AI AND ADMINISTRATION OF JUSTICE IN RUSSIA

Vladislav GUBKO, Margarita NOVOGONSKAYA,
Pavel STEPANOV and Maria YUNDINA[1]

I. Predictive policing

1. National practices

In Russia, the development of the use of artificial intelligence and the corresponding regulation is at an early stage. However, the Russian authorities and individual legal entities are making serious efforts to develop this industry as quickly as possible.

There is no legal definition of predictive policing in Russia. However, in legal doctrine and the media, this term is sometimes used, it refers to a preventive strategy based on computer calculations, with the help of which the police can assess the degree of risk of committing certain crimes in certain places.

Nevertheless, it is possible to note the presence of a significant amount of use of systems based on artificial intelligence in predictive policing and related fields.

The modern application of artificial intelligence in all spheres of activity is impossible without working with Big Data. To this end, the Ministry of Internal Affairs of Russia, together with leading research centers and start-ups, is holding large joint conferences on the most relevant breakthrough approaches in the use of artificial intelligence and Big data in order to combat crime. In December 2021, the second major event of this kind is being held on the basis of the Academy of Management of the Ministry of Internal Affairs of Russia.

In Russia, the greatest breakthrough has been achieved in the use of artificial intelligence algorithms for video surveillance. In Moscow, the capital of Russia, about 70% of all registered crimes are solved using this technology.

The Safe City program is a complex of software and hardware systems and organizational measures to ensure video security and technical security carried out through video surveillance. Part of this system is the FindFace Security face recognition system, created by the Russian company NtechLab in 2015. Only in Moscow more than 178,000 cameras are connected to the face recognition system. The city's video surveillance system includes cameras installed in courtyards, at the entrances of residential buildings, in parks, schools, clinics, shops and construction sites, as well as in office buildings and other public places. As noted on the NtechLab website, the main goals of their created program are advanced analytics, search for offenders, search for missing people, ensuring the safety of public events, as well as transport security. That is, as a rule, criminals are searched for using this system.

As a result of the implementation of this program, an information and analytical system for monitoring the crime situation (IASMCS) appeared in Moscow. This is an interactive map of the city, which displays the hotbeds of criminal activity. With the help of IASMCS, in-depth monitoring of the crime situation in the city districts is carried out. This approach has had a positive effect - in the

[1] Vladislav Gubko is PhD Student of the Department of Criminal Law and Criminology Lomonosov Moscow State University Law School (vladislav2012g@yandex.ru); Margarita Novogonskaya is PhD Student of the Department of Forensics Lomonosov Moscow State University Law School (ritan2297@gmail.com); Pavel Stepanov is Assistant Professor of the Department of Criminal Law and Criminology (PhD) Lomonosov Moscow State University Law School (p_stepanov@law.msu.ru); Maria Yundina is PhD Student of the Department of Criminal Law and Criminology Lomonosov Moscow State University Law School (yundina.maria@gmail.com).

surveyed areas it is possible to achieve better dynamics of reducing the number of crimes in comparison with the city-wide indicators. IASMCS analyzes records containing information about criminal and administrative offenses, road accidents, economic crimes and a number of others. With its help, the executive authorities of the city of Moscow, together with law enforcement agencies, monitor the crime situation in the city, as a result of which measures are taken to reduce the influence of negative factors on the state of crime and public safety in Moscow. According to official data, these measures have reduced the number of crimes in the city by 23% in 10 months.

However, the functionality of FindFace Security is not limited to this. During the 2018 FIFA World Cup, the system made it possible to detain more than 180 people included in the bases of offenders. The system was used both to monitor compliance with isolation measures during the Covid-19 pandemic and to search for protesters who participated in the 2021 winter rallies.

According to the developer of this program (NtechLab company), a key role in facial recognition is played by facial biometrics technologies that allow you to instantly identify offenders, locate wanted persons and accumulate massive amounts of "big data" necessary for planning public transport and utilities. FindFace video analytics is capable of processing streams of hundreds of thousands of video cameras in real time, and the face of each person that comes into the field of view of any video camera connected to the system will be automatically recorded by the system and saved for further processing. At the same time, FindFace allows you to connect and process in real time not only stationary cameras, but also cameras of mobile devices. All this makes it possible to establish his location and time of appearance in front of the camera from the photograph of the wanted person. Advanced analytics features make it possible to study habitual routes and supposed social connections, and identify possible accomplices. Biometric monitoring allows you to organize a search for a suspect in hot pursuit, issuing notifications at the moment of his appearance in the field of view of CCTV cameras, while the response speed in the "hot search" mode is only 2 seconds. In addition, the company has already created augmented reality glasses (AR), which allow increasing the efficiency of law enforcement officers during patrolling, ensuring the safety of cultural events. The video stream of the camera built into the glasses is analyzed by the system, and when the wanted person enters the field of view of the wanted person, a notification is displayed on the screen built into the lens.

The quality of the technology is confirmed by research centers from all over the world, including NIST (National Institute of Standards and Technology of the USA), IARPA (Agency for Advanced Research in Intelligence, USA).

Face identification is organized as follows. The neural network is trained to determine the unique characteristics of a face in order to then find similar faces in the database. The NtechLab algorithm works with face databases on a global scale, performing a search in a split second; declared recognition accuracy FNMR = 0.008 @FMR <10-6, that is, 1 billion images in less than 0.5 seconds. When working with features, it is impossible to restore the original face image - this allows you to follow the rules for protecting personal data. The algorithm analyzes a video frame. The video sequence consists of frames; a still image from a footage consists of an array of pixels. Each pixel has a unique color code, which is represented in the RGB palette as three numerical values. That is, the neural network receives a matrix of RGB pixel values as input. Further, the algorithm detects faces: the algorithm is able to detect an unlimited number of faces in the frame, which makes it a good solution for ensuring security in crowded places. The speed of the detector does not depend on the number of faces in the frame. So the algorithm determines where the faces are on the image and gives out the coordinates of the bibox boundaries: the upper left and lower right boundaries of the face for further work with each face. A specially created algorithm is able to determine the position of the head and correct visual distortions:

for example, "turn" the face to the frontal position, which allows it to work in difficult conditions and effectively displays faces in the image or video even with a significant lack of lighting as well as when changing the pose, turning and tilting the head. After that, the algorithm extracts the characteristics of the face: the network finds and assigns each face a feature vector or, in other words, a biometric face template[2]. Further, there is a search and comparison with the image base - a comparison of facial features with others that are in the database. At the same time, the algorithm finds faces, even if significant age-related changes have occurred, a beard or mustache appears, glasses are worn, or part of the face is covered. In addition to this, the algorithm uses several neural networks for search and identification: one of the networks detects a face in a photo or video stream, the other extracts a biometric template, others work with attributes (gender, age, glasses, beard, and others).

The Moscow Department of Information Technology (DIT)[3] reported that, in addition to NTechlab's developments, they use algorithms from VisionLabs and Tevian, claiming that "advanced face recognition systems" give no more than one error per 10 million scanned faces[4].

In the explanations dated 08/04/2020, the representative of DIT claims that the face recognition technology consists of a detection module and a face recognition module. The first one correctly identifies at least 95% of faces in the video stream, and no more than 2% of all identified faces are erroneously identified. The accuracy indicators of the second are as follows: the number of successfully formed biometric indices (biometric casts of faces) is at least 90% of uploaded photographs, the number of correctly identified face matches when searching in the database is at least 90% of all matches with the same parameters in the shooting area of the video camera[5].

Face recognition technology NtechLab received a certificate from the FSB - it allows you to implement the technology at transport infrastructure facilities. The company explained that before issuing the certificate, FSB specialists conducted tests to make sure that FindFace meets the requirements of government decree № 969 concerning the characteristics of technical means of ensuring transport security[6].

The developers of this technology managed to achieve 93% accuracy on a base of 10,000 images, but on large bases the accuracy of the system dropped, for example, on a base of 1 million images, the accuracy was only 73%.

The Findface Security User Guide specifies a default similarity threshold of 0.75[7]. So during the pandemic, Muscovites received fines based on the recording from the camera. At the same time, in the annex to the decision on the appointment of an administrative penalty, it was indicated that the degree of coincidence of the specified person with the face recorded by the camera was about 75%[8].

---

[2] Biometric template - a certain sequence of numbers formed by a neural network as a result of transforming the original image, and used for comparison with other templates.

