DOI 10.52468/2542-1514.2025.9(4).15-25

APPROACHES TO THE LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE APPLICATION IN LAW ENFORCEMENT

Oleg A. Stepanov, Mikhail M. Stepanov
Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, Russia

Article info
Received –
2024 December 11
Accepted –
2025 September 20
Available online –
2025 December 20

Keywords
Artificial intelligence, law enforcement, Russian Federation, legal regulation, Eastern approach, Western approach, protection of citizens' rights, legal mechanism of appealing decisions

The article considers the Eastern (People's Republic of China) and Western (USA, European countries) approaches to the legal regulation of relations related to the use of artificial intelligence in law enforcement.

The subject of the study is the relations arising in the process of such regulation.

The purpose of the study is to analyze the legal regulation of the use of artificial intelligence in the process of collecting information about citizens, its processing and taking into account the decisions prepared by AI for law enforcement officials.

The methodological basis of the study is logical and systematic methods of scientific cognition, as well as methods of analysis and synthesis of legal phenomena.

Foreign and domestic experience of legal regulation is studied. Special attention is paid to the need to ensure the protection of citizens' rights in the process of collecting information about them, its processing and taking into account the decisions prepared by artificial intelligence for law enforcement officials. It is pointed out that the peculiarities of legal regulation in this sphere of life activity of society are conditioned by the correctness of conclusions formulated by artificial intelligence, as well as the competence of algorithm developers and persons carrying out its training. Legal regulation of the relevant relations is considered through the prism of the results of law enforcement. The Eastern approach assumes the assessment of the actions of individuals by a number of parameters, taking into account which their trustworthiness index is determined, implying the assignment of a personal id to them personal identification code (social rating). The Western approach is that the United States and Western states actively using digital control tools based on AI technologies in the field of law enforcement do not inform the population about the total surveillance of people. It is noted that at present the regulation of this sphere in the Russian Federation is more oriented to the Western approach. At the same time, at the national level there is no mechanism of legal regulation on the consequences of actions of a person in the field of law enforcement. Attention is drawn to the fact that while in China for “unreliable” persons only a number of restrictions are imposed on their movement (use of airplanes and trains), occupation (prohibition to hold managerial positions in certain areas), obtaining financial services (refusal to issue loans), in the United States such persons are placed without trial in secret prisons, where they are tortured.

It is concluded that taking into account this circumstance requires the creation in the Russian Federation of a legal mechanism for appealing decisions taken by law enforcement officials on the basis of recommendations developed by artificial intelligence, by developing and adopting norms of law to prevent the use of its potential for purposes incompatible with the goals of law enforcement. This implies the need to develop a system of theoretical ideas about the most rational forms and methods of legal regulation in considering.

ISSN 2542-1514 (Print)

1.Introduction

The development of big data and algorithmic technologies entails the development of new ways of controlling the population (political, economic, social) [1, p. 420] related to the analysis of heterogeneous and unstructured data about citizens based on Big Data technology [2; 3; 4; 5]. The most important characteristic of this technology is the use of artificial intelligence (AI).

Since Big Data and AI are widely used in law enforcement activities, in modern conditions, both the possibility of using innovative products in law enforcement activities and the relevant legal regulations are becoming relevant.

Currently, there are two main approaches to the legal regulation of relations related to the use of AI in the field of law enforcement. Conventionally, they can be designated as eastern (People's Republic of China) and western (USA, European countries).

2. The experience of the People's Republic of China

In China, the interests of society based on traditional values are prioritized over the interests of the individual, his individual rights and freedoms. This trend can also be traced in the legal regulation of relations related to the use of AI in the field of law enforcement.

At the same time, it should be noted that increased attention is being paid to the development of AI in China. Back in 2017, the State Council of the People's Republic of China adopted a Plan for the development of a new generation of artificial intelligence, which stated that by 2030 China should reach a world-leading level in the general theory, technology and application of artificial intelligence, become the world's largest innovation center for artificial intelligence, as well as achieve significant results in the "smart" economy and "a smart society"[1].

The use of AI in public and public administration, as well as for law enforcement purposes in China, is carried out within the framework of the development of the social credit system (social rating system, social trust system), which is currently being implemented at the regional level with varying degrees of readiness. At the moment, it is considered the largest and most complex structure in the world for monitoring and subsequent influence on the behavior of both individuals and society as a whole. Its creation began on June 14, 2014, when the State Council of the People's Republic of China adopted the "Plan for the construction of the Social Credit System (2014-2020)"[2]. In the development of the Plan, local regulatory legal acts are adopted at the local level [6].

