Russian experience of using digital technologies and legal risks of AI

Elena Trikoz[1,*], *Elena* Gulyaeva[2], and *Konstantin* Belyaev[3]

[1] Moscow State Institute of International Relations (MGIMO University), Peoples' Friendship University of Russia (RUDN University), Moscow, Russia;
[2] Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Moscow, Russia
[3] Company Garant; Russian New University (RosNOU) Moscow, Russia

Abstract. The aim of the present article is to analyze the Russian experience of using digital technologies in law and legal risks of artificial intelligence (AI). The result of the present research is the author's conclusion on the necessity of the practical implementation of legal provisions in this area, and their judicial enforcement in federal subjects with the aim of compliance with international standards of human rights. The authors concluded that in the Russian Federation, there is no normative and technical regulation of the process of destruction of personal data, which creates serious problems for operators. The research methodology based on general scientific and private scientific methods of cognition (the dialectical method, methods of analysis and synthesis, deduction and induction, comparative legal and historical legal methods). Moreover, the range of legislative and law enforcement problems in the field of using AI technology is very extensive. For this reason, the authors of the article used the methodology for collecting data on legislative acts and legal regulation in the field under research. A number of federal and regional legal acts were analyzed using systemic-structural and formal-dogmatic methods, including the research of their practical orientation and effectiveness for modern challenges.

1 Introduction

Scientific and technological progress so far allows the creation of the so-called «weak» artificial intelligence (hereinafter – AI), which does not have its own consciousness. Nevertheless, today this technology has a generalizing ability at the heart of its algorithm and due to this factor; artificial intelligence is able to create results going beyond the design of the developers.

Today, AI is already used to free humans from monotonous work by automatically creating software; decision support; automation of hazardous types of work; support of communication between people [1]. In the not too distant future, AI technology is going to become basic as the Internet and cellular communications. At the same time, AI is a

* Corresponding author: alena_trikoz@mail.ru

centralized system for storing and processing data, in contrast to the blockchain, with the decentralized technology.

If in 2017 only five countries in the world were planning the development of AI technologies, then at the beginning of 2020 their number had already increased over 30. Russia with its digital technologies and the introduction of AI has serious competitive advantages considering its mathematics schools. The relevance is due to the dynamic development of digital technologies and the transition of state bodies of the Russian Federation and legal entities to a digital method of exchanging legally significant information in the field of public services, performing public functions, and expanding public-private partnerships within the ecosystem of the digital economy in the Russian Federation.

A number of products of Russian developers with their solutions in the field of digital technologies can be considered as the examples of the AI integration into the everyday life:

«Yandex» company, which is developing a control system for unmanned vehicles and created a virtual voice assistant Alice; 2) «VisionLabs Luna» face recognition platform; 3) «ABBYY» with its solutions in the field of text recognition and linguistics; 4) Russian software the «Vera» robot for effective casting of candidates and interviews; 5) personalized advertising system «MyTarget» for Mail Group users; 6) library of conversational AI – «DeepPavlov» for natural language processing and complex dialog systems; 7) software from the company «Wikium» for the analysis, visualization of brain activity and enhance the cognitive abilities of users; 8) Patent search system «PatSearch» from Rospatent, in which AI methods are used during the examination of applications for inventions and utility models. At the same time, a number of areas in the Russian Federation remain unaffected by digital technologies and AI.

According to the President of the Russian Federation, «the development of artificial intelligence is a matter of national security and the survival of our State. The capabilities of artificial intelligence will affect all spheres of life, both defense and the rate of economic development» [2]. Not so long ago, at a meeting on the development of information and communication technologies, the President Vladimir Putin instructed the Government of the Russian Federation to take measures to approve a separate federal project «Artificial Intelligence» by August 31, 2020.

In August 2020, the news was confirmed for the Russian Federation as the host country of the XXth UN «Internet Governance Forum» [3], which will be held in 2025 in Moscow as one of the main international events to discuss development of the Internet and digital technologies, cybersecurity and personal data protection issues, «Internet of things», AI, blockchain and big data.