[3] The Moscow Department of Information Technologies is an executive body of the Moscow City subordinate to the Moscow Government. The main function of the Department of Information Technologies is to carry out urban policy and carry out intersectoral coordination in the field of informatization of other executive authorities of the city of Moscow. The department also performs functions related to the implementation of management in the field of communications and the development of telecommunication technologies.

[4] 'Turn away, controllers. Public activists propose introducing video-recognition-free zones' (Kommersant) <https://www.kommersant.ru/doc/4917632> accessed 10 November 2021.

[5] Bobrinsky N.A., 'Moscow punitive innovation: intermediate results' (2021) 6 Law 54.

[6] 'NtechLab's FindFace facial recognition technology receives FSB certification' (RB) <https://rb.ru/news/findface-sertifikat-fsb/> accessed 1 November 2021.

[7] 'FindFace Security documentation' (NtechLab) <https://docs.ntechlab.com/projects/ffsecurity/en/4.4/> accessed 19 May 2023.

[8] 'Moscow's surveillance system has a margin of error of more than 20%: Penalty imposed if photo does not closely resemble the original' (Open Media) <https://openmedia.io/news/n3/u-sistemy-slezhki-za-moskvichami-pogreshnost-bolee-20-shtrafuyut-pri-nepolnom-sxodstve-foto-s-originalom/> accessed 12 November 2021.

In 2015, NtechLab took part in the University of Washington's Megaface photo face recognition competition and entered the top five for each of the four competition tasks, and won two of them, beating the Google team.

In 2017, the development of NtechLab was recognized as the best in the rating of the world benchmark Facial Recognition Vendor Test, the National Institute of Standards and Technology (NIST) of the US Department of Commerce, and also took first place in the competition of the American agency for advanced research in the field of intelligence in the categories "most accurate" and the "fastest" algorithm. In 2018, NtechLab became one of the three winners of the WIDER Pedestrian Challenge to detect pedestrians based on their silhouettes. In May 2021, NtechLab technology won the FRVT facial recognition algorithm competition, which is regularly hosted by the US Department of Commerce's National Institute of Standards and Technology (NIST).

The city's network of video surveillance cameras in Moscow was connected to the face recognition system from NTechLab, which created Findface. During two months of testing, six suspects were arrested in several districts of the city, whom they could not catch for several years[9].

Ntechlab claims on its website that more than 50% of the criminals arrested using the FindFace technology have not been found for several years. In addition, in the same place, the organization refers to a statement by the press service of the Ministry of Internal Affairs that since the beginning of 2019, 3249 crimes have been solved using a video surveillance system with facial recognition in the capital[10].

In addition, the head of the Investigative Committee's Forensic Center Zigmund Logis in an interview said that the law enforcement agencies are armed with the Crime series linkage software, developed by the Research Institute of Forensic Science on the basis of machine learning algorithms, is already registered in the register of computer programs of the Russian Federal Service for Intellectual Property. Now the program uses a model database containing information about the handwriting of persons who have committed a total of over one thousand serial crimes. The results of this work are in great demand. In addition, an algorithm has been created for constructing a portrait of a serial rapist based on a number of features that are established by the investigator at the beginning of the investigation. This system is based on artificial intelligence algorithms, namely neural networks, and allows us to accurately predict the distance from the crime scene to the place of residence of such a criminal, his age, mental illness and criminal record, family status, the fact of committing a crime using a car and without it, the presence of a connection between the offender and the victim before the act was committed. For a number of these indicators, the forecasting accuracy exceeds 90 percent and even approaches one hundred percent. Now these programs are being tested in the Investigative Committee's Forensic Center[11].

It is worth noting that in accordance with Russian legislation, only software designed to protect state secrets is subject to mandatory certification; other software, including systems based on AI, are not subject to such requirements.

---

[9] 'Moscow authorities connected a system from Findface to CCTV cameras and arrested six people' (Tjournal) <https://tjournal.ru/tech/59995-moscow-faceid> accessed 15 December 2021.

[10] 'Urban security system for a megacity in eastern Europe' (NtechLab) <https://ntechlab.com/ru/success-stories/dit/> accessed 1 December 2021.

[11] The Investigative Committee's Forensic Center is a subdivision of the Investigative Committee of Russia, which is engaged in the development, testing and implementation of new technology into investigative practice, works on methods of investigating crimes, strengthens mobile teams for operational visits to the scene of incidents, assists the investigation, and provides psychological support for the investigation of crimes.

In addition, active cooperation on the use of artificial intelligence to combat cybercrime is carried out in cooperation with large banks, their cyber defense structures and IT structures working in the prevention and investigation of cybercrimes.

So, let's give an example of an anti-fraud system, Fraud Hunting Platform is a Group-IB[12] product that is used by Sberbank[13], Post Bank[14], Raiffeisenbank[15]. This program allows detecting payment fraud, combating money laundering, identifies fraudsters[16]. According to Sberbank, in 2018, using the introduced anti-fraud system, it was possible to save more than 32 billion rubles belonging to depositors[17]. The technology quality is confirmed by the international Cybersecurity Excellence Awards.

However, it is also worth noting criticism of the use of artificial intelligence technologies in Russia.

The use of technologies based on artificial intelligence is discussed and criticized in the media. So, we can highlight the following comments on both individual technologies and, in general, the ideas of using artificial intelligence in law enforcement:

1. Articles confirming the effectiveness of systems (primarily foreign ones, such as PredPol) were carried out either by its developers or by researchers affiliated with the organization;

2. Due to corporate secrecy, predictive algorithms become opaque even for the police officers who use them. This makes independent verification of the performance of systems like PredPol nearly impossible;

3. Possible bugs in the system, such as in the case of the Horizon software created by Fujitsu;

4. Significant cash costs;

5. The possibility of hacking programs and using them for criminal purposes;

6. Increase in the number of the police force due to the creation of a new profession - Big Data analysts;

7.Difference in ethical recommendations for the use of artificial intelligence in the police and the judicial system: if the transparency of judicial databases is not in doubt, then there are serious restrictions on police officers due to their secrecy and possible negative consequences for both sources of information and victims, suspects and the accused.

Thus, Russian national practice, one can note the successful use of artificial intelligence technologies in predictive policing, despite the fact that, in general, there are some aspects that require improvement both on the part of the Russian authorities and legal entities involved in the development of artificial intelligence technologies.

[12] Group-IB is a Russian legal entity, a leading developer of solutions for detecting and preventing cyber-attacks, detecting fraud and protecting intellectual property in the network, a partner and participant in joint investigations of Interpol and Europol.
[13] Sberbank is the largest Russian bank, 50% of which is owned by the Russian government.
[14] Post Bank - Russian retail bank with state participation.
[15] Raiffeisenbank is a universal Russian bank, a subsidiary of the Austrian banking group Raiffeisen Bank International.
[16] 'Online fraud prevention' (F.A.C.C.T.) <https://www.facct.ru/products/fraud-protection/> accessed 17 May 2023.
[17] 'Overview of bank fraud prevention systems (anti-fraud)' (Anti-malware) <https://www.anti-malware.ru/analytics/Market_Analysis/anti-fraud-Bank-systems> accessed 2 November 2021.

2. Normative framework

However, the main problem of using artificial intelligence technologies in law enforcement in Russia is the minimum level of legal regulation.

Currently, there is no legislative regulation of the use of AI-based systems for predictive *policing* in the Russian Federation. There is only a limited set of general rules. Nevertheless, such algorithms are used in medical, banking, sports and other fields.

For example, special technical means of fixing administrative offenses, operating in automatic mode and having the functions of photographing and filming, video recording, or means of photographing and filming, video recording. The data received and processed by such devices is the basis for bringing the person, if necessary, to administrative responsibility. (Chapter 12 of the Administrative Offenses Code of the Russian Federation Administrative offenses in the field of road traffic). There is no requirement to inform the subject about the granting of the right to object. In this context, there are fewer guarantees of human rights than, for example, provided by European legislation (GDPR).

Russia is considering adopting legislation concerning AI-based systems for predictive policing, but currently there are some difficulties.

First of all, an approbation period for adopting legislation concerning AI-based systems for predictive policing is needed, during which the areas of regulatory regulation that require the most attention will be identified, as well as legislative gaps will be eliminated. If we talk about the areas of law that need to be paid the most attention, these are civil legislation (of course, as the basis of intellectual property), as well as administrative law, criminal law. It is regulation at the level of branches of law that will lay the foundation for the regulation of machine learning without reference to a specific area of the economy or society.