The Russian literature notes that one of the goals of the development and implementation of the social credit system was to change the social situation in the country and the need to stabilize it. Since the traditional practices of protective response to the protest movement in China, which had developed earlier, had exhausted themselves, the introduction of a social credit system began to be considered as a tool for controlling people's behavior, combating crime, investigating crimes and offenses [7, p. 82], influencing the law-abiding citizens [8, p. 105].

This system is associated with evaluating the actions of individuals according to a number of parameters, on the basis of which their trustworthiness index (social rating) is determined. Therefore, its basis is the collection and processing of information about the subject. This activity is carried out both at the level of the Government of the People's Republic of China and at the level of individual regions. For the convenience of data processing, each individual was assigned a personal identification code (ID number) in accordance with the Law on the Identification of a Citizen of the People's Republic of China, adopted back in 2003[3].

Today, an 18-digit identification code is

[1] URL: https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (date of request: 11.12.2024).

[2] URL: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm (date of request: 11.12.2024).

[3] https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%B1%85%E6%B0%91%E8%BA%AB%E4%BB%BD%E8%AF%81%E6%B3%95/182464?fromModule=lemma_inlink#3 (date of request: 11.12.2024).

required to receive government services, use electronic payment systems, make purchases in online stores, issue travel documents, purchase SIM cards, register as Internet users, etc. [9; 10]. Information about its use is collected, processed and stored. On its basis, dossiers of individuals are formed, which are stored in the corresponding credit platform [11, p. 151].

Along with this, data on Chinese citizens is obtained using SMART gadgets [12]. For example, when selling smartphones, mandatory applications are installed that track a person's movement, purchases, orders, payments, health status, contacts, activity on social networks and the Internet, and much more. It should be borne in mind that in China, every phone, like a SIM card, is linked to its owner, whose identity has been identified [13].

Surveillance cameras are a significant source of information about the behavior of Chinese residents in public space. In order to identify any Chinese citizen by his photo on an identity card, a video surveillance project "Sharp Eyes" was implemented in China. As part of this project, by 2020, 626 million video surveillance cameras were supposed to be installed in China[4], information from which was processed by artificial intelligence. Currently, the video surveillance system in China continues to develop [14, p. 40], including in the direction of camera recognition of persons hidden by protective medical masks, the wearing of which significantly reduced its effectiveness [15, p. 133].

Not only law enforcement and other government agencies have access to street cameras in China, but also ordinary citizens who can connect to them in real time using special set-top boxes and smartphones, and if any offense is detected, report it to the police.

CCTV cameras are used in China in conjunction with facial recognition technology, which allows for automatic search for wanted offenders. In addition, law enforcement and intelligence officers use glasses equipped with this technology in places where there are no cameras or their activities are difficult. The use of these technological solutions significantly increases the effectiveness of the detection of wanted persons[5].

It is interesting to note that as a result of the operation of video surveillance cameras equipped with AI technology, in the period from 2012 to 2016, crime in eight types of serious crimes, including drug trafficking, theft and intentional infliction of bodily harm in China decreased by 42.7%[6].

Among the regional social credit systems, the system implemented in the Xinjiang Uygur Autonomous Region (hereinafter – XUAR) stands out. Its main features are enhanced control over the behavior of citizens and a focus on performing a law enforcement function. In this regard, DNA and voice samples were obtained from the residents of XUAR, as well as the iris of the eyes was scanned. All video cameras in the SWAR are integrated into a single system. In addition, information is captured from GPS trackers in cars, facial recognition scanners at checkpoints and large public facilities. Special applications on smartphones record suspicious messages and recordings. As a result of the introduction of the system in the XUAR, there was a certain decrease in the level of extremism [16].

It should be noted that the idea of a social rating could not be fully implemented in China – this was done taking into account the economic opportunities only in the territories of individual provinces. Therefore, the social credit system in China is currently fragmented from a territorial and law enforcement point of view [17, p. 18]. It consists of dozens of pilot projects implemented locally by authorities at various levels and commercial organizations [18, p. 68-69], differing from each other in terms of content, legal regulation and the degree of control over the behavior of the population based on the collection of information about citizens and the formation of their digital personalities [19; 20; 21].