What legal and organizational-practical issues arise when AI technologies are introduced into legal circulation and functioning in Russia? In this study, we are going to consider the most «hot issues» of legal regulation and practical use of digital technologies in Russia, namely: 1) the legal definition of the concept of «artificial intelligence»; 2) the legislative framework in Russia for the fields of application of AI; 3) security and confidentiality of data, legal responsibility; 4) an experimental «legal regime» of AI in Moscow and the federal subjects of the Russian Federation; 5) ethics of data circulation and use of AI in Russia; 6) intellectual property in the field of AI functioning; 7) the functioning of big data technology; 8) the use of AI technology on the example of the products of the company «Garant».

2 Methodology

In the Russian Federation, the range of legislative and law enforcement problems in the field of using AI technology is very extensive. For this reason, the authors of the article

used the methodology for collecting data on legislative acts and legal regulation in the field under study. A number of federal and regional legal acts were analyzed using systemic-structural and formal-dogmatic methods, including the research of their practical orientation and effectiveness for modern challenges.

3 Results

3.1. The concept of artificial intelligence in Russian law

The legislative definition of AI was first formulated in the Decree of the President of the Russian Federation dated 10.10.2019, which also approved the «National Strategy for the Development of Artificial Intelligence for the Period until 2030». It is understood as a complex of technological solutions that allows to simulate human cognitive functions and obtain results comparable, at least, to the results of human intellectual activity.

At the same time, it is separately noted that simulation includes self-learning and search for solutions without a predetermined algorithm. It is important to pay attention to the fact that the definition fully covers the currently available types of artificial intelligence in a broad sense: artificial intelligence working on the basis of predetermined tasks (existing knowledge), and artificial intelligence working autonomously, that is, a technology that performing tasks can potentially completely replace a person.

3.2. Legislative base in Russia by industry of AI application

In Russia, the Doctrine of Information Security of the Russian Federation No. 4 is in force. Here, the «information sphere» means a set of information, objects of informatization, information systems, sites on the «Internet», communication networks, information technologies and subjects whose activities are related to the formation and processing of information, the development and use of these technologies, ensuring information security, as well as a set of mechanisms for regulating the relevant social relations.

Within the ensure information security measures in the Russian Federation, among other things, purely legal measures to detect, prevent, repel information threats and eliminate their consequences were named. The Doctrine emphasizes that the likelihood of information threats increases significantly in connection with the practice of information technologies without linking them to ensuring information security. The development of the national management system for the Russian segment of the Internet, increasing the security of the critical information infrastructure and the stability of its functioning, as well as ensuring the security of information transmitted through it and processed in information systems on the territory of the Russian Federation. As a result, a year later a special law on the security of critical information infrastructure was passed [5].

Since October 2019, the so-called digital rights law, providing for the amendments to the Civil Code of the Russian Federation has come into force [6]. So, in the new article 141.1 of the Civil Code of the Russian Federation, it is established that the content and conditions for the exercise of digital rights will be determined by the rules of the information system, which has to meet the characteristics established by law. The holder of a digital right is to be one who, in accordance with the rules of the information system, is able to dispose of this right. Disposal of digital rights is possible only in the information system without contacting a third party. In addition, the written form of the contract is equivalent to the conclusion of a transaction through electronic or other technical means. However, it is prohibited to draw up a will using electronic or other technical means. Finally, this law introduced «self-executing» transactions, or smart contracts, into the Civil

Code of the Russian Federation, which are considered concluded and valid when performed remotely, for example, by sending SMS or filling out a form on the Internet. The creation of an agreement on the delivery of services for the information provision is introduced with the condition of its nondisclosure to third parties to ensure the protection of the collection and processing of significant amounts of impersonal information («big data»).

On January 1, 2020, the Federal Law of December 16, 2019 No. 439-FZ «On Amendments to the Labor Code of the Russian Federation Regarding the Formation of Information on Labor Activity in Electronic Form» came into force to ensure the seamless transition to the formation of basic information on labor activities and work experience of the employee in electronic form instead of paper employment history. Such electronic employment histories designed to save business, personnel departments of companies from unnecessary labor costs. In addition, they will help minimize the risk of employees losing information about their work experience; relieve them of the obligation to restore data on where and how long they worked. The situation where, due to the reorganization or liquidation of the organization, an employee cannot confirm his length of service will become outdated.

