



LEGAL MECHANISMS FOR ENSURING PRIVACY IN THE USE OF ARTIFICIAL INTELLIGENCE

Madiev Fakhriddin

Tashkent State Law University
Senior lecturer of the Department of Constitutional Law
+99890 805 2472 / fmadiev92@gmail.com
OrchidID: 0000-0002-3034-7334

Article history:	Abstract:
Received: June 6 th 2023 Accepted: July 4 th 2023 Published: August 4 th 2023	Legal mechanisms for ensuring privacy in the use of artificial intelligence, the widespread introduction of AI technologies in the life of our society, and the need to carry out scientific research on ensuring the privacy of citizens living in our country. Therefore, it is necessary to study and analyze the concept of the right to privacy from a conceptual, scientific and methodological point of view.
Keywords: Digitization, privacy, privacy, personal data, protection from interference with personal life, protection from interference with personal life, non-disclosure of information concerning honor and dignity without their consent, personal identification data.	

As we know, today the space of information and communications is rapidly developing, and this also affects the human factor. As we live in the information age, we cannot imagine our life without technology. On the one hand, the use of technology has become one of the necessary measures, and on the other hand, how to ensure human rights during its use has become one of the urgent problems. One of such legal problems is the issue of ensuring the right to privacy.[1]

Artificial intelligence emerging in the form of technology and applications programmed for it, on the one hand, serves to ease the burden of the human factor and create convenience for it. But at the same time, these technical manuals are also endangering our lives. However, the more technical risk arises, the more necessary it is to create other technical means for its prevention and countermeasures. The most popular of such risks and the most important to protect is the violation of the right to privacy [2].

We are witnessing that such violations occur in any information and communication means, mobile communication techniques. The creation of algorithmic programs to prevent such violations and the legal regulation of such programs are among the most urgent problems of today.[3]

Before looking at solutions to these problems, first, what is artificial intelligence and what is its history? "what is it used for?" "What are its advantages and disadvantages?" It would be appropriate if we could put such questions in front of us and answer these questions in detail.

Artificial intelligence is a technological feature created entirely by artificial means and works only by using the operating system of machines without

using any living organisms by imitating human characteristics and behavior. These features are from many of the applications we use on our phones, such as navigation, facial recognition systems, and more. Also, in these applications, artificial intelligence is increasingly used as part of creating algorithms based on stored data. Although artificial intelligence offers simple solutions to our lives through applications, it is a technology that is much more complex than applications and cannot know in advance how it will work or what commands it will execute.[4]

According to experts, many companies have started to integrate artificial intelligence into the technologies they use, based on the experience gained and the increased use of online in our lives and the increased need for electronic systems due to the pandemic. This has led to a further increase in the level of popularization of artificial intelligence. But the companies could not fully ensure the security of these systems. Many companies have experienced data loss. Even when they provide these valuable technologies, they face the risk of data loss due to their unpredictable nature. For this reason, artificial intelligence, which offers simple solutions in people's lives, has been assessed as a serious threat to fundamental rights and freedoms.[5]

If we turn to the history of artificial intelligence, it has a long history. The emergence of artificial intelligence, according to experts, mil. avv. It dates back to the 1st century. During this period, a device for predicting astronomical events was created in Greece. This equipment is also said to have artificial intelligence. First, in 1950, Alan Turing proved the possibility of using mathematical artificial intelligence. That is, a computer



such as artificial intelligence was created, this computer executed the given command, but did not have the ability to remember. And today's Artificial Intelligence has the ability to remember and can refresh its memory. It is with this quality that he can imitate the human mind. This gives him the opportunity to think like a human, and you will see whether artificial intelligence will become your assistant. After that, in 1956, the first artificial intelligence program was demonstrated at Dartmouth University. [6]

The term artificial intelligence was first used in 1958 (in English - Artificial Intelligence (AI)) by the American scientist John McCarthy, who succeeded in creating an artificial intelligence named Lips. After that, artificial intelligence (AI) began to develop rapidly during the years 1957-1974. In the 1970s, scientists predicted the creation of artificial intelligence equal to human consciousness within 3-8 years. By the 1980s, much larger investments were being made in artificial intelligence. By 1997, an artificial intelligence named Deep Blue had defeated world chess champion Garry Kasparov in a chess tournament, making artificial intelligence a global news story.[7]

Since then, many artificial intelligence devices and programs have been created. They are programmed into our computers and mobile phones that we use in our daily life in the form of applications. Today, the most popular and popular of them is Google software. This program was founded on September 4, 1998. Google is a form of early artificial intelligence in the Internet world. Later, a speech recognizer version of artificial intelligence called Dragon was created. To date, such types of artificial intelligence as Chat GPT, Big, Meet Journey have been developed and presented to the public.[8]