When using AI and Big Data in the fight against crime, one must proceed from the serious legal and ethical problems that arise. The Russian Ministry of Internal Affairs is attentive to the recommendations of the United Nations Office on Drugs and Crime, the United Nations International Research Institute (UNICRI), the Center for Artificial Intelligence and Robotics and the Interpol Innovation Center, Europol.

It is advisable to single out three controversial issues in this discussion:

1) Implications of the introduction of AI in conjunction with other technologies of the new industrial revolution on changes in the number of police. It is believed that this will significantly reduce the number of police, as is the case, for example, in banking structures. But, in our opinion, direct analogies cannot be made here. For example, the introduction of AI into a video surveillance system and the expansion of this system will undoubtedly increase the volume of incoming information about illegal manifestations that need to be given a criminal procedural assessment. And this will automatically require an increase in the staff of operational workers, interrogators, investigators, and experts. Already, it is required to train a large number of specialists in a new profession - Big Data analysts. Therefore, the introduction of AI will necessitate an increase in the staffing of the police.

2) Differences in ethical guidelines for the use of AI in the police and the judiciary. In all of the recently adopted documents on the use of AI in police and judicial activities, these recommendations and restrictions are the same for the police and for judges. But in reality, serious contradictions arise here. For example, in the application of the principle of database transparency for courts and police. If the transparency of judicial databases is beyond doubt, then there are serious restrictions regarding

police officers, especially those obtained in the course of intelligence (in European terminology) or operational-search activities (in the terminology of the laws of the Russian Federation), related to their secrecy and possible negative consequences as sources of information and for victims, suspects and accused.

3) Criteria for the collection of information by the police about citizens using AI tools. Consensus between police and civil society is important for the use of this data. If we are talking about the prevention and disclosure of terrorism, corruption, and other crimes, then such a consensus is achievable. And this requires the use of mechanisms for collecting information to predict criminal behavior based on the appropriate criminological and forensic criteria. But if this information is used to restrict the rights and freedoms of citizens on the basis of dubious social credit ratings (as is now observed in certain regions of China), then consensus is hardly achievable.

Decree of the President of the Russian Federation of October 10, 2019 N 490 "On the development of artificial intelligence in the Russian Federation" (hereinafter - Decree N 490), which approved the National Strategy for the Development of Artificial Intelligence for the period up to 2030, set the task of adapting the entire system to legal science legal regulation to changing conditions, in particular, with regard to human interaction with artificial intelligence. First of all, it is necessary to determine the nature of this legal act, since the strategic plan document contains the basic concepts that are not in the fourth part of the Civil Code of the Russian Federation (artificial intelligence, data set, data markup, computing system, technological solution, etc.), and also proclaims the basic principles development and use of artificial intelligence technologies, among which there are not only general legal principles (protection of human rights and freedoms), but also principles of a political (technological sovereignty) and economic nature (reasonable frugality). Decree N 490 sets the task of creating a comprehensive regulation of social relations arising in connection with the development and use of artificial intelligence technologies, including the development of appropriate ethical rules for human interaction with artificial intelligence.

By order of the Government of the Russian Federation of August 19, 2020 N 2129-r <On approval of the Concept for the development of regulation of relations in the field of artificial intelligence and robotics technologies until 2024>, the main goals of the development of artificial intelligence, including in the field of predicting policing, are defined.

The purpose of the Concept for the development of regulation of relations in the field of artificial intelligence and robotics technologies (hereinafter - the Concept) is to determine the main approaches to the transformation of the regulatory system in the Russian Federation to ensure the possibility of creating and applying such technologies in various sectors of the economy with respect for the rights of citizens and ensuring personal safety, society and state. At the same time, the goals of the Concept are to create the prerequisites for the formation of the foundations of legal regulation of new social relations that are emerging in connection with the development and application of artificial intelligence and robotics technologies and systems based on them, as well as to identify legal barriers that impede the development and application of these systems.

The priority goal of regulating relations in the field of artificial intelligence and robotics at this stage of their development is to stimulate the evolution, implementation and use of such technologies, the creation of artificial intelligence and robotics systems in a trusted and safe design, which will contribute to achieving high rates of economic growth, improving welfare and quality of life of citizens, ensuring national security and law and order, achieving sustainable competitiveness of the Russian economy, including leading positions in the world in the field of artificial intelligence.

The same main goals of the development of artificial intelligence can be found in The Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030, approved by the Decree of the President of the Russian Federation of May 9, 2017 N 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030".

Also, the use of artificial intelligence technologies, namely the previously described video surveillance system and face recognition technology, raises legal questions and, as a result, appeals to the judicial authorities.

So, in 2019, in connection with the use of this system, an administrative claim was filed against the capital's Main Directorates of the Ministry of Internal Affairs of Russia and the Department of Information Technology, which is the operator of the SIS "Unified Data Processing Center" (UDPC). The lawsuit noted that in accordance with the Law on Personal Data, the processing of biometric personal data, as a general rule, can be carried out only with the consent in writing of the subject of personal data. And since the federal laws of the Russian Federation do not establish the grounds for the use of face recognition technology (collection and processing of biometric data of citizens by the authorities, state bodies), the actions of administrative defendants on the use of face recognition technology on the territory of Moscow in the "City video surveillance system", built on the basis of the UDPC, constitute a violation of Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. However, the court indicated that there was no personal identification procedure, and therefore the video image data cannot be considered biometric personal data. Nevertheless, this case illustrates that the use of such technologies can sometimes conflict with the law, and therefore requires a change in legal regulation.

Thus, we have to admit that in Russia, the normative regulation of the use of artificial intelligence technologies in law enforcement needs significant revision and amendments to the current legislation.

3. General principles of law

In Russia, the discussion on general principles of law in the context of the application of artificial intelligence technologies occurs both at the level of individual companies that adopt codes of ethics for the development of artificial intelligence, and at the state level.

In May 2021, the Board of Sberbank approved the principles of ethics for the development and application of artificial intelligence (AI) technologies in the Sberbank Group[18]. The list of principles includes controllability and controllability of AI systems, transparency and predictability of functioning, stability and reliability, responsible use and impartiality.

Mandatory software certification is provided only for software that is used to protect information constituting state secrets. The law on state secrets provides for the mandatory certification of information security tools, including software. Including such software can be based on the use of artificial intelligence. For software, the use of which does not affect state secrets, mandatory certification is not required.

Mandatory certification of such software is organized by the FSTEC of Russia[19], the FSB of Russia and the Ministry of Defence of Russia, while these bodies themselves establish their own certification

[18] 'Sber's principles of artificial intelligence ethics' (Sberbank) <https://www.sberbank.com/ru/sustainability/principles-of-artificial-intelligence-ethics> accessed 2 May 2023.

[19] The Federal Service for Technical and Export Control (FSTEC) is the federal executive body of Russia that implements state policy, organizes interdepartmental coordination and interaction, special and control functions in the field of state security on ensuring the security (by non-cryptographic methods) of information in information and telecommunications infrastructure

system. The certification procedure involves the examination of selected samples of information security tools and documentation for it for compliance with information security requirements.

Manufacturers of means of protecting information of limited access that do not constitute a state secret are subject to compulsory licensing by the FSTEC of Russia.

The legislation does not provide for the obligation of state bodies to constantly monitor and adjust such systems. The installation and maintenance of the video surveillance system with the face recognition function is carried out by the Sitronics company, which received a contract with DIT after winning the tender.

At the moment, the Russian legislation does not regulate the issue of liability for unjustified prosecution by means of an artificial intelligence solution. There are several approaches to this issue and they are related to the legal status of artificial intelligence. In the case of recognizing AI only as an object of law, which is so far inclined in the world, responsibility should be distributed over different stages of the AI life cycle (development stage, operation stage, disposal stage). If an AI is recognized as an entity, it is possible to establish a regime of joint responsibility, when the AI creator and its owner or other subject can bear subsidiary responsibility, the study says[20]. In practice, there have already been cases when artificial intelligence mistakenly brought a person to administrative responsibility for violating the self-isolation regime (for example, paralyzed persons). It is noted that at the moment, challenging such decisions is extremely difficult, since access of third-party experts to the systems is closed[21].

It should be noted that according to the National Strategy for the Development of Artificial Intelligence for the Period up to 2030, the development of predictive police is not indicated as a priority area for the development and use of artificial intelligence technologies.

Speaking about the compliance of these systems based on AI with the principles of law, it is worth noting that Russia has adopted the National Strategy for the Development of Artificial Intelligence for the period up to 2030.