3.3. Data security, confidentiality of information, and legal responsibility in the field of digital technologies and AI in Russia

In the Russian Federation, there is special legislation on the security of critical information infrastructure (hereinafter – CII) while being under computer attack. The subjects of CII include: government agencies and state institutions, Russian legal entities and sole proprietors which, on the basis of ownership, lease or other legal basis, are in possession of information systems, information and telecommunication networks, automated systems in healthcare, science, transport, communications, energy, financial market, fuel and energy complex, nuclear energy, defense, rocket and space, mining, metallurgical and chemical industries.

A special corpus delicti called a «computer incident» is highlighted, which means the fact of violation and (or) termination of the operation of the CII facility, telecommunication network or violation of the security of the processed information, including that occurred in case of a computer attack. At the same time, in the CII telecommunication networks, the federal executive body organizes the installation of tools designed to search for signs of computer attacks.

The legal regulation of relations in the field of ensuring the security of CII in the Russian Federation is supplemented by the Federal Law of 07.07.2003 No. 126-FZ «On Communications». In addition, the Criminal Code of the Russian Federation has a specific offence for unlawful influence on the critical information infrastructure of the Russian Federation (Article 274.1) in Chapter 28 «Crimes in the field of computer information» [7]. Thus, for violation of the rules for the operation of means of storing, processing or transferring protected computer information in the field of CII, it threatens with forced labor for up to five years or imprisonment for up to six.

Currently, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation is developing a set of documents on the technological independence of the CII Russian Federation [8]. It includes a draft Decree of the President of the Russian Federation, which stipulates the approval of requirements for software and equipment at CII facilities, and the procedure for switching to the predominant use of Russian software.

In mid-2019, the Government of the Russian Federation, within the framework of the federal project «Normative Regulation of the Digital Environment», prepared a bill «On the National Data Management System and on Amendments to the Federal Law» on

Information, Information Technologies and Information Protection in the Russian Federation»» [9].

It contains new terminology and consolidates such concepts as «state data», «processing of state data», «state information resource», etc. It planned to systematize and manage the volume flow of digital content created by the state, to introduce at the federal level the «Unified Information Platform National Data Management System» and «Digital Analytical Platform for Providing Statistical Data».

In the summer of 2020, the Federal Law on the creation of a unified federal information register of the population details of the Russian Federation was passed. This register, which is supposed to be operated by the Federal Tax Service of Russia, will include all information about citizens of the Russian Federation, foreigners and stateless persons temporarily or permanently residing in the Russian Federation, recognized as refugees or received temporary asylum in Russia, as well as about foreign citizens temporarily staying for work. On the one hand, the creation of such a centralized information resource will shorten the time for the provision of public services, increase the collection of payments to budgets, a qualitatively new level of calculation and assessment of taxes, reduction of fraudulent activities when receiving social support measures and paying taxes, etc.

But on the other hand, it raises the problem of confidentiality and the proper level of protection of information that will be included in this Big Data Database, namely: personal data of individuals, including full name, date and place of birth and death, gender, citizenship and marital status ; details of the passport and documents on education and qualifications; an account on the Unified portal of public services; data on tax and military registration; and others. Indeed, according to this law, the Federal Tax Service of Russia is obliged to report information from the Register at the request of the court, prosecutor's office, investigative bodies, enforcement bodies, etc.

On June 30, 2020, the law on obtaining an enhanced unqualified electronic signature [11] came into force in Russia. It provides for the issuance of key certificates by the certification authority for verifying electronic signatures. Thus, a certificate can be issued upon application in electronic form without the personal presence of the applicant in relation to enhanced unqualified electronic signatures. But at the same time, identification of a person takes place remotely according to a simple electronic signature of a citizen, the key of which was previously obtained during his personal appearance and provided that the certification center interacts with a unified identification and authentication system.

Let us recall that «information in electronic form» signed with a simple electronic signature or an unqualified electronic signature is recognized as an «electronic document» equivalent to a paper document signed with a handwritten signature, in established cases in accordance with the agreement of the participants in electronic interaction (Article 5 and 6 of the Federal Law of 06.04.2011 No. 63-FZ «On Electronic Signatures»). For example, in the Russian Federation, complaints about decisions of registration authorities on state registration and refusal to register it can be submitted in electronic format, through Internet services called «Contact the Federal Tax Service of Russia» or «Personal account of a taxpayer» on the website of the Federal Tax Service of the Russian Federation. In this case, the electronic complaint must be signed only with the enhanced qualified electronic signature of the applicant [12].

