of applied ethics, appeared relatively recently and does not yet have a generally accepted definition. A sufficiently accurate working definition of the term and a description of the fundamentals of data ethics are offered by the British data ethics framework. Data ethics is an emerging branch of applied ethics which describes the value judgements and approaches we make when generating, analysing and disseminating data. This includes a sound knowledge of data protection law and other relevant legislation, and the appropriate use of new technologies. It requires a holistic approach in corporating good practice in computing techniques, ethics and information assurance. A core aspect of data ethics is using data science appropriately. (British data ethics framework ,2018).

To develop AI technologies, it is necessary to use data collection and processing technologies, so on the relationship between AI and data is almost 100%. The main question today is: how to use maximum data with minimum risks? Due to modern computing power, AI technologies can analyze huge amounts of data and find complex and deeply hidden connections. However, cybersecurity is not always possible.

The greatest minds of our time Hawking (2018), Gates and Musk bring to the fore the problem of technological singularity – the moment when computers in all their manifestations will become smarter than people. According to Kurzweil (2006), when this happens, computers will be able to grow exponentially in comparison with themselves and reproduce themselves, and their intelligence will be billions of times faster than humans (p. 156). According to Bostrom (2016) in 60 years the AI will become a serious threat to humanity. By 2022, the similarity of the thinking processes of robots and humans will be about 10 %, by 2040 – 50 %, and in 2075, the thinking processes of robots can no longer be distinguished from human ones, the similarity will reach 95 %. However, the pace of technological development suggests that the process would be much faster (p. 344).

It should be noted that not only the greatest minds of mankind are concerned about the threats that carry the development of AI. In Asia there is a genuine fear that machines with AI are becoming more intelligent than people. In general, the vast majority of respondents (85 %) are concerned with ensuring the security of AI technology (ARM, 2018, p. 14).

Ethical problems associated with the use of AI can be divided into 2 groups:

1) problems related to the collection, analysis and processing of digital data;

2) problems related to making AI decisions based on generalized data.

Ethical difficulties are caused primarily by the collection, analysis and processing of citizens ' digital data-big data, social data and personal data. Businesses need them for AI training, for online advertising and online commerce, and the state needs them for making management decisions, interacting with citizens, and ensuring national security.

Due to the collection and analysis of big data using AI, technology giants are able to build correlations that people themselves cannot yet recognize.

Excessive restrictions on access to data can slow down the development of AI technologies. well-Thought-out legislation and careful enforcement would allow maintaining a balance of regulating the volume and degree of anonymization of personal data without imposing numerous prohibitions. But such legislation has yet to be created.

The second problem is related to the ethics and humanity of AI decisions. Professor Arkin, who is engaged in the development of robots for military needs, notes that his research has significant ethical risks, possible when using his developments for criminal purposes. The use of AI in wartime can save thousands of lives, but weapons that are intelligent and standalone pose a threat even to their creators.

Foreseeing the potential risks of his developments, Arkin developed a set of algorithms ("ethical guide"), which is designed to help robots to act on the battlefield: in what situations to stop the fire, in what situation to seek to minimize the number of victims (Rutkin, 2014).

However, if the potential risks of using AI in the military sphere are obvious, and scientists are already working to minimize them, the situation is quite different in the "peaceful" areas of AI application.

The use of AI inevitably leads to the problem of ethical choice. This problem is especially relevant for unmanned vehicles controlled by AI. Kingston (2016) described a hypothetical situation in 2023 where an AI-driven car moving through the city streets would knock down a pedestrian, and wondered about the criminal responsibility. Unfortunately, the situation became real at the beginning of 2018, when the unmanned vehicle of the American international company hit a woman in the US state of Arizona due to the program's features (Bergen, 2018).

In early 2016, MIT launched a large-scale study called "Moral Machine" ("Ethics for the car"), within which a special website was created, where the user of the pilot car simulated situations with various force majeure situations. Scenarios provided an opportunity to choose on the road in an emergency, whose lives to sacrifice in the first place in the event of an accident, the tragedy of which is already inevitable. Analysis of the responses showed that respondents often prefer to save people rather than animals, young people instead of the elderly. In addition, the study showed that respondents' religious preferences play a significant role in choosing the appropriate gender of a potential victim: men are less likely to leave women alive, and religious people most often prefer saving people rather than animals. Representatives of the German automobile company "Mercedes-Benz" in turn noted that their cars would give priority to passengers (Casmi, 2018). The Ministry of transport of Germany was immediately answered that to make such a choice on the basis of a number of criteria would be illegal, and in any case, the manufacturer will be responsible (Karlyuk, 2018).