Some of the basic principles for the development and use of artificial intelligence technologies, the observance of which is mandatory in the implementation of this Strategy, are:

- transparency: explainability of the work of artificial intelligence and the process of achieving results, non-discriminatory access of users of products that are created using artificial intelligence technologies to information about the algorithms of artificial intelligence used in these products

- protection of human rights and freedoms: ensuring the protection of human rights and freedoms guaranteed by Russian and international legislation, including the right to work, and providing citizens with the opportunity to acquire knowledge and acquire skills for successful adaptation to the digital economy;

- safety: the inadmissibility of using artificial intelligence for the purpose of deliberately causing harm to citizens and legal entities, as well as preventing and minimizing the risks of negative consequences of using artificial intelligence technologies;

---

systems that have a significant impact on the security of the state in the information sphere, including in information systems and telecommunication networks functioning as part of critical facilities of the Russian Federation, destructive information impacts on which can lead to significant negative consequences.

[20] 'HSE experts break down who should be held accountable for the actions of artificial intelligence' (Higher school of economics) <https://www.hse.ru/news/480104979.html> accessed 2 May 2023.

[21] 'Artificial intelligence is being looked for a fix. It is proposed to be excluded from a number of areas of activity' (Vedomosti) <https://www.vedomosti.ru/technology/articles/2021/04/12/865680-iskusstvennii-intellekt> accessed 2 May 2023.

Also in the legislation there are such principles for systems based on AI, such as:

- non-discriminatory access to the results of using artificial intelligence
- protection of human and civil rights and freedoms, ensuring the safety of individuals, society and the state

On October 26, 2021, the largest IT companies (Sberbank, Gazprom Neft[22], Yandex[23], VK[24], MTS[25], Skolkovo[26] and others) signed the AI Code of Ethics, which is a document of voluntary self-regulation in the field of AI.

Among the principles of ethics and rules of conduct, the following are distinguished:

- non-discrimination, which means the following: in order to ensure fairness and non-discrimination, AI Actors must take measures to ensure that the algorithms and data sets they use, the processing methods used for machine learning, with the help of which grouping and / or the classification of data concerning individuals or groups of individuals does not deliberately discriminate against them. Actors are encouraged to create and apply methods and software solutions that identify and prevent discrimination based on race, nationality, gender, political views, religious beliefs, age, social and economic status, or information about private life (in this case, explicitly declared discrimination cannot be recognized as discrimination. By the AI actor, the rules for the functioning or application of the AI for different groups of users, segmented taking into account such signs).

- respect for human autonomy and free will, which is understood as the following: AI actors must take the necessary measures aimed at preserving human autonomy and free will in making decisions, the right to choose and, in general, preserve human intellectual abilities as an independent value and a system-forming factor of modern civilization. AI actors should, at the stage of AI creation, predict possible negative consequences for the development of human cognitive abilities, and prevent the development of AI that purposefully cause such consequences.

- risk and humanitarian impact assessments. AI actors are encouraged to assess the potential risks of using AI, including the social consequences for humans, society and the state, the humanitarian impact of AI on human rights and freedoms at different stages of its life cycle, including during the formation and use of data sets; carry out long-term monitoring of the manifestation of such risks; take into account the complexity of AI behaviour, including the interconnection and interdependence of processes in the AI life cycle, when assessing risks. For critical AI applications, in

[22] Gazprom Neft is a Russian vertically integrated oil company. The main activities are exploration and development of oil and gas fields, oil refining, production and sale of oil products.

[23] Yandex is a Russian multinational information technology company, whose head office is registered in the Netherlands, and owns an Internet search engine of the same name, an Internet portal and web services in several countries. It occupies the most prominent position in the markets of Russia, Belarus and Kazakhstan. Yandex is also one of the fastest growing corporations in Russia.

[24] VKontakte (international name - VK) is a Russian social network headquartered in St. Petersburg. The site is available in 85 languages; especially popular among Russian-speaking users. VKontakte allows users to send messages to each other, create their own pages and communities, exchange images, audio and video recordings, transfer money, play browser games. It also positions itself as a platform for promoting business and solving everyday problems using mini-applications.

[25] MTS (Mobile TeleSystems) is a Russian company providing telecommunications, digital and media services in Russia, Armenia and Belarus under the MTS trademark. The company provides cellular services (in the GSM, UMTS (3G), LTE and 5G standards), wired telephone services, mobile and fixed, broadband Internet access, mobile television, cable television, satellite television, digital television, media services. and entertainment content, financial services, as well as converged IT solutions in the field of the Internet of things, monitoring, process automation; data processing and cloud computing.

[26] The Skolkovo Innovation Center is a modern scientific and technological innovation complex operating in Moscow for the development and commercialization of new technologies, the first science city to be built from scratch in the Russian Federation. The complex provides special economic conditions for companies operating in Russia and engaged in research activities that meet the country's scientific and technological development strategy.

special cases, it is encouraged to conduct a risk assessment through the involvement of a neutral third party or an authorized official body, but without compromising the performance and information security of such AI, as well as protecting the intellectual property and trade secrets of the developer.

In Russian Federation, the protection of the right to privacy in relation to systems based on artificial intelligence is being discussed. So, in 2019, a resident of Moscow Alena Popova went to court, in her opinion, the processing of images of citizens' faces without their written consent violates the law on personal data and the right to privacy (Articles 23 and 24 of the Constitution of the Russian Federation[27]). In April 2018, Alena Popova held a single picket near the State Duma[28] building, for which the court brought her to administrative responsibility and fined her 20,000 rubles.

During the consideration of the case, the court examined the recordings from CCTV cameras, which showed an increase in the image (32 times) with fixation on the applicant's face - and these are signs of the use of face recognition technology. According to the law on personal data, information characterizing the physiological and biological characteristics of a person, on the basis of which it is possible to establish his identity and which is used by the operator to establish an identity, are classified as biometric personal data. They can only be processed with written consent - except as described in the defence, security and counter-terrorism laws.

Face recognition in Moscow inherently and in real time is illegal, Ms. Popova believed, and violates her constitutionally guaranteed privacy rights[29]. As a result, the Moscow court rejected the activists Alena Popova on recognizing the use of the face recognition system as illegal, since the face recognition technology is not prohibited, moreover, it is aimed at implementing public state tasks, and filming is also carried out in public places, which makes it legitimate. According to the position of the court, data from city surveillance cameras are not personal, since they are collected and stored in an anonymized form, and the linking of the image to a specific person is made by law enforcement agencies that have access to the city base.

It should be noted that despite the massive introduction of face recognition technologies and a large amount of data collected by the authorities, the use of such technologies in Russia is still not legally regulated, with the exception of the banking sector. More and more actively they begin to talk about the need to protect the right to personal freedom. Everyone even discusses the mistakes that the face recognition system makes. So, in 2020, a man was detained by mistake in the Moscow metro. The facial recognition system identified him as a wanted person, instantly alerting the police. The police later admitted the mistake[30].

Thus, when using artificial intelligence technologies in Russia, there is a tendency to develop and comply with basic legal guarantees, but this area still needs detailed regulation at the legislative level.

---

[27] 'A Moscow resident asks a court to ban facial recognition by the city's video surveillance system. The use of this technology violates the constitutional right to privacy, says the applicant' (Vedomosti) <https://www.vedomosti.ru/politics/articles/2019/10/06/812955-moskvichka-prosit-sud> accessed 14 May 2023.

[28] The State Duma of the Federal Assembly of the Russian Federation - the lower chamber of the Federal Assembly - the parliament of the Russian Federation. The highest representative and legislative body of power in Russia along with the Federation Council.

[29] 'A Moscow resident asks a court to ban facial recognition by the city's video surveillance system. The use of this technology violates the constitutional right to privacy, says the applicant' (Vedomosti) <https://www.vedomosti.ru/politics/articles/2019/10/06/812955-moskvichka-prosit-sud> accessed 14 May 2023.

[30] 'Russia: Widespread use of face recognition technology poses a threat to human rights' (Human Rights Watch) <https://www.hrw.org/ru/news/2021/09/17/379919> accessed 14 May 2023.

II. Predictive justice

There is no legal definition of predictive justice in Russia. As noted in the doctrine, predictive justice – artificial intelligence-based programs that anticipate the outcome of lawsuits, including potential compensation. These programs provide algorithms for analyzing in a short time a huge number of situations that allow you to anticipate the outcome of a dispute or at least assess the chances of success. These systems allow[31]: to choose the most correct method of protection; to choose the most appropriate arguments; to estimate the estimated amount of compensation; etc.