At present, the Bank of Russia is developing an information service for assessing the risk of credit institutions' clients «Know your client» [13]. This digital platform distributes bank customers by risk zones in terms of conducting operations for financing terrorism or legalization (laundering) of proceeds from crime. Nevertheless, this also raises the question of protecting the confidentiality of data and legal responsibility for their illegal distribution. After all, such information can be used not only by banks of the Russian Federation, and besides, such data critically determines the mode of working with a client (for example,

making a decision to conduct an operation and open an account or to refuse it). At the same time, using such a digital platform, Russian banks will be able to allocate so-called dubious clients and identify minor and technical ML / TF risks.

Rospatent is introducing a digital platform for patent search through international sources, including based on AI. In 2021, testing of the software of this service will begin, which will allow an automatic search for information across the entire world patent fund. Another fact is that the Federal Antimonopoly Service of Russia has developed an antimonopoly package that takes into account the peculiarities of the influence of «price robots» (programs that can be based on AI algorithms) on competition [14].

3.4. Experimental «legal regime» of AI in Moscow and the federal subjects of the Russian Federation

Nowadays, a comprehensive regulation of such legal regimes is being actively developed. Therefore, in May 2020, the draft law of the Ministry of Economic Development of Russia No. 922869-7 «On Experimental Legal Regimes in the Field of Digital Innovations in the Russian Federation» [15] was introduced. In it, such a regime refers to the application of special regulation in the field of digital innovations to a certain circle of people for a certain period.

In turn, the special regime means the non-proliferation of certain legal acts or norms of law, although they contain mandatory requirements, for example, for licensing, certification, accreditation, obtaining accesses, permits, by means of identifying participants in the sphere of digital innovations. If the bill is passed, it is possible that experiments on the introduction of various technologies will soon be introduced in other regions.

From June 1, 2020, a one-year experiment has begun on the remote use of an enhanced unqualified electronic signature when providing services and performing other actions using the USIA (draft Decree of the Government of the Russian Federation «On conducting an experiment on the remote use of an enhanced unqualified electronic signature when providing services and performing other actions with using the federal state information system «A unified system of identification and authentication in the infrastructure providing information and technological interaction of information systems used to provide state and municipal services in electronic form»). With the help of this signature, it will be possible, among other things, to make transactions using the portal of state services, make lease agreements for federal property, sign documents for employment purposes, and provide tax reporting of citizens.

On July 1, 2020, a five-year experiment on the implementation of AI technologies began in Moscow within the framework of the National Program «Digital Economy of the Russian Federation» [16]. Law No. 123-FZ regulates the conditions for the development and implementation of AI technologies, the subsequent use of the results of its application.

5. Ethics of data circulation, digital technologies and the use of AI

In December 2019, as part of the Russian Internet Week (RIW-2019), «the Code of Ethics for the Use of Data» in the Russian Federation was adopted, with the participation of the «Big Data Association» [17]. This set of professional ethical behavior standards has consolidated the principles of interaction between citizens, business and government representatives in the collection, processing, use and storage of data. The Code aims to create a framework for regulatory initiatives in the field of data use, as well as general rules and boundaries of acceptable behavior of the professional community in connection with the circulation of private, industrial and other types of data. These include the principles of legality of data use, good faith, professional responsibility, inadmissibility of interference with privacy when processing data, etc.

In the 2019 Code, among the standards of professional ethics of data storage, the provision of an appropriate level of security for the means and methods used, an investigation of unauthorized access to data, a fair exchange of experience on ways to counter torts that violate information security are also enshrined. Also, principles were added in the processing and use of data: prevention of deliberate discrimination of citizens, prohibition of data falsification, prevention of harm or damage to users, automated processing of citizens' data only with their written or electronic consent, prohibition of misleading users that they are participate in market research.

The professional community has already assessed this code of ethics as an acceptable basis for self-regulation of data market participants that can normalize their interaction with each other and with citizens, legal entities and the state in the data industry.