[4] Hersey F. China to have 626 million surveillance cameras within 3 years. TechNode. Nov. 22, 2017. URL: https:// technode.com/2017/11/22/china-to-have-626-million-surveillance-cameras-within-3-years/.

[5] Mozur P. Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras./ The New York Times. July 8, 2018. URL: https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[6] Facial recognition, AI and big data poised to boost chinese public safety. Global times. Oct. 17, 2017. URL: http://en.people.cn/n3/2017/1017/c90000-9280772.html.

ISSN 2542-1514 (Print)

3. The experience of the USA and European countries

The Western approach to regulating the use of AI in law enforcement is characterized by the fact that in the United States and European countries, digital control tools based on AI technologies are also actively used in the field of law enforcement, but the population is not informed about total surveillance.

The existence of the relevant programs became widely known in June 2013 after the publication of classified information leaked to the press by Edward Snowden, an analyst at the US National Security Agency (NSA).

As part of the PRISM, XKeyscore, Tempora, and other projects, the special services of the United States and its allies monitor information transmitted through various means of communication, both by American citizens and citizens of other countries, in order to identify unreliable individuals, potential terrorists, and individuals who have already committed crimes.

The surveillance of the world's population by Western countries has acquired such proportions that it has become the subject of proceedings in the structures of the United Nations. UN General Assembly Resolution A/RES/68/167 of December 18, 2013 [7] and UN General Assembly Resolution A/RES/69/166 of December 18, 2014[8] were issued on this issue. They called on States to put an end to human rights violations, review national legislation, including those governing communications surveillance, interception, and collection of personal data, and bring it into line with international human rights law.

In the reports of the Office of the United Nations High Commissioner for Human Rights dated June 30, 2014, A/HRC/27/37 and December 19, 2014, A/HRC/28/39, on the problems of human rights violations during surveillance using digital communication technologies (Internet, mobile smartphones, WiFi-enabled devices), interception The issues of protecting the right to privacy in the context of national and extraterritorial surveillance, as well as the interception and collection of personal data, including on a massive scale, were considered[9].

It should be noted that the USA and Great Britain are pioneers in the use of video surveillance systems in order to ensure public order [22, p. 136]. Currently, the number of video cameras in Western countries is increasing, and their software is being improved, including towards the introduction of AI-based products. The development of intelligent video surveillance systems has even made it possible to talk about the emergence of a "surveillance state" ("surveillance state") in the West[10].

The data collected on citizens is analyzed by various programs based on AI technologies. The leader in this field is Palantir (Palantir Technologies, Inc.). Initially, the CIA became its main customer and investor. Subsequently, Palantir software products began to be used by various military structures, law enforcement and special services, including the CIA, the FBI, and the police. For example, Palantir software is currently widely used in the work of the Los Angeles Police Department[11].

Thus, in the USA and other European countries, personal data about the population is also collected and processed for law enforcement purposes. At the same time, the capabilities of AI are widely used. However, unlike in China, this

[7] Resolution of the UN General Assembly dated December 18, 2013 A/RES/68/167 "The right to privacy in the digital age". URL: https://undocs.org/ru/A / RES/68/167 (date of request: 11.12.2024).

[8] Resolution of the UN General Assembly dated December 18, 2014 A/RES/69/166 "The right to privacy in the digital age". URL: https://undocs.org/ru/A/RES/69/166 (date of request: 11.12.2024).

[9] Report of the Office of the United Nations High Commissioner for Human Rights dated June 30, 2014 A/HRC/27/37 "The right to privacy in the digital age". URL: https://undocs.org/ru/A/HRC/27/37 (date of request: 12/11/2024); Report of the Office of the United Nations High Commissioner for Human Rights dated December 19, 2014. A/HRC/28/39 "Summary of the panel discussion on the right to privacy in the digital age". URL: https://www.undocs.org/ru/A/HRC/28/39 (date of request: 11.12.2024).

[10] Devlin H. «We are Hurtling Towards a Surveillance State»: The Rise of Facial Recognition Technology. The Guardian. Oct. 5, 2019. URL: https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state

[11] Matt Burns. Leaked Palantir Doc Reveals Uses, Specific Functions And Key Clients // Techcrunch. Jan. 11, 2015. URL: https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/

information is hidden from citizens who are practically unaware of this aspect of the state's activities. There are no officially published regulatory legal acts regulating it, as well as a mechanism for protecting citizens' rights in the process of its implementation.