Although briefly, we described the concept of artificial intelligence and the history of its origin. Now, to better understand the concept of artificial intelligence and have more detailed information about it, it would be more appropriate to dwell on how these programs work. The general working system of artificial intelligence consists of five stages:

- **Information Department;**
- **Hypothesis;**
- **Analytical department;**
- **Memoirs Department;**
- **Summary section.**

In these stages, the following actions are performed:

✓ In the data department, the artificial intelligence performs the preliminary process to execute the order made by the customer. In this process, all information in the virtual world is collected;

✓ Then automatically the artificial intelligence goes to the second section, where it collects

the necessary information to execute the command and transmits it to the analysis section;

✓ begins the process of analyzing the data collected there. As a result of the analysis, he collects information suitable for the order given by the customer and forms it in his mind. The thinking of artificial intelligence is done in this section. It is this section that generates the results and formulates the answer you need;

✓ The generated information is stored in the fourth section, which is the memory section;

✓ And finally, in the last section - the conclusion, the database is formed and the answer you need is presented. You want to present some task or task, question to the artificial intelligence and spend a lot of time on it. But it only takes seconds for artificial intelligence to perform these tasks and provide you with an answer.[9]

We have given an overview of how artificial intelligence works above. Now we will explain in detail how and on what basis the working process of Artificial Intelligence is realized. Artificial intelligence is the imitation of the problem-solving and decision-making of the human mind in computers and machines. They work with large amounts of data to make intelligent decisions and analyze that data to generate answers based on that data. It performs these tasks with the help of Machine Learning and Deep Learning. Computers are trained by humans through neural networks.

What are Neural Networks? in other words, it is known from medicine that neural networks exist in the human brain, and a neuron, i.e. a neuron, is the main structural and functional unit of the nervous system, consisting of short dendrites and a long axon.[10]

It is those neurons that are artificially installed in the artificial mind. Neural networks ensure knowing exactly what shape it is, regardless of what shape it is. That is, we can draw a shape with the same name on a plain paper and reflect these shapes in different ways. For example, we want to write the number seven, and we can depict it vertically, slightly deviated to the right or left, and no matter how we write this shape, we know in our mind that it is the number seven, and we can say the number seven. The modern types of artificial intelligence that are being created today have developed the ability to know such forms. Until now, robots have been taught to recognize written forms in exactly the same way.

For example, when we use various social networks or applications, we are asked to create a profile and are told that we need to encrypt this profile or account to protect it. The system that gives this command, which is not visible to us, is also artificial intelligence. It's just that artificial intelligence is not very developed. Let's look at this process step by step:



➤ we enter our personal data in our profile-account, which consists of name, surname, patronymic, date of birth, month, year and phone number;

➤ after that, we will need to enter a code to protect our profile-account from external influences and risks;

➤ Before entering the code, we enter our personal information in the application command, and at the end, we are asked to confirm that we are not a robot. Only by solving that test can we confirm that we are not robots;

➤ If we pay attention to this test, this test will combine different forms, and we will have to define those that are in different ways but have the same form or appearance and meaning;

➤ Only if we solve the test correctly will we be allowed to proceed to the next process or complete the work.

This example alone shows how artificial intelligence works, what kind of consciousness it has. So artificial intelligence itself can check that we are not artificial. But the types of artificial intelligence that have been created so far have not been able to solve such tests. Newly developed artificial intelligence systems created in 2023 are said by experts to be able to solve even these tests. This shows that the danger of artificial intelligence has increased. Advanced artificial intelligence can even undermine the security of our social network sites, profiles, accounts and other personal information. In such a situation, the protection of our personal data will be at risk and the possibility of violation of our right to privacy will increase.

Also, based on the scope of our topic, we met with experts about artificial intelligence and collected information from them. Based on this information, we gained the following knowledge. That is, the neural network creates conditions for artificial intelligence to see, learn and recognize. Such neural networks are called pixel-neurons.