4 Discussion

To begin with, the problem of the poor-quality state of information security in the country is widely discussed in the Russian Federation. There is a low level of implementation of domestic developments and insufficient professionalism in the field of information security, low awareness and inertia of Russian citizens in matters of personal information security. Measures to ensure the security of information infrastructure in the Russian Federation, including the use of Russian information technologies and software still do not have a comprehensive framework. There is no full-fledged system of administrative, legal and normative technical regulation in the field of AI. There is an incompatibility of a number of provisions of Russian data protection legislation with AI technologies.

The legal community is discussing a vague, too broadly interpreted and technically controversial definition of AI in the law No. 123-FZ. It aims to capture a broad range of possible advances in AI development. Much of this definition consists of listing the areas of potential applicability of AI technology.

Thus, the formulation «imitation of cognitive functions» of a person included in the legislative definition of AI evokes various interpretations. Further, a broad interpretation of the phrase about «the ability of a machine to learn and solve problems without algorithms» is allowed. The question arises about the controllability of the self-learning process. Therefore, the neural network is already capable of making accurate forecasts, for example, on market quotes. Does this make the market trading software artificial intelligence? On the other hand, does artificial intelligence still need properties of substantivizes and the ability to perceive? [18].

Nevertheless, there is also an opposite position. Its proponents support a broad definition of AI in Russian legislation. It notes that this legal definition reflects all the most important features of AI: 1) the complex nature of such technology; 2) the ability to self-learning and look for solutions without predetermined algorithms; 3) the comparability of the results obtained with the results of human intellectual activity, although they may be perfect.

The problem of data protection in digital technologies and strengthening of the information confidentiality regime is discussed. In the Russian Federation, any actions (operations) for research purposes with personal data should be carried out only with the condition of their obligatory depersonalization (Article 6 of the Federal Law «On Personal Data»). Another innovation in the legislation on personal data was the expansion of the conditions for processing special categories of personal data. These ones relate to race and nationality, political views, religious or philosophical beliefs, health, intimate life.

In addition, here the problem of the special legal status of such a special category of personal data arises. Indeed, if the conditions for their processing are violated, especially negative consequences for the subject may occur. For example, the processing of personal

data concerning the state of human health is allowed only if this occurs after the anonymization of personal data, and is required in order to improve the efficiency of public administration.

An «alarming» aspect of the application of AI technology in the Russian Federation remains the problem of security and compliance with strict control over its activities. Although this is contrary to the very essence of the functioning of AI. One of the aspects of this area of discussion is related to the strengthening of liability for offenses with computer information.

For example, the «Skolkovo» Foundation and the Russian Ministry of Economic Development and Trade have introduced an initiative to amend the Criminal Code in terms of liability for illegal access to protected computer information and violation of the rules for using means of storing, processing or transmitting such information (parts 2 and 3 of Art. 274.1 of the Criminal Code of the Russian Federation). The fact is that in the current version of this article, the concept of «harm» has not been disclosed. In practice, this leads to unjustified prosecution on formal grounds of specialists in the maintenance of critical infrastructure facilities. For example, today, for a short-term server failure or an unsuccessful software update, because of which the website of a government agency, bank or hospital stopped working, the site administrator and the server owner are prosecuted, even if no socially dangerous (material harm) consequences were established. Therefore, it is proposed to include in Art. 274.1 of the Criminal Code of the Russian Federation the following phrase: «causing major damage (more than 1 million rubles)».

Another aspect of this discussion is associated with the active introduction of unmanned vehicles in the Russian Federation and the legal responsibility of AI for harm to human life and health. The most typical example is the functioning of an unmanned vehicle without a test engineer, and then the question arises about the distribution of legal responsibility in an accident. Practicing lawyers believe that Articles 264 or 268 of the Criminal Code of the Russia on liability for violation of traffic rules or the operation of vehicles are not suitable for these cases of accidents involving an unmanned vehicle. The reason lies in the strictly formal nature of the provisions of the Criminal Code, which clearly defines the subjects of traffic offences. One of the ways out of such a conflict may be the qualification of harm caused by drones under Part 2 of Art. 238 of the Criminal Code of the Russian Federation, as «the provision of services that do not meet safety requirements, if they have caused, by negligence, the infliction of grievous bodily harm or death of a person».