Thus, it is essential to emphasize the need for a clear, rigorous and effective ethical framework in the design, construction, production, use and modification of AI.

No exception is the sphere of health care, where the introduction of AI in the process of treating and diagnosing oncological diseases has had mixed consequences. Occurred in the summer of 2018 leaked internal documents of one of the world's largest manufacturers and suppliers of hardware and software – the "IBM" company suggests that she has

developed medical AI "WatsonHealth" used in 230 hospitals worldwide for the treatment of 13 types of cancer at 84 000 patients, commit a medical error. "WatsonHealth" offers treatments that can lead

The leaked internal documents of one of the world's largest manufacturers and suppliers of hardware and software, IBM, in the summer of 2018 indicate that WatsonHealth, the medical AI developed by it, used in 230 hospitals around the world to treat 13 types of cancer at 84,000 patients makes medical errors. WatsonHealth offers incorrect treatments that can lead to the death of the patient (Kolenov, 2018).

Main Characteristics of AI that Pose a Threat to Cybersecurity

The problem of ensuring the security of confidential information is one of the key for all subjects of the digital economy, including the problem of cybersecurity using AI (Wilner, 2018, pp. 308-316). The world community is concerned about the use of AI for criminal purposes. Thus, in early 2017, the FBI held a major conference on the use of AI by law enforcement agencies and criminals. At the conference it was noted: the data of Interpol, Europol, FBI and law enforcement agencies of other countries, the results of studies of leading universities indicate the lack of activity of criminal structures to create their developments in the field of AI. According to Ovchinsky (2018), despite the lack of information about the development of cybercriminals in the field of AI, the potential for such a phenomenon exists. Cybercriminal has plenty to choose from to create their own powerful AI platforms. Almost all the development of AI with an open outcome code are containers. A container is a platform where with the help of API can mount the place any third-party programs, services, databases, etc. If earlier, when creating their own program or service, everyone had to initially develop algorithms from beginning to end, and then, using one or another programming language, translate them into code, today it is possible to create products and services in the same way as builders build a house – from standard parts delivered to the construction site (p. 150).

Thus, the processes of using AI for criminal purposes have increased public danger (Van der Wagen & Pieters, 2015, pp. 578-595). However, the use of open source communications for crime assessment seems to be a promising idea, including in the era of big data (Williams et al., 2017, pp. 320-340).

At the same time, for example, an AI error in the program of diagnosis of diseases that has made an incorrect diagnosis can lead to incorrect treatment of the patient, and as a consequence, a possible violation of his health (Momi, Ferrigno, 2010, pp. 715-727).

The analysis of trends in the creation and use of AI allowed us to identify two types of criminological risk of using AI: direct and indirect.

Direct criminological risk of using AI – the risk associated with direct effect on a person and a citizen of a danger caused by the use of AI.

These risks include:

1. AI with the ability to self-training, made the decision about the actions/inactions, constitutes a crime. Criminal act implies deliberate commission by the AI system of a socially dangerous attack on: human life and health; freedom, honor and dignity of the individual; constitutional rights and freedoms of man and citizen; public security; peace and security of mankind, which have caused socially dangerous consequences.

2. Intentional actions with the software of the AI system, which caused socially dangerous consequences. Criminal act implies illegally accessed to the system, resulting in damage or modification of its functions, as a result of which a crime was committed.

3. AI was created by criminals to commit crimes.

Criminals actively adopt AI and robotics. The IT threats that AI can generate were also analyzed in the recently published report The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (Brundage et el., 2018), developed by a group of it security experts working at Oxford, Cambridge, and Stanford universities, the Electronic Frontier Foundation and Open AI organizations, and a number of companies specializing in information security.

The researchers classified possible IT threats that could be created using AI in three ways:

a) malware attacks,
b) attacks using social engineering techniques,
c) physical attack.

The first type of IT threat is based on making it easier for hackers to detect software vulnerabilities due to the capabilities of artificial intelligence in the speed and efficiency of software analysis of various types.

The second type of IT threats is the use of "human thinking vulnerabilities" based, for example, on the use of artificial intelligence technologies for speech synthesis or the creation of "contextual" malware. These technologies will "lull the vigilance" of the person who clicks the link that its criminals need. In the same group of IT threats, the researchers placed the use of AI to disorient people in the political sphere and to monitor dissenters. AI can be used for personalized mass disinformation campaigns.