Currently, artificial intelligence-based systems for predictive justice are not used in Russia, but the possibility of their implementation is being actively discussed.

The use of artificial intelligence-based systems by the state is beyond the scope of the current legislation, therefore, public authorities, including the judiciary, have not yet applied systems of fully automatic decision-making. There are only general principles for the development and use of artificial intelligence (see *"I. predictive policing"*). As previously noted (see *"I. predictive policing"),* AI-based systems are not subject to mandatory certification, licensing in Russia. Also, AI-based systems for predictive justice does not require prior permission to sell.

In the scientific literature, there are judgments about the poor prospects for the use of artificial intelligence in justice, primarily due to the risks of artificial intelligence intrusion into the sphere of judicial discretion[32]. Scientists think that predictive justice can lead to a violation of the right to be heard in court, not to mention a violation of the principle of judicial independence[33]. Some researchers emphasize that regardless of the degree of automation of legal processes and the use of artificial intelligence in these processes, a person should have a direct impact on the decisions made[34] – "you cannot trust a machine to make decisions that directly concern the fate of many people. AI should only be an assistant to whom the lawyer shifts part of his routine work, which does not require a creative and reasonable start"[35].

Now there are discussions on the introduction of an electronic system for determining the optimal punishment measure – the "electronic scales of justice" - into the judicial process. This system was created to assist the court in choosing the optimal punishment for the crime committed. The measure chosen with the help of the system should be proportionate to the public danger of the crime and the identity of the perpetrator. It is reported that the test approbation of the system showed that with a probability of 96-98%, the system copes with the choice of a fair punishment. In addition, due to the "electronic scale of justice", its creators seek to weaken the influence of the human factor, ensure uniform judicial practice and strengthen the authority of the courts[36].

The "electronic scales of justice" are based on a matrix of sentencing and algorithms for its individualization. The sentencing matrix refers to the framework rules embedded in the system's software platform, fixed on two scores, in which circumstances mitigating and aggravating

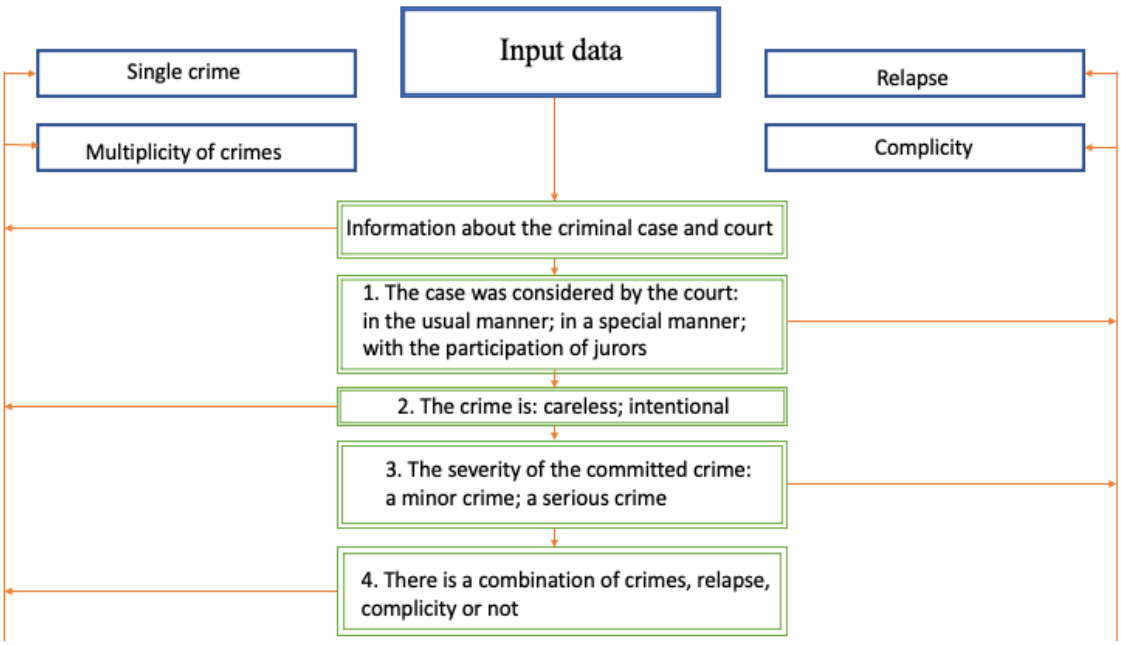
[31] Biryukov P.N., 'Artificial intelligence and "predicted justice": foreign experience' (2019) 11 Lex Russica 79-87.
[32] Kovalenko K.E., Pechatnova Yu. V., Statsenko D.A., Kovalenko N.E., 'Judge-robot as overcoming contradictions of Judicial Discretion (Legal aspects)' (2020) 4 Legal vesntik of DGU 169-173.
[33] Branovitsky K.L., V.V. Yarkov., 'Possible Ways of the Civil Process Transformation under Digitalization and Pandemic: Predictive Justice' (2021) 4 Law and Digital Economy 7-13.
[34] Nagrodskaya V.B., 'New technologies (blockchain/artificial intelligence) in the service of law. Scientific and Methodological Guide' (Prospekt 2019).
[35] Poskryakov R.S., 'The Use of Artificial Intelligence in Judicial Work' (2019) 16 Ogarev-Online.
[36] Alikperov K.D., 'The Electronic Technique of Determination of the Optimal Punishment. The Electronic Scales of Justice' (2020) 4 Russian Judge 59 - 64.

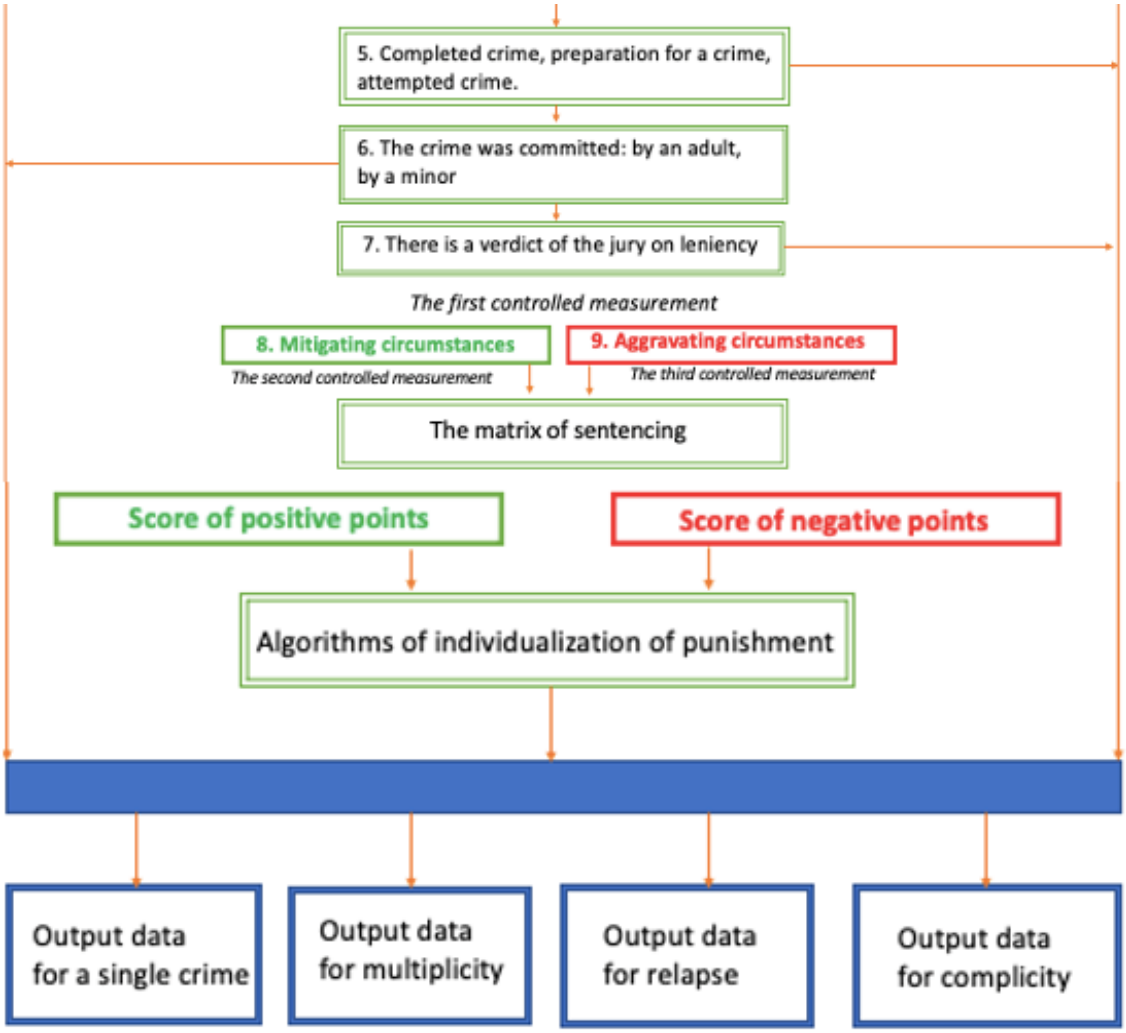
punishment (depending on their positive and negative properties) are indexed by metrically commensurate positive and negative scores. The number of these points is determined based on the principle of reasonableness, as well as on the basis of the formula of the "golden section", the sequence of Fibonacci numbers.