The planned implementation of the «National Data Management System» in Russia will open access on the Internet to all processed state data, which will be open-source and free. In addition, it is warning that information related to a secret protected by law or restricted in access may also be available to an unlimited number of persons if it is transformed into impersonal information.

In recent years, LegalTech technology has been gaining popularity among Russian lawyers. Scientific-production enterprise company «Garant» is a well-known developer of the legal information system and a complex of information and legal services (GARANT, www.garant.ru) for lawyers and economists in Russia. The Company Garant was recently included in the list of backbone organizations of the Russian economy (over 600 companies) according to the criterion "provision of services for the development and operation of state information systems, socially significant services on the Internet" [19, p. 285]. It recently started developing LegalTech solutions as a cloud-based technology, even before this term became common. The services are available via the Internet even when working abroad. This ability is especially important given in line with modern trends aimed at creating a digital workplace and a new ecosystem of services in Russian companies.

One of the services of Garant's product line is the «Sutyazhnik» analytical system, which has gained popularity as a product since its launch in February 2018. This automated

service focused on the selection of Russian judicial practice, corresponding to the content and topics of the uploaded documents. Moreover, the system is able to build a list of court decisions with a reference links to their texts, as well as display the claims of the complainant, the conclusions of the court, and the subject of the legal relationship, in conjunction with key topics (Table 1).

Table 1. How does this server work?

How does this server work?			
			
Upload your document	The robot will process it	Get the finished result	To win a court case
There are drafts of claim documents, statement of defense, claims, drafts of resolutions and decisions delivered by courts	The service uses a deep linguistic analysis of the entire text and provides the result in a split second	You get an access to the list of legal practice and legal regulations that needed to be taken into account for the preparation for litigation	Analyze the result using built-in filters and win a court case

The «Sutyazhnik» system is a synthesis of modern technologies and extensive experience in working with the legal information of the «Garant» company, as well as dealing with Big Data – tens millions of court decisions.

Why was such an AI product created for finding court practice? Usually the client has in his hands a kind of statement of claim, which he himself made or which was prepared by the opposite party, and it is necessary to quickly find the relevant judicial practice, which will be as similar as possible in its plot and set of legally significant circumstances.

A very useful function of the AI service «Sutyazhnik» is the accessibility of lists of frequently mentioned material and procedural legal rule. It is important to find them, because the better the legal basis of the claim, the more chances of winning a litigation. Even if the document does not directly mention a legal act and it is unknown what regulates the sought legal relationship, the «Sutyazhnik» system will find suitable court decisions and build a list of frequently mentioned legal norms.

How exactly is the search carried out in the «Sutyazhnik» AI service? This is not a search for keywords or similar norms. The entire text and, more precisely, its meaning converted into a kind of mathematical indicator, since the model is trained on the entire multimillion array of judicial practice.

The vector space model (VSM) used as a kind of mathematical indicator. Its main idea is to represent each document of the collection as a point in a multidimensional space (a vector in a vector space). Dots that lie close to each other correspond to semantically similar documents. In search and analytical systems, the user's request is considered as a vector (as a pseudo-document), and then the documents are sorted in ascending order of distance to the pseudo-document and presented as a list to the user. The cosine of the angle between vectors can be used as a function of the nearest neighbor distance.

Since the texts of documents presented in natural language, then for their translation into an information retrieval language, it is required to carry out linguistic processing of the original text. One of the elements of this processing is the text normalization.

The indicators of accuracy and completeness measure the efficiency of the information retrieval system. Accuracy is an estimate of the conditional probability that a document issued by the system is actually relevant to the request. Completeness is an estimate of the conditional probability that a document relevant to the query will be issued by the system to the user.

Normalization increases the completeness of the search and at the same time decreases its accuracy. However, when simplified, the word can change the original meaning, which reduces the accuracy of information retrieval. In large collections, it is often more important to find documents with high accuracy, and therefore, text normalization is carried out using less «rigid» methods.

5 Conclusion

For a clearer interpretation of the term AI in Russia, one should take into account the experience and practice of IT companies and sole proprietors involved in the creation, implementation, realization and circulation of AI technologies. This will facilitate the removal of the normative and technical regulation of artificial intelligence in the Russian Federation from the «gray» zone, clarification of the definition and legal regime [20].