The third type of IT threat is the organization of attacks on physical objects, for example, using combat drones controlled by artificial intelligence.

Indirect criminological risk of using AI – the risk associated with unintended hazards in the context of the use of AI.

These risks include:

1. Random errors in the software of the AI system (errors made by the developer of the AI system that led to the commission of the crime.

2. Errors made by the AI system during its operation.

According to Lines and Lucivero (2014) responsibility for the actions and harm caused to the AI, is borne by the person who programmed it or the person responsible for its operation within the limits established by the law (p. 194-222).

The Problem of Criminal Prosecution for Illegal Actions of Artificial Intelligence

Analysis of foreign experience in the legal regulation of relations in the field of the use of artificial intelligence and robotics indicates the presence of several models of regulation of relations arising in connection with the use of artificial intelligence.

Many countries today quite reasonably realize that legal regulation can hardly be considered as the only or main mechanism for regulating the use of artificial intelligence. There is a fairly widespread practice of private initiatives that combine the efforts of a number of companies to develop the use of artificial intelligence technologies and consolidate the basic principles of working with such technologies. For example, Asilomar

AI principles are aimed at creating useful intelligence, maintaining human values and the confidentiality of personal data (Khisamova et al, 2019).

In the European Union, after a number of tragic incidents involving the use of unmanned aerial vehicles, the possibility of granting robot's legal status, and as a result, the possibility of bringing an electronic person (electronic subject) to justice, has been widely discussed. Thus, the resolution of the European Parliament, together with the recommendations of the Civil Law Regulation Commission on Robotics of the European Parliament of 16 February 2017 "Civil Standards on Robotics" is aimed at regulating the legal status of robots in human society through the following actions: the establishment of a special European agency for robotics and AI; development of a regulatory definition of "Autonomous intelligent robot"; development of a registration system for all versions of robots , as well as a system for their classification; development of requirements for developers to provide risk prevention guarantees; development of a new reporting structure for companies that use or need robots, which will include information about the impact of robotics and AI on the company's economic performance (Delvaux, 2016, p. 10).

It is noteworthy that the text of the resolution of the European Parliament notes the continuous change of robots, which predetermined not only the ability of robots to perform certain types of activities, but also the ability to independently study and make autonomous "independent" decisions.

However, already today there is an active discussion about giving the AI legal personality and the prospects of bringing AI to responsibility for the damage caused. Scientists have found it difficult to determine the responsible subject for AI failures (Prakken, 2016, p. 43).

Among legal scholars dealing with issues of the legal personality of AI, there are 3 key approaches:

- the endowment of AI with legal personality corresponding to human;
- giving AI legal personality similar to the legal status of a legal entity;
- the endowment of AI with limited legal personality (Robertson, 2014, p. 593).

We support the opinion that it is inappropriate to involve AI designers and developers, where the result of the final AI decision largely depends on the situation of its application and the tasks assigned to it (Morkhat, 2017, p. 233).

We agree with the opinion of Nevjans (2016) that the legal personality of AI cannot be equated with the human or legal status of a legal entity. A person with legal status acts on the basis of mental processes, guided by subjective beliefs. Behind the actions of a legal entity are individuals, without which the activities of a legal entity are impossible. AI, in turn, acts independently, without consciousness or feelings (p. 15).

The idea of recognizing AI as a subject of law contradicts such ideas about the subject of law as socio-legal value, dignity, autonomous legal will, and also conflicts with the composition of the legal relationship, the composition of the offense and is insignificant within the framework of the institution of representation. At the same time, AI does not have the necessary and sufficient characteristics of the subject of law, in particular, it does not have the potential to independently acquire and exercise subjective rights and legal obligations, to bear legal responsibility, to independently make legal decisions, it does not have its own legal interests and aspirations and so forth (Bikeev et al., 2019).

At the same time, some authors note that AI can be endowed with separate rights different from the rights of a real individual (Asaro, 2007, p.3). In this case, it is appropriate to talk about legal fiction, a technique in which a specific legal personality acts.

Hallevy (2010) notes that the mandatory elements of crime are: criminal behavior – actus reus and internal (mental) element –mens rea. It is impossible to establish a mental element and it is impossible to recognize the commission of AI as a crime (p. 178). However, as Hallevy (2010, pp. 191-192) and Kingston (2016) rightly point out, there are "serious violations ", in which the establishment of mens rea is not mandatory, and it is justified that in these circumstances the AI can be recognized as the subject of the violation. However, there are well-founded doubts about the effectiveness of traditional forms of criminal punishment, such as a fine or less ode for the purpose of re "criminal AI". (p. 276).