As a result, for example, on May 25, 2021, the European Court of Human Rights issued a ruling in the case of Big Brother Watch and Others v. the United Kingdom. The court concluded that the UK had violated the European Convention for the Protection of Human Rights and Fundamental Freedoms, as it was actively engaged in intercepting the communication data of its citizens (calls, SMS messages, electronic correspondence, etc.) and illegally obtaining information about users from communication service providers[12]. However, this situation has not received any further development, except for the statement of these facts.

4. The experience of the Russian Federation

The realities of using AI in the domestic sphere of law enforcement allow us to conclude that currently legal regulation is more focused on the Western approach to these relations.

Data on the country's population is constantly being collected. The legal basis for this activity, first of all, is Federal Law No. 374-FZ of July 6, 2016 "On Amendments to the Federal Law on Countering Terrorism and Certain Legislative Acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety".[13]

Article 13 of the Federal Law amended Federal Law No. 126-FZ of July 7, 2003 "On Communications"[14], imposing on telecom operators the obligation to store information on the facts of receiving, transmitting, delivering and (or) processing voice information, text messages, images, sounds, video or other communications from users of communication services – for three years; and text messages, voice information, images, sounds, videos, and other communications from users of communication services - for up to six months. According to article 15 of the said Federal Law, amendments were made to Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection"[15], obliging organizers of information dissemination on the Internet to store information on the facts of reception, transmission, delivery and (or) processing on the territory of the Russian Federation. voice information, written text, images, sounds, video or other electronic messages of netizens and information about these users – for one year; text messages from netizens, voice information, images, sounds, videos, and other electronic messages – up to six months.

In addition, various types of SORM programs (a system of technical means to ensure the functions of operational search activities)[16], the Tuning Fork program, etc. are used to collect information. It is interesting to note that back in 2015, upon the application of SORM, the European Court of Human Rights decided that the operation of this system (according to Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms)[17] violates the right to respect for private and family life.

Another source of information about the Russian population used in law enforcement activities is data obtained as a result of the operation of video surveillance cameras and their processing by AI. The legal regulation of this activity is carried out by the

[12] Judgment of the European Court of Human Rights dated May 25, 2021 in the case "Big Brother Watch and Others v. the United Kingdom" (Complaint No. 58170/13 and two other complaints) // Bulletin of the European Court of Human Rights: Russian Edition. Moscow, 2022. No. 1 (235).

[13] Collection of legislation of the Russian Federation. 2016. No. 28. Art. 4558.

[14] Collection of legislation of the Russian Federation. 2003. No. 28. Art. 2895.

[15] Collection of legislation of the Russian Federation. 2006. No. 31 (ch. I). St. 3448.

[16] See: Order No. 70 of the State Committee of the Russian Federation for Communications and Informatization dated April 20, 1999 "On Technical Requirements for a system of technical means to ensure the functions of operational search measures on telecommunication networks of the Russian Federation". SvyazInform. 1999. № 6.

[17] Judgment of the European Court of Human Rights of December 4, 2015 in the case of Roman Zakharov v. the Russian Federation (complaint No. 47143/06) // Bulletin of the European Court of Human Rights: Russian edition. Moscow, 2016. No. 6 (168).

subjects of the Russian Federation independently. For example, February 7, 2012 The Moscow Government adopted Resolution No. 24-PP "On Approval of the Regulations on the State Information System "Unified Data Storage and Processing Center"[18]. Cameras of this information system are currently installed in courtyards, entrances, crowded places and other places. In 2021, Moscow entered the top 30 megacities in the world in terms of the number of surveillance cameras per square kilometer. Currently, there are more than 227200 installed. Information from them was used in the investigation of 70% of crimes[19].

It should be noted that Russian companies working in the field of video analytics are among the leading in the world. The software products they create are often superior to their foreign counterparts. Thus, the use of an anti-terror system based on FindFace facial biometrics technologies, which is part of the Safe City system, allows you to instantly identify offenders in Moscow, identify weapons and other objects, and locate wanted persons. The program has a mobile application that allows police officers to use the full range of its functions from anywhere in the city. For patrolling streets or mass events, it is possible to connect mobile phone cameras and augmented reality glasses. Based on photos or videos seized from the crime scene (for example, from an ATM camera or from a video surveillance system), the FindFace program allows you to establish the place of residence of the wanted person, his movement routes, identify his social connections, including potential accomplices, and obtain other valuable operational information.