A neural network consists of three parts:

1. **In put** - part that receives data;
2. **Hidden- layer** is a hidden layer, the main work is done here ;
3. **Out put** is the part that transmits the generated responses.[11]

The more information is fed into an artificial intelligence's neural network, the more it can remember. It will evolve based on the information it has generated and will have the ability to provide you with faster, easier and better answers the next time you enter that same information. In such situations, it becomes difficult to believe that it is done by artificial intelligence. Artificial intelligence uses statistics as a basis. This is how the neural network of artificial

intelligence works, just as the human brain works. For example, humans also use statistics as a basis, that is, we guess and answer based on the information we have seen and have before. Artificial intelligence also collects information from data and sound waves in the virtual world and stores it in a database.[12]

There are three types of artificial intelligence in terms of strength and weakness:

1) ANI - Artificial Narrow Intelligence - the weakest artificial intelligence;

2) AGI - Artificial General Intelligence - artificial intelligence with general power (for example, Google);

3) ASI - Artificial Super Intelligence - the strongest artificial intelligence (experts say that such AIs have not yet been created, but there is a possibility of their creation).[13]

Above we gave detailed information about artificial intelligence. But along with its benefits, it also has its disadvantages. Especially in the field of law, this can cause negative consequences. This is clearly manifested in the violation of the right to privacy, which is established and guaranteed in our basic law - the Constitution.

As a result of the development of artificial intelligence, how can we ensure the privacy of our personal data? Below is a look at the consequences if our personal information is not kept private and protected in the virtual space.

First, the privacy of our personal data is convenient for us, because it will not be possible to use our personal data for malicious purposes.

Secondly, ensuring the confidentiality and protection of our personal data leads to ensuring the right to privacy. If our personal information is disclosed, using it may serve as a causative factor that threatens our honor, reputation, dignity, free and inviolable life.

Third, it poses risks to our use of electronic services. For example, we connect and use our personal cards in electronic applications to make payments from our credit cards , and if our personal information is disclosed and not protected, our account funds can be withdrawn, and this is certainly harmful to our economy.

Fourthly, the national site - my.gov.uz, which is used as the government's electronic desk, contains personal information about citizens of the Republic of Uzbekistan. But its privacy and protection are not sufficiently ensured. If our personal information is not kept private and secure, it can be seen by other people and used for their malicious purposes.

It is worth mentioning here that almost all information about us is stored on the my.gov.uz site, and we will be able to access it through our personal One ID. But other people have access to this information. That is, if you have the series and number



of another person's passport or ID, you can easily access his personal office and get information about him through this site. This will cause many negative consequences and create the ground for the commission of various other offenses.

Fifth, it is possible to post photos and videos on various social networks, but its protection is not ensured. Anyone who has created a personal account on social networks can post his or someone else's photos and videos on these networks. On the one hand, this is the right of the owner of that account, but on the other hand, it can serve as a causal factor for committing the crime of extortion. That is, photos and videos are also personal information and they can be photoshopped and damage the reputation and honor of the person. Or it can be used for financial gain by threatening to distribute his pictures and videos with malicious intent. In order to prevent such crimes, it is necessary to ensure the privacy of personal data and its protection.

Artificial intelligence has many benefits for our lives, but according to scientists, in particular, the business investor, engineer and inventor - Elon Reeve Musk, as well as the founder, CEO, chief engineer of SpaceX, Tesla Inc. and founder and CEO of Neuralink, co-founder and chairman of SolarCity, co-chairman of OpenAI, and founder of X.com, which merged with Confinity to become PayPal, has described artificial intelligence as a major threat to human civilization.[14] Experts say that it can cause many negative consequences for humanity.

Above, we discussed the advantages and disadvantages of artificial intelligence for the human factor. We have witnessed many events and processes in our life and we know that these events and processes have both positive and negative sides. When we think, we can see both sides of every thing and phenomenon and we look for ways to use it, introduce it into our lives, and protect ourselves from negative consequences as a result of mastering its positive aspects. Sometimes we find solutions to these problems by studying deeply and sometimes by just thinking. We need to know how to introduce artificial intelligence into our lives, how to use it, and how to protect ourselves from its negative consequences.

Especially today, as a result of the development of digital technologies, we are experiencing rapid development and growth processes in our lives.

Naturally, we have to accept and adapt to such changes. Otherwise, we may lag behind development and progress, which may create dangerous situations for future generations. We need to prevent such risks and make changes and additions to our legislation.

At the same time, issues of ensuring privacy in the context of artificial intelligence are becoming one of the most urgent problems for humanity. [15] The experience of developed countries in the field of law shows that privacy, that is, ensuring the confidentiality of information and their protection, has become a legal problem in today's digital technology era. Of course, legal states that have made great progress in the field of technology and law are suggesting that trends to eliminate these problems should be developed and put into practice. [16]

As a result of studying and conducting research on this topic, we were able to develop a number of proposals and recommendations to ensure and protect the privacy of personal information. [17] That is, in the age of digital technologies, it is appropriate to use artificial intelligence itself to ensure the protection of personal data in the conditions of using artificial intelligence. [18]

In order to protect personal data, privacy risk, privacy policy, privacy officer, privacy engineering, internet officer) to create artificial intelligence programs and implement legal regulatory measures in our legislation.[19]¹ We developed these proposals using the experience of developed countries and as a result of studying the topic.[20]²

In conclusion, we can say that the right to privacy never loses its importance as long as a person lives. The reason is that this gift was given to man by the Creator himself, and it is inalienable and sacred. Therefore, no one will ever be allowed to take this right away from us anywhere, and it must be ensured at all times, under any circumstances.