However, some legal scholars are of the opinion that it is necessary to bring robots and AI to criminal liability. According to Ying Hu from Yale University, special types of punishment should be provided for AI, such as deactivation, reprogramming, or assigning the status of a "criminal", which will serve as a warning to all participants (Kopfstein, 2017), Uzhov (2017, p. 360). Rehabilitation of AI can only be done through its complete reprogramming, which in a certain sense can be compared with a lobotomy against a person. That is an absolute and probably irreversible change in the properties of AI. The second way is to dispose of the machine. It is also possible to integrate the operation of the safety switch into the mechanism, as well as certain software for the immediate shutdown of all processes in emergency situations (Radutny, 2017, p. 132-141).

AI can be perceived as a non-standard legal position, different from reality. It is known that the existence of legal fictions is due to the need to bridge legal gaps and eliminate uncertainty in public relations. We believe that such a decision can remove a number of legal restrictions that exist today and prevent the active involvement of AI in the legal space.

In this regard, the forecast outlined in the resolution of the European Parliament on the possibility of granting robots a legal status is of particular interest. However, it should be noted that the legal status of an electronic person will differ significantly from the status of an individual.

Conclusion

The foregoing account information are evidence of the high crime risk of application of AI prisoners in intelligent technologies, and the weak theoretical readiness of the science of criminology to study the problem under consideration.

In the near future (approximately 10-15 years), the pace of development of systems and devices with AI will lead to the need for a total revision of all branches of law. In particular, the institutions of intellectual property, the tax regime, etc. will require deep processing, which will ultimately lead to the need to resolve the conceptual problem of endowing an autonomous AI with certain "rights" and "duties".

Today, it is not only and not so much the law that affects the development of relations in the field of using digital technologies, as the latter force the right to transform and interact with other regulators, to use digital technologies for their own purposes of self-

development at various levels of life. One of these technologies is artificial intelligence (Sidorenko, Khisamova, 2020).

In our opinion, the best way is to endow AI with a specific "limited" legal personality (through the application of legal fiction), in terms of endowing an autonomous AI with the responsibility to bear responsibility for the harm and negative consequences.

This approach will undoubtedly require a rethinking of the key postulates and principles of criminal law, in particular, the institutions of the subject and the subjective side of the crime. At the same time, in our opinion, the AI systems will require the creation of an independent institution of criminal law, unique in its essence and content, different from the traditional anthropocentric approach. Such a legal institution requires a completely new approach. Within the framework of this institution, it seems appropriate to provide for different from the traditional understanding of the subject, based on the symbiosis of technical and other characteristics of AI, as well as alternative types of responsibility, such as deactivation, reprogramming or endowing with the status of "criminal", which will serve as a warning for all participants of legal relations. We believe that such a solution in the future can minimize the criminological risks of using AI.

References

Afanasyev, A. (2018). Artificial intelligence or intelligence of subjects of detection, disclosure and investigation of crimes: what will win? *Library CSL. Scientific journal*, № *3*(38), 28-34.

Amores, J. (2013). Multiple instance classification: review, taxonomy and comparative study. *Artificial Intelligence*, *201*, 81-105.

ARM (2018). *AI today. AI tomorrow. Awareness, acceptance and anticipation of AI: a global consumer perspective*. Retrieved from: https://pages.arm.com/rs/312-SAX-488/images/arm-ai-survey-report.pdf.

Arm Limited (2017). *Global Artificial Intelligence Survey.* Retrieved from: http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence.

Asaro, P. M. (2007). *Robots and Responsibility from a Legal Perspective*. Internet-site of Dr. Peter M. Asaro, 2007, 5. – Retrieved from: http://www.peterasaro.org/writing/ASARO%20Legal%20Perspective.pdf.

Barrat D. (2013). *Humanity's Latest invention: Artificial intelligence and the end of the era of Homo sapiens*. New York: Thomas Dunne Books, St. Martin's Press.

Bellman, R.E. (1978). *An introduction to artificial intelligence: can computers think? Thomson course technology*. San Francisco: Boyd &. Fraser Publishing Company; Thomson Course Technology, 146.