During the 2018 FIFA World Cup matches in Russia, the use of the FindFace Multi system made it possible to successfully identify and take timely measures to detain about 100 people out of 50,000 wanted offenders, including those on the federal wanted list, extremists and football fans (including foreign ones) with a ban on attending matches, as well as pocket money thieves and supervised persons[20].

The number of video surveillance cameras, including those equipped with AI technologies, is growing rapidly in Russia. Thus, in 2023, the number of video surveillance systems increased by 12%. By the end of 2024, it is projected to grow by another 11%. In terms of the number of surveillance cameras, the Russian Federation ranks third after China and the United States. Most of the cameras with AI technology are used to record traffic violations. Their number by the end of 2023 amounted to 22183, in 2024 it is planned to install another 909 cameras[21]. In 2023 220.9 million rulings worth about 140.9 billion rubles were issued with the help of video cameras for traffic violations[22].

5. Conclusion

To summarize, AI technologies are currently widely used to control the behavior of the population in all countries of the world where appropriate technologies are available. Among other things, this activity is carried out in order to protect public order and combat crime.

An analysis of Eastern and Western approaches to the legal regulation of relations related to the use of AI in law enforcement leads to the conclusion that the problem of ensuring and protecting citizens' rights in the process of collecting information about them, processing it and making decisions on this basis by competent authorities and officials is increasing, since these decisions may cause restrictions. the rights and freedoms of citizens, including in connection with bringing them to legal responsibility.

Thus, in China, a number of restrictions have

[18] Bulletin of the Mayor and Government of Moscow. 2012. № 8.

[19] City video surveillance system // The portal of the Moscow government. URL: https://video.dit.mos.ru / (date of request: 11.12.2024).

[20] NTECHLAB company website. URL: https://ntechlab.ru/solution/public-safety / (date of request: 11.12.2024).

[21] Kodachigov V. Not at first glance: the number of "penalty" cells in the Russian Federation will increase dramatically // Izvestia. May 7, 2024. URL: https://iz.ru/1692531/valerii-kodachigov/ne-pervyi-vzgliad-v-rf-rezko-vyrastet-kolichestvo-shtrafnykh-kamer.

[22] In the Russian Federation in 2023, fines on cameras for traffic violations amounted to a record amount in five years // TASS. February 23, 2024. URL: https://tass.ru/obschestvo/20064853 .

been introduced for "unreliable" individuals, related, for example, to their movement (using airplanes and trains), occupation (prohibition to hold senior positions in certain areas), obtaining financial services (refusal to issue loans), etc. [23, pp. 23-24; 24, p. 748]. And in the United States, such persons can be placed in secret prisons without trial, where they are tortured [25; 26].

Given that the correctness of the conclusions formulated by AI is determined by the competence of algorithm developers and those who train it, expanding the scope of AI and giving it additional powers, including making legally significant decisions, requires the creation of additional guarantees for the protection of citizens' rights in cases of error by these specialists. Taking this circumstance into account presupposes the creation in the Russian Federation of a mechanism for appealing decisions based on AI data (or AI directly) by developing legal norms that consolidate it, and aims to develop theoretical ideas about the most rational forms and methods of legal regulation in the field of public practice under consideration.

REFERENCES

1. Naumenko T., Sekretareva K. China's Social Credit System: Dystopia or Public Welfare Factor?. *Zhurnal issledovanii sotsial'noi politiki = The Journal of Social Policy Studies*, 2022, vol. 20, no. 3, pp. 419–432. DOI: 10.17323/727-0634-2022-20-3-419-432. (In Russ.).

2. Plotnikov V.A. Digitization as a logicalstage in the evolution of an economic system. *Ekonomicheskoe vozrozhdenie Rossii = Economic Revival of Russia*, 2020, no. 2 (64), pp. 104–115. DOI: 10.37930/1990-9780-2020-2-64-104-115. (In Russ.).

3. Prolubnikov A.V. Platform model of state economic policy, in: *Mnogourovnevoe obshchestvennoe vosproizvodstvo: voprosy teorii i praktiki*, collection of scientific papers, Ivanovo, 2020, iss. 18 (34), pp. 21–34. (In Russ.).