To index mitigating and aggravating circumstances, these circumstances are classified into 7 groups and decomposed into cells of the scores of the sentencing matrix: mitigating circumstances in one of them, aggravating circumstances in the other. After that, they are endowed with positive and negative points, respectively, in the amount depending on the socio-legal significance. Thus, 25 mitigating and 25 aggravating circumstances were identified; these circumstances correspond to a total of 208 positive and 208 negative points.

The algorithms of individualization of punishment are framework rules in which, depending on the points, the upper and lower limits of punishment are determined, within which the court, taking into account the provisions of the Criminal Code of the Russian Federation, carries out individualization. In each score, positive and negative scores were ranked according to 16 steps of the algorithm of individualization of punishment for intentional crimes and 13 steps for careless ones. A fixed distance is established between these steps along the ascending and descending lines, the value of which is determined in the proportion of 1:1.618 (the formula of the "golden section"), that is, in the ratio of 38 to 62. To determine the quantitative parameters of the points for each stage, the distance between the steps, etc., a sequence of Fibonacci numbers and the formula of the "golden section " were also used. The result is the receipt of a fractional part of the punishment (one third, etc.), so that the application of the system will not be hindered by changes in the law.

Scheme:





Thus, the algorithm is as follows:

1) the judge determines the mitigating and aggravating circumstances that are introduced into the system;

2) the program, based on two scores of the sentencing matrix, indexes them with positive and negative scores, subtracts negative points from the sum of positive points, sets the total number of dominant (positive or negative) points;

3) based on the form of intent, the characteristics of the subject, the severity of the act and other circumstances, the prevailing number of points is compared with the scale of the corresponding stage of the algorithm of individualization of punishment and determines the optimal measure of the main and additional types of punishment.

The use of artificial intelligence-based systems in law enforcement requires legislative regulation. However, not all the scientific community supports the idea of introducing "electronic scales of justice"[37]. So, in addition to technical problems that can be eliminated by improving the algorithm, it

[37] Maslov I.V., 'A review of the monograph by LL.D., Professor Alikperov Khanlar D. The Electronic Technique of Determination of a Punitive Measure. The Electronic Scales of Justice' (2020) 11 Russian Judge 55 - 60.

is noted that the consequence of using the system will be a decrease in the authority of the judge, since it will free him from mental stress and a generation of incompetent judges will appear[38].

There is also no consensus on the very idea of using predictive justice systems. It is noted that information technologies can provide tools to facilitate the decision of judges or better orient the choice of citizens and their representatives. Predictive justice programs provide analysis of cases already considered and identification of similar situations. Using algorithms, plaintiffs will be able to learn about the success of such cases and, if necessary, adjust their strategies[39].

It is a matter of concern that the introduction of predictive justice as the main tool of justice will entail the scrapping of the legal system, since this tool has the properties of another legal family - the common law system. Therefore, we can only talk about the introduction of predictive justice as an auxiliary tool, but some problems will appear in this case. For example, there is a considerable probability that judges will rely heavily on artificial intelligence, which is able to analyze a volume of information many times larger than a judge can[40]. However, the essence of judicial activity is that the decision-making process should remain with the judge. For these reasons, scientists believe that the ideal form of cooperation between a judge and artificial intelligence is as follows: instant processing of information and preparation of documentation by a robot, but making the final decision by a judge[41].

The development of a single service "Justice Online" is also underway. The main task of artificial intelligence in the “Justice Online” service will be the automated drafting of judicial acts based on the analysis of the text of the procedural appeal and the materials of the court case. It is indicated that artificial intelligence cannot become a guarantor of the protection of human rights and freedoms and ensure fair and humane justice. Therefore, its application is possible only in a limited form, with clearly defined limits and rules. However, at the moment these rules and frameworks are not fixed anywhere.

Despite the fact that predictive justice systems are not used in the Russian Federation, artificial intelligence-based systems have been introduced into the judicial system. So, since September 1, 2019, Russia has introduced an automated distribution of cases. The system operates both in commercial dispute courts and in courts of general jurisdiction and is designed to ensure a fair distribution of the burden between judges and to exclude the influence of interested parties on this process. The program contains two domains. One of them contains information about judges - specializations and pending cases. In the second domain, information is entered on each incoming case in order to assess its complexity. Thus, the complexity of a criminal case is assessed according to nine criteria, including the order of consideration of the case, the amount of material, the number of defendants etc.

However, even this AI activity can be influenced by the chairman of the court. So, if he sets out to have the machine distribute the case to a specific judge, he can temporarily exclude some judge from the system with an indication of the reason. When a particular case goes to court, before it is entered into the system, the chairman will lift the ban, and the machine will automatically entrust the case to this particular judge as having no cases in its proceedings. The AI may also incorrectly assess the

[38] Krainova N.A., ‘Electronic Scales of Justice: Digitalization of Processes or Digitalization of Tasks?’ (2019) 1 Criminoligy: yesterday, today, tomorrow 37.
[39] Biryukov P.N. (n 30).
[40] Konstantinov P.D., ‘Comparative Prospects of the Introduction of Predictive Justice in Different Law and Order Types’ (2021) 8 Arbitration and civil procedure 10 - 11.
[41] Kovalenko K.E., Pechatnova Yu. V., Statsenko D.A., Kovalenko N.E. (n 31).

complexity of the case, since it does not take into account social and political factors, the identity of the defendant, etc. [42]

Also of interest is the legal robot LegalApe, developed on the basis of neural networks. The robot answers questions of a legal nature and simplifies the work of lawyers in solving mechanical routine tasks. The pilot version of the LegalApe 2.8 robot was publicly tested for the first time on May 17, 2018 at the VIII St. Petersburg International Legal Forum as part of the "legal battle" between a person and a computer.

The questionnaire part of the robot is designed to ensure the reliability of the entire system and contains an extensive database of logical branches of legal analysis, which allows you to form reasonable legal answers with a built logic of legal statements and a broad description of the subject of a given problem. The neural part is responsible for flexibility, its task is to classify incoming information and choose the logic of the response depending on the circumstances of the case under consideration. The resulting system accepts freely formulated texts and builds the logic of the answer based on the context that is undefined in advance. Tasks such as "question - answer" and "statement - question" were solved by using an array of data, including judicial practice, business correspondence, legal positions of lawyers, scientific works.

The result was the following bot features:

1. to answer questions of a legal nature, preserving the logic of statements;
2. to form questions on the circumstances of the case in the context of previous statements;
3. to form a legal opinion (the text of the legal content), depending on the criteria laid down, questions, explanations and comments, which describes the problem, uses legal constructions and the logic of legal thought.

The neural part of the bot was created using Word2vec technology, with the use of CBOW (Continuous Bag of Words) and Skip-gram learning algorithms, as well as machine learning and Named Entity Recognition (NER) methods

When analyzing the opponent's speech, the robot selects the main entities described in natural language from the entered texts. On the basis of these entities, the texts of debates and conclusions are automatically constructed from pre-laid blocks. To recognize entities, a bidirectional LSTM network is used to obtain deep features and the method of conditional random fields for tagging words. To exclude linking to specific words in the question text and automatic accounting of synonyms, neural network search technologies were used instead of technologies based on keywords and a reverse index. For each question, a vector of dimension 300 is constructed based on the Word2Vec neural network. Then this vector is compared with similar vectors from the embedded database of questions and answers. The comparison takes place with the help of a pre-trained Siamese neural network, as a result of which the neural network, based on an in-depth analysis of the essence of the question, finds the answer most relevant to the question in the database.