In the Russian Federation, there is no normative and technical regulation of the process of destruction of personal data, which creates serious problems for operators. What means by «destruction», whether in a particular case it is complete or selective, and how to interpret such actions. For this reason, it proposed to supplement Art. 21 of the Federal Law «On Personal Data» a new rule on the obligation of operators of personal data to destroy such data, taking into account the requirements of Roskomnadzor. In addition, if the operator is not able to destroy personal data in a timely manner, then it must block them and still ensure the destruction of this data within six months.

We support the implementation of an experimental legal regime in Moscow, where a huge number of IT companies are concentrated, so that legal regulation can be tested more effectively. Otherwise, the introduction of such experiments with a «digital sandbox» in several constituent entities of the Russian Federation at once could only put the formation of a uniform practice and a working legal mechanism.

Technological progress is interpreted as the development of omniscience mechanisms and all-seeing technics intended to study human life (so called biopolitics). During the pastpandemic of COVID-19 pandemic the new reality began to be called a return to the concept of a ‘walled city’, when a new reading of the classical interpretation of biopolitics is developing, namely: it is directly associated with the development of biotechnologies, digital technologies, ecosystems and “biocapital” [21].

Application of AI, which is introduced into the private life of persons and is capable of replacing workers, depriving them of jobs, etc., raises a great ethical problem. In the not too distant future, the introduction of AI will lead to a reorientation of the labor market, and one can see positive consequences in this: low-skilled workers will get their jobs.

References

1. 2019 Roadmap for the development of «end-to-end» digital technology «Neurotechnologies and Artificial Intelligence» (Moscow)
2. Artificial intelligence is a national security issue, http://www.garant.ru/news/1310389/#ixzz6UbCvtiw0
3. Anniversary UN Forum on Internet Governance will be held in Russia, https://digital.gov.ru/ru/events/39982/

4. Decree of the President of the Russian Federation of 05.12.2016 No. 646 (SPS Garant) http://base.garant.ru/71556224/
5. Federal Law of 26.07.2017 No. 187-FZ (SPS Garant) http://base.garant.ru/71730198/
6. Federal Law of 18.03.2019 No. 34-FZ (ATP Garant) http://base.garant.ru/72198096/
7. The Criminal Code of the Russian Federation dated 13/06/1996 No. 63-FZ (SPS Garant) http://base.garant.ru/10108000/
8. Draft Decree of the President of the Russian Federation «On measures to ensure information security in the economic sphere when using software and equipment at critical information infrastructure facilities» and draft resolutions of the Government of the Russian Federation on the federal portal of draft regulatory legal acts, https://regulation.gov.ru/ (ID: 01/03 / 05-20 / 00102172)
9. The text of the bill and materials thereto on the Federal portal of draft regulatory legal acts, https://regulation.gov.ru/ (ID: 04/13 / 08-19 / 00093755)
10. Federal Law of 08.06.2020 No. 168-FZ, http://base.garant.ru/74232857/
11. Federal Law of 23.06.2020 No. 183-FZ (SPS Guarantor) http://base.garant.ru/74292066/
12. Information and legal portal GARANT.RU, http://www.garant.ru/news/1380684/Text of information about the platform on the official website of the Bank of Russia, https://www.cbr.ru/press/event/?id=6837
13. Voinikanis E A, Semenova E V, Tyulyaev G S 2018 Vestnik VSU. Series: Law 4 138
14. The text of the bill No. 922869-7 (State Duma of the Russian Federation)
15. Federal Law of 24.04.2020 No. 123-FZ (SPS Garant) http://base.garant.ru/73945195/
16. http://www.garant.ru/news/1309157/#ixzz6UXNYiZHF
17. Sazonova M Artificial intelligence and law: is there contact? (SPS Garant) http://www.garant.ru/news/1401154/#ixzz6Uj2lZQ8C
18. Malinovsky A A, Osina D M, Trikoz E N 2021 Engineering Economics: Decisions and Solutions from Eurasian Perspective. Engineering Economics Week 2020. Lecture Notes in Networks and Systems Springer, Cham 139 283
19. Danelyan A A, Gulyaeva E E 2020 Moscow Journal of International Law 1 44
20. Denisenko V, Trikoz E 2020 E3S Web of Conferences 175 14013