Bergen, M. (2018, March 19). *Uber halts autonomous car tests after fatal crash in Arizona Bloomberg.* Retrieved from: https://www.bloomberg.com/news/articles/2018-03-19/uber-autonomous-car-involved-in-fatal-crash-in-arizona.

Bikeev, I., Kabanov, P., Begishev, I., & Khisamova, Z. (2019). *Criminological risks and legal aspects of artificial intelligence implementation.* In Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing (AIIPCC '19). Association for Computing Machinery, New York, NY, USA, 1–7.

Bostrom, N. (2016). *Strategic Implications of Openness in AI Development*. Technical Report, 1. Retrieved from: https://www.fhi.ox.ac.uk/reports/2016-1.pdf.

British Data Ethics Framework Guidance. (2018). Retrieved from: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework.

Brundage, M., Avin, Sh., Clark, J., Toner, H., Eckersley, P. Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, Th., Filar, B., Anderson, H., Roff, H., Allen, G., Steinhardt, J. , Flynn, C., Heigeartaigh, S., Beard, S., Belfield, H., & Farquhar, S., Amodei, D. (2018). *The malicious use of artificial intelligence: forecasting, prevention, and mitigation.* Retrieved from: https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf.

Carriço, G. (2018). The EU and artificial intelligence: a human-centred perspective. *European View*, 17 (1), 29-36.

Casmi, E. (2018, October, 26). *Opinion of millions of people: autonomous cars have to push the elderly and the young to save.* The Network edition "Cnews". Retrieved from: http: //www.cnews.ru/news/top/2018-10-26_mnenie_millionov_chelovek_bespilotnye_avto_dolzhny.

Delvaux, M. (2016). *Draft Report with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)). Committee on Legal Affairs, European Parliament, PE582.443v01-00, 22 p. Retrieved from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=%2F%2FEP%2F%2FNONSGML%20COMPARL%20PE-582.443%2001%20DOC%20PDF%20V0%2F%2FEN.

Hallevy, G. (2010). The criminal liability of artificial intelligence entities – from science fiction to legal social control. *Akron Intellectual Property Journal*, *4*(2), 171-201.

Hawking, S. (2018) *Brief Answers to the Big Questions.* London: Random House LLC, 2018, 256.

Karlyuk, M. V. (2018) *Investments in the future: artificial intelligence. Non-profit partnership "Russian Council for international Affairs"*. Retrieved from: http://russiancouncil.ru/analytics-and-comments/analytics/eticheskie-i-pravovye-voprosy-iskusstvennogo-intellekta.

Khisamova, Z. I., Begishev, I. R., & Gaifutdinov, R. R. (2019) On methods to legal regulation of artificial intelligence in the world. *International journal of innovative technology and exploring engineering (IJITEE)*. *9*(1).

Kingston, J. K. (2016) *Artificial intelligence and legal liability*. Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV: Conference Paper, 269-279.

Kolenov, S. (2018, July 27) *AI-oncologist IBM Watson was convicted of medical errors. Network edition "Hightech.plus"* Retrieved from: https://hightech.plus/2018/07/27/ii-onkologa-ibm-watson-ulichili-vo-vrachebnih-oshibkah.

Kopfstein, J. (2017). *Should Robots Be Punished for Committing Crimes?* Vocativ Website. Retrieved from: https://www.vocativ.com/417732/robots-punished-committing-crimes.

Kurzweil, R. (1990.) *The Age of Intelligent Machines*. Cambridge MIT Press.

Kurzweil, R. (2006). *The singularity is near: when humans transcend biology.* Penguin Books, 672.

Leenes, R., & Lucivero, F. (2014). Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behavior by Design. Law, Innovation and Technology, *6*(2), 194-222.

Markets and Markets Research Private Ltd. (2018). *AI in Fintech Market by Component (Solution, Service), Application Area (Virtual Assistant, Business Analytics & Reporting, Customer Behavioral Analytics), Deployment Mode (Cloud, On-Premises), and Region. Global forecast to 2022.* Retrieved from: https://www.marketsandmarkets.com/Market-Reports/ai-in-fintech-market-34074774.html.

Marr, B. (2018). *The key definitions of Artificial Intelligence (AI) that explain its importance.* Retrieved from: https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial intelligence-ai-that-explain-its-importance/#4da358124f5d.

Marron, D. (2018). Alter Reality: Governing the Risk of Identity Theft. *The British Journal of Criminology*, *48*(1), 20-38.