The internal blocks of the bot's judgments are activated when a new incoming question is received, entities are recognized in the opponent's speech and answers to questions. Each of these blocks has its own weight and description of the judgment depending on the context. Based on these blocks, the robot formulates questions to the opponent and asks them in priority order. Then the same blocks are

[42] Kolokolov N.A., 'Artificial Intelligence in Justice – The Future is Inevitable' (2021) 3 Vestnik of Moscow University of the Ministry of Internal Affairs of Russia 201 - 212.

used at the debate stage. The bot refers to the questions previously asked to it and mentions the arguments given by the opponent.

When analyzing the opponent's speech, the robot selects the main entities described in natural language from the entered texts. On the basis of these entities, the texts of debates and conclusions are automatically constructed from pre-laid blocks. To recognize entities, a bidirectional LSTM network is used to obtain deep features and the method of conditional random fields for tagging words. To exclude linking to specific words in the question text and automatic accounting of synonyms, neural network search technologies were used instead of technologies based on keywords and a reverse index. For each question, a vector of dimension 300 is constructed based on the Word2Vec neural network. Then this vector is compared with similar vectors from the embedded database of questions and answers. The comparison takes place with the help of a pre-trained Siamese neural network, as a result of which the neural network, based on an in-depth analysis of the essence of the question, finds the answer most relevant to the question in the database.

The internal blocks of the bot's judgments are activated when a new incoming question is received, entities are recognized in the opponent's speech and answers to questions. Each of these blocks has its own weight and description of the judgment depending on the context. Based on these blocks, the robot formulates questions to the opponent and asks them in priority order. Then the same blocks are used at the debate stage. The bot refers to the questions previously asked to it and mentions the arguments given by the opponent.

On May 17, 2018, a battle between LegalApe 2.8 and private law specialist Roman Bevzenko took place within the framework of the VIII St. Petersburg International Legal Forum.

The battle was constructed according to the model of the trial: at first, the parties made justifications for their position, then answered questions, and then moved on to the debate. The subject of the dispute between LegalApe 2.8 and Bevzenko was the issue of the possibility of registering real estate on leased land. Interaction with LegalApe 2.8 was carried out using voice input and output of information and was broadcast on the screen.

The bot lost in this dispute to Roman Bevzenko with a score of 178:243 (out of 300 possible). The results of the duel were monitored, among others, by the Chairman of the Government of Russia Dmitry Medvedev and the Minister of Justice Alexander Konovalov.

The developers announced the beginning of work on the creation of the third generation of the robot. The task is to create a system with less dependence on the skeleton of rigid logical structures. Thus, on the basis of the second generation of LegalApe, adapted for working with documents, it is planned to create a flexible conversational legal robot.

In Russia, there is definitely a certain movement on the part of the state towards the further use of systems based on artificial intelligence. Speaking on February 12, 2018 at a meeting - seminar of judges of courts of general jurisdiction and arbitration courts of Russia, Dmitry Medvedev (former Chairman of the Government of the Russian Federation) stressed that work continues on digitalization of the judicial system. In addition, suggestions are made by the leadership of the Supreme Court of the Russian Federation and the Council of Judges of Russia regarding the gradual introduction of "weak artificial intelligence" in the court, capable of solving highly specialized tasks[43].

According to the decree of the Government of the Russian Federation dated 08/19/2020 No. 2129-r "On the approval of the Concept for the development of regulation of relations in the field of artificial

[43] Laptev V., 'Artificial intelligence in court: how it will work' <https://pravo.ru/opinion/232129/> accessed 17 September 2021.

intelligence technologies and robotics until 2024": "Identification and analysis of areas in which limited use of artificial intelligence systems is allowed when making legally significant decisions, drawing up a list of such areas, preparation of proposals for the adjustment of relevant regulatory legal acts are required. At the same time, at least during the time period considered in the Concept, the legislation of the Russian Federation should allow only point-by-point "delegation" of certain decisions to artificial intelligence systems, where it is objectively expedient and does not pose a threat to fundamental human rights and freedoms, national defense and state security. The instrument of experimental legal regimes ("regulatory sandboxes") can be actively used to implement individual elements of "delegation"."

At the moment, predictive justice systems are not being operated, and therefore it is difficult to draw conclusions about whether they will provide the right to protection, include the right to challenge the scientific validity of the algorithm and the decision review mechanism, however, opinions are expressed that such systems will not be able to take into account all the circumstances important for decision-making, and therefore will not be able to make the right decision. The legislative consolidation of the need to apply the system in this regard will give rise to problems of respect for the rights of the accused.

III. Evidence

In the Russian Federation, there are systems based on AI technology created for big data operations, sales forecasting, etc. AI-based systems are used in business, mainly B2B consultants, in the industries of industrial production, telecommunications, energy and finance and insurance.

At the same time, there is no regulatory framework regulating the production of evidence of AI-based systems and their use during criminal proceedings.

The International Organization on Computer Evidence (IOCE) has developed standards that must be taken into account when developing AI-based systems for working with evidence. Thus, the basic principles that must be followed when working with digital evidence are highlighted:

- all general forensic procedural principles must be observed;
- actions to investigate the seized computer evidence should not make changes to them;
- if it is necessary to provide someone with access to the original computer evidence, they must be trained and instructed accordingly;
- all activities related to the confiscation (seizure), access, storage and transfer of computer evidence must be fully documented and available for review;
- the person in possession of the computer evidence proof is fully responsible for all actions taken with respect to this proof;
- any agency that is responsible for the retrieval from memory, seizure, storage or transfer of computer evidence is responsible for agreeing to these principles.

There are systems used to assist in the investigation – the automated fingerprint information system "Papilon", which with certain conventions can be attributed to artificial intelligence systems (expert type; not based on machine learning[44]). The tasks of the system include

- identification of citizens by fingerprints and traces of fingers and palms, including by conducting operational identity checks by fingerprinting in real time;
- identification of unidentified dead bodies;
- establishing the involvement of persons in previously committed crimes;
- combining crimes committed by the same person.

These tasks are achieved by accumulating an electronic database of fingerprint cards and handprints and cross-searching between them.

The “Papilon” is an integral part of fingerprinting in Russia, which allows to solve identification tasks in the shortest possible time when searching for a person who left traces at the scene. It is noted that with the help of the available database, the facts of forgery of handprints are excluded, since with any coincidence, the program gives a large coefficient of coincidences and a recommendation list[45]. At the same time, despite the fact that the system is automated, the last and main conclusion is made by the expert operator, based on his expert experience, knowledge and inner conviction.

In case of identification, it is necessary to make a request for the fingerprint card of the individual with

[44] The two main components of an expert system are an inference engine and a knowledge base. The inference engine applies logical rules based on facts from the knowledge base. These rules are typically in the form of *if-then* statements. Expert systems require a real human “expert” to input knowledge into the knowledge base, whereas in machine learning, no such “expert” is needed. While machine learning algorithms typically work out of the box and can be improved by tuning parameters, expert systems usually don’t work until they are almost done being developed. This is part of the reason why they have gradually declined in use since their inception in 1965.

[45] Voronkov L.Yu., ‘The Possibilities of Using ADIS “PAPILON” in The Expert Study of Fingerprint Traces containing a Gap Zone’ (2021) 5 Vestnik of Saratov State Law Academy 194.

whom the match was found and compare the physical objects again. These actions are necessary in order for the conclusion to become evidence in the case.

On the basis of various research centers and universities in Russia, work is underway to create technological solutions of a forensic orientation, which in the future can be used in the activities of subjects of investigation. Projects designed to computerize solutions to various tasks that an investigator faces in the course of an investigation are being actively developed.

For example, the project of scientists of the Nizhny Novgorod University named after N.I. Lobachevsky "FORVER", which allows forming the most promising versions about the identity of the criminal, the relational database of K.A. Nelyubin, containing in a systematic form the main elements of the criminalistic characteristics of murders, ensuring the effectiveness of the investigation of murders in the Sverdlovsk region.

After processing a certain amount of initial information, "FORVER" provides the investigator with a system of versions ranked by probability. Based on the data obtained, the investigator instructs the operational staff to search for persons endowed with specific characteristics defined by the program: gender, age, occupation, remoteness of the criminal's place of residence from the crime scene, the nature of the relationship with the victim. Thus, the program allows to use standard versions, to form a probable portrait of the criminal, to revise the plausibility of versions when receiving additional information. As a result, the circle of potential suspects is specified, reduces the time spent on working out versions. Assessing the effectiveness of the program, the researchers note that it allows for "a high degree of probability to identify the accused by general and particular features, in a wide range of suspects, which is unsurpassed and high-precision quality assistance in the investigation of criminal cases."[46]

On the basis of the Department of Criminalistics of the Ural State Law University, an artificial neural network is being developed, focused on identifying signs of forgery of signatures made without the use of mechanical and computer devices.