REFERENCES

1. Fakhridin, M. (2023). STAGES OF DEVELOPMENT OF THE CONSTITUTIONAL GUARANTEES OF THE RIGHT TO PRIVACY IN UZBEKISTAN. *World Bulletin of Management and Law*, 19, 67-72.
2. <https://www.inspiringapps.com/Blog/94/personal-privacy-in-the-digital-age/>.

¹ Тикашева, Г. (2022). ОБЕСПЕЧЕНИЕ ПРАВ РЕБЁНКА В РЕСПУБЛИКЕ УЗБЕКИСТАН И НЕКОТОРЫЕ ПРЕДЛОЖЕНИЯ В ЭТОЙ СФЕРЕ. *Zamonaviy dunyoda innovatsion tadqiqotlar: Nazariya va amaliyot*, 1(22), 93-95

² Анварова Д. А. ХОТИН-ҚИЗЛАР ИЖТИМОЙ ҲУҚУҚЛАРИНИ ТАЪМИНЛАШНИНГ ТАШКИЛИЙ ҲУҚУҚИЙ

МЕХАНИЗМЛАРИНИ ТАКОМИЛЛАШТИРИШ //SIYOSATSHUNOSLIK, HUQUQ VA XALQARO MUNOSABATLAR JURNALI. – 2023. – Т. 2. – №. 2. – С. 17-24.



3. Fakhridin M. STAGES OF DEVELOPMENT OF THE CONSTITUTIONAL GUARANTEES OF THE RIGHT TO PRIVACY IN UZBEKISTAN //World Bulletin of Management and Law. - 2023. - T. 19. - S. 67-72.
4. Council of Europe, Artificial Intelligence and Data Protection, Published in Council of Europe, November 2019, <https://edoc.coe.int/en/artificial-intelligence/8254-artificial-intelligence-and-data-protection.html>.
5. RM Zulunov "Use of artificial intelligence technologies", Journal of Integrated Education and Research 1 (6) 53-56, 2022, <https://ojs.rmasav.com/index.php/ojs/article/view/427>.
6. https://en.wikipedia.org/wiki/Artificial_intelligence .
7. <https://jolt.law.harvard.edu/digest/a-primer-on-using-artificial-intelligence-in-the-legal-profession> .
8. https://en.wikipedia.org/wiki/Artificial_intelligence .
9. <https://www.javatpoint.com/types-of-artificial-intelligence> .
10. National encyclopedia of Uzbekistan, Volume One. Tashkent, 2000, <https://n.ziyouz.com/kutubkhona/category/11-o-zbekiston-milliy-ensiklopediyasi>.
11. https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_quick_guide.htm .
12. <https://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?article=1405&context=fs> .
13. <https://www.javatpoint.com/types-of-artificial-intelligence> .
14. <https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-ai-is-more-dangerous-than-nuclear-weapons.html> .
15. <https://www.accessnow.org/un-privacy-resolution/> .
16. Hashim Uguli MF PROSPECTS OF INTRODUCTION OF PRIVACY PROTECTION SYSTEM IN VIRTUAL SPACE //E Conference Zone. - 2023. - S. 27-31.
17. Тикашева, Г. (2022). ОБЕСПЕЧЕНИЕ ПРАВ РЕБЁНКА В РЕСПУБЛИКЕ УЗБЕКИСТАН И НЕКОТОРЫЕ ПРЕДЛОЖЕНИЯ В ЭТОЙ СФЕРЕ. Zamonaviy dunyoda innovatsion tadqiqotlar: Nazariya va amaliyot, 1(22), 93-95
18. Анварова Д. А. ХОТИН-ҚИЗЛАР ИЖТИМОЙИЙ ҲУҚУҚЛАРИНИ ТАЪМИНЛАШНИНГ ТАШКИЛИЙ ҲУҚУҚИЙ
19. Tirkasheva, G. (2022). CYBERBULLYING AMONG CHILDREN: CONCEPT, MODERN FORMS AND DEFENSE MECHANISMS.

*Collection of scientific papers «SCIENTIA»,
(April 22, 2022; Chicago, USA), 64-65.*