McCarthy, J. (2007, November 12). *What is artificial intelligence?* Computer Science Department Stanford University. Retrieved from: www-formal.stanford.edu/jmc/whatisai.pdf.

McCarthy, J., Minsk, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. August 31, 1955. *AI Magazine*, *27*(4), 12-14.

McCulloch, W. S. (1965). *Embodiments of Mind. Cambridge*, MA: MIT Press.

Momi, E. De., Ferrigno, G. (2010). *Robotic and artificial intelligence for keyhole neurosurgery: the ROBOCAST project, a multi-modal autonomous path planner.* Proceedings of the Institution of Mechanical Engineers, part H: Journal of Engineering in Medicine, *224*(5), 715-727.

Morkhat, P. M. (2017). *Artificial intelligence: legal view.* M.: BukiVedi, 257.

Nevjans, N. (2016). *European civil law rules in robotics: study. Policy Department C: «Citizens' Rights and Constitutional Affairs», European Parliament's Committee on Legal Affairs. PE 571.379, 15.* Retrieved from: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU%282016%29571379_EN.pdf.

Ovchinsky, V. S. (2018) *Criminology of the digital world.* M.: Norm: INFRA–M, 352.

Pega (2017). *What Consumers Really Think About AI.* Retrieved from: https://www1.pega.com/system/files/resources/2017-11/what-consumers-really-think-of-ai-infographic.pdf.

Pitts, H. W. (1942) Some observations on the simple neuron circuit. *Bulletin of Mathematical Biophysics*, 4 (3), 121-129.

Ponkin, I. V., & Redkina, A. I. (2018) Artificial intelligence from the point of view of law. *Bulletin of the Russian University of friendship of peoples. Series: Legal Sciences*, 1 (22), 91-109.

Prakken, H. (2016). *How AI & law can help autonomous systems obey the law: a position paper*. In Proceedings of the 22nd European conference on artificial intelligence workshop on artificial intelligence for justice. Hague: VU University Amsterdam, 42-

46. Retrieved from: http://www.ai.rug.nl/~verheij/AI4J/papers/AI4J_paper_12_prakken.pdf.

PwC (2017). *Artificial intelligence: do not miss the benefit.* Retrieved from: https://www.pwc.ru/ru/press-releases/2017/artificial-intelligence-enlargement.html.

Radutniy, O. E. (2017). Criminal liability of the artificial intelligence. *Problems of legality*, 138, 132-141.

Reiff, N. (2017). Artificial intelligence hedge funds outperforming humans. *Investopedia.* Retrieved from: https://www.investopedia.com/news/artificial-intelligence-hedge-funds-outperforming-humans/#ixzz4YszizhII.

Robertson, J. (2014). Human rights vs. robot rights: forecasts from Japan. *Critical Asian studies*, 46 (4), 571-598.

Román, J. A., Rodríguez, S., Corchado, J. M., Carrascosa, C., & Ossowski, S. (2015). Specialization: a new way to improve intelligent systems. *International Journal of Artificial Intelligence*, *13*(1), 58-73.

Rutkin, A. (2014, September 13). The robot's dilemma. *Magazine issue*. 2986.

Sidorenko, E. L., & Khisamova, Z. I. (2020). *The readiness of the economy for digitalization: basic methodological approaches.* Digital Age: Chances, Challenges and Future. ISCDTE 2019. Lecture Notes in Networks and Systems, 84.

Smolin, D.V. (2004). *Introduction to Artificial Intelligence*: Lecture notes. M: Fizmatlit, 208.

Statista (2017). *Artificial Intelligence.* Report. Retrieved from: https://www.statista.com/study/50485/artificial-intelligence/

Turing, A. (1950). Computing Machinery and Intelligence. *Mind, New Series*, 59 (236), 433-460.

Uzhov, F. W. (2017). Artificial intelligence as subject rights. *Gaps in Russian legislation*, *3*, 357-360.

Van der Wagen, W., Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *The British Journal of Criminology*, *55*(3), 578-595.

Williams, M. L., Burnap P., & Sloan L. (2017). Crime Sensing with Big Data: The Affordances and Limitations of using open-source communications to estimate crime patterns. *The British Journal of Criminology*, *57*(2), 320-340.

Wilner, A. (2018). Cybersecurity and its discontinuities: Artificial intelligence, the Internet of things, and digital misinformation. *International Journal*, *73*(2), 308-316.

Winston, P.G. (1980). *Artificial Intelligence*. Mir, 520.