In addition, the following AI-based systems are used in practice[47]:

- The "Block" system, which provides information forensic support for the investigation of economic crimes;
- The "Maniac" system, which provides information in the investigation of serial murders on sexual grounds;
- The "Octopus" system, which helps to establish contact contacts of criminals;
- The "Safe" system, which systematizes information about the theft of funds from the vaults.

The Ministry of Internal Affairs of the Russian Federation has signed a contract according to which by the end of 2022 the agency will receive the Mirror program, which allows identifying signs of intra-frame video editing, which is performed using artificial neural networks that allow synthesizing video images of people (deepfake)[48].

Another area of artificial intelligence development used in criminology is computational linguistics. Currently, text recognition systems are actively used, as well as the analysis of Internet content in order to isolate information of certain content (most often extremist and terrorist).

---

[46] Kovalenko S.I. Tolstolutskiy V.Yu., 'The Program "FORVER" in Atypical Investigative Situations' (2014) 5 Vestnik RZI 56.

[47] Bahteev D.V., 'Artificial Intelligence in Forensic Science: Current State and Application Potential' (2018) 2 Russian law: education, practice, science 44.

[48] Sretentsev D.N., Volkova V.R., 'Prospects for the Introduction of Artificial Intelligence Systems in Crime Investigation' (2021) 11 Russian investigator 38 – 42.

Basically, these databases and software complexes are focused on solving either one specific task or a group of homogeneous tasks. For example, programs for the nomination of investigative versions can quite cope with typical versions, but if it is necessary to nominate atypical versions, their potential is significantly reduced. Therefore, at the moment, the issue of creating software complexes is very relevant, whose capabilities of complex heuristic information processing are as close as possible to the capabilities of the forensic thinking of the investigator.

It is worth noting that the evidence itself is collected using AI-based systems, but is not obtained by AI-based systems directly (evidence collected by AI-based systems can be attributed with a certain degree of conditionality to evidence collected by cameras using facial recognition technologies – this technology and its application issues were described earlier in the section "predictive policing"). In this regard, new types of evidence for the purposes of criminal justice are not created, and related issues such as their reliability, neutrality, standards of methods of contesting are not raised.

Also, AI-based systems are not used in Russia to assist judges (or courts or regulators) in evaluating evidence in criminal cases. Consequently, it is not possible to answer questions about how the system evaluates the credibility of evidence, assesses the guilt of a person etc.

References:

1. Alikperov K.D., 'The Electronic Technique of Determination of the Optimal Punishment. The Electronic Scales of Justice' (2020) 4 Russian Judge.
2. Bahteev D.V., 'Artificial Intelligence in Forensic Science: Current State and Application Potential' (2018) 2 Russian law: education, practice, science.
3. Biryukov P.N., 'Artificial intelligence and "predicted justice": foreign experience' (2019) 11 Lex Russica.
4. Bobrinsky N.A., 'Moscow punitive innovation: intermediate results' (2021) 6 Law.
5. Branovitsky K.L., V.V. Yarkov., 'Possible Ways of the Civil Process Transformation under Digitalization and Pandemic: Predictive Justice' (2021) 4 Law and Digital Economy.
6. Kolokolov N.A., 'Artificial Intelligence in Justice – The Future is Inevitable' (2021) 3 Vestnik of Moscow University of the Ministry of Internal Affairs of Russia.
7. Konstantinov P.D., 'Comparative Prospects of the Introduction of Predictive Justice in Different Law and Order Types' (2021) 8 Arbitration and civil procedure.
8. Kovalenko K.E., Pechatnova Yu. V., Statsenko D.A., Kovalenko N.E., 'Judge-robot as overcoming contradictions of Judicial Discretion (Legal aspects)' (2020) 4 Legal vesntik of DGU.
9. Kovalenko S.I. Tolstolutskiy V.Yu., 'The Program "FORVER" in Atypical Investigative Situations' (2014) 5 Vestnik RZI.
10. Krainova N.A., 'Electronic Scales of Justice: Digitalization of Processes or Digitalization of Tasks?' (2019) 1 Criminoligy: yesterday, today, tomorrow.
11. Laptev V., 'Artificial intelligence in court: how it will work' <https://pravo.ru/opinion/232129/> accessed 17 September 2021.
12. Maslov I.V., 'A review of the monograph by LL.D., Professor Alikperov Khanlar D. The Electronic Technique of Determination of a Punitive Measure. The Electronic Scales of Justice' (2020) 11 Russian Judge.
13. Nagrodskaya V.B., 'New technologies (blockchain/artificial intelligence) in the service of law. Scientific and Methodological Guide' (Prospekt 2019).

14. Poskryakov R.S., 'The Use of Artificial Intelligence in Judicial Work' (2019) 16 Ogarev-Online.

15. Sretentsev D.N., Volkova V.R., 'Prospects for the Introduction of Artificial Intelligence Systems in Crime Investigation' (2021) 11 Russian investigator.

16. Voronkov L.Yu., 'The Possibilities of Using ADIS "PAPILON" in The Expert Study of Fingerprint Traces containing a Gap Zone' (2021) 5 Vestnik of Saratov State Law Academy.

17. 'A Moscow resident asks a court to ban facial recognition by the city's video surveillance system. The use of this technology violates the constitutional right to privacy, says the applicant' (Vedomosti) <https://www.vedomosti.ru/politics/articles/2019/10/06/812955-moskvichka-prosit-sud> accessed 14 May 2023.

18. 'A Moscow resident asks a court to ban facial recognition by the city's video surveillance system. The use of this technology violates the constitutional right to privacy, says the applicant' (Vedomosti) <https://www.vedomosti.ru/politics/articles/2019/10/06/812955-moskvichka-prosit-sud> accessed 14 May 2023.

19. 'Artificial intelligence is being looked for a fix. It is proposed to be excluded from a number of areas of activity' (Vedomosti) <https://www.vedomosti.ru/technology/articles/2021/04/12/865680-iskusstvennii-intellekt> accessed 2 May 2023.

20. 'FindFace Security documentation' (NtechLab) <https://docs.ntechlab.com/projects/ffsecurity/en/4.4/> accessed 19 May 2023.

21. 'HSE experts break down who should be held accountable for the actions of artificial intelligence' (Higher school of economics) <https://www.hse.ru/news/480104979.html> accessed 2 May 2023.

22. 'Moscow authorities connected a system from Findface to CCTV cameras and arrested six people' (Tjournal) <https://tjournal.ru/tech/59995-moscow-faceid> accessed 15 December 2021.

23. 'Moscow's surveillance system has a margin of error of more than 20%: Penalty imposed if photo does not closely resemble the original' (Open Media) <https://openmedia.io/news/n3/u-sistemy-slezhki-za-moskvichami-pogreshnost-bolee-20-shtrafuyut-pri-nepolnom-sxodstve-foto-s-originalom/> accessed 12 November 2021.

24. 'NtechLab's FindFace facial recognition technology receives FSB certification' (RB) <https://rb.ru/news/findface-sertifikat-fsb/> accessed 1 November 2021.

25. 'Online fraud prevention' (F.A.C.C.T.) <https://www.facct.ru/products/fraud-protection/> accessed 17 May 2023. 'Overview of bank fraud prevention systems (anti-fraud)' (Anti-malware) <https://www.anti-malware.ru/analytics/Market_Analysis/anti-fraud-Bank-systems> accessed 2 November 2021.

26. 'Russia: Widespread use of face recognition technology poses a threat to human rights' (Human Rights Watch) <https://www.hrw.org/ru/news/2021/09/17/379919> accessed 14 May 2023.

27. Sber's principles of artificial intelligence ethics' (Sberbank) <https://www.sberbank.com/ru/sustainability/principles-of-artificial-intelligence-ethics> accessed 2 May 2023.

28. 'Turn away, controllers. Public activists propose introducing video-recognition-free zones' (Kommersant) <https://www.kommersant.ru/doc/4917632> accessed 10 November 2021.

29. 'Urban security system for a megacity in eastern Europe' (NtechLab) <https://ntechlab.com/ru/success-stories/dit/> accessed 1 December 2021.