4. Shvetsov A.N., Rysina V.N. "Digitalization" of public management in Russia against the background of best international practice. *ECO*, 2020, vol. 50, no. 2, pp. 60–80. DOI: 10.30680/ECO0131-7652-2020-2-60-80. (In Russ.).

5. Vertakova Y.V., Golovina T.A., Polyanin A.V. Synergy of Blockchain Technologies and “Big Data” in Business Process Management of Economic Systems, in: Popkova E., Sergi B. (eds.). *Digital Economy: Complexity and Variety vs. Rationality (ISC 2019)*, Lecture Notes in Networks and Systems; vol. 87, Cham, Springer Publ., 2020, pp. 856–865. DOI: 10.1007/978-3-030-29586-8_97.

6. von Blomberg M. The Social Credit System and China’s rule of law. *Mapping China Journal*, 2018, no. 2, pp. 78–112.

7. Goncharov V.V., Petrenko E.G., Borisova A.A., Tolmacheva L.V., Dmitrieva I.A. The system of social trust (social rating) in China: problems and prospects of implementation in the Russian Federation. *Administrativnoe i munitsipal'noe pravo = Administrative and municipal law*, 2023, no. 3, pp. 78–91. DOI: 10.7256/2454-0595.2023.3.39983. (In Russ.).

8. Katrashova Yu.V., Mityashin G.Yu., Plotnikov V.A. Social Rating System as a Form of State Control Over Society: Prospects for Implementation and Development, Threats to Realization. *Upravlencheskoe konsul'tirovanie = Administrative Consulting*, 2021, no. 2, pp. 100–109. DOI: 10.22394/1726-1139-2021-2-100-109. (In Russ.).

9. Creemers R. Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. *Journal of Contemporary China*, 2017, vol. 26, no. 103, pp. 85–100. DOI: 10.1080/10670564.2016.1206281.

10. Creemers R. *China's Social Credit System: An Evolving Practice of Control*. May 9, 2018. 32 p. DOI: 10.2139/ssrn.3175792.

11. Popov D.I. The Social Credit System Construction Plan as a Roadmap for Social Management Reform in China in the 2010s. *Vestnik Omskogo universiteta. Seriya "Istoricheskie nauki" = Herald of Omsk University. Series "Historical Studies"*, 2020, vol. 7, no. 1, pp. 147–157. DOI: 10.24147/2312-1300.2020.7(1).147-157. (In Russ.).

12. Petrov A. Human digital informational footprint. *Torgovaya politika = Trade policy*, 2020, no. 2 (22), pp. 62–86. DOI: 10.17323/2499-9415-2020-2-22-62-86. (In Russ.).

13. Petrov A.A. Chinese Digital Profile or Social Trust Scoring System. *Chronos*, 2020, no. 8 (46), pp. 11–24. (In Russ.).

14. Klimovich A.P. The impact of digital technologies on modern society. An example of a social credit rating system in China. *Tsifrovaya sotsiologiya = Digital Sociology*, 2020, vol. 3, no. 3, pp. 35–44. DOI: 10.26425/2658-347X-2020-3-3-35-44. (In Russ.).

15. Razumov E.A. New trends in the system of social rating and information security of China in the face of escalation of epidemiological situation. *Vestnik Dal'nevostochnogo otdeleniya Rossiiskoi akademii nauk = Vestnik of the Far East Branch of the Russian Academy of Sciences*, 2021, no. 1, pp. 132–135. DOI: 10.37102/0869-7698_2021_215_01_15. (In Russ.).

16. Buyarov D.V. The social credit system in the Xinjiang Uygur Autonomous Region of China. *Genesis: istoricheskie issledovaniya*, 2024, no. 4, pp. 99–108. DOI: 10.25136/2409-868X.2024.4.70522. (In Russ.).

17. Antoncheva O.A., Apanasenko T.E. Impact of the Social Credit System in China on Political Communication. *Upravlencheskoe konsul'tirovanie = Administrative Consulting*, 2022, no. 10, pp. 12–27. DOI: 10.22394/1726-1139-2022-10-12-27. (In Russ.).

18. Golubev S.G., Suhak V.K. Chinese social credit system as the tool of governance in the digital era. *Zhurnal Belorusskogo gosudarstvennogo universiteta. Sotsiologiya = Journal of the Belarusian State University. Sociology*, 2019, no. 4, pp. 62–74. (In Russ.).

ISSN 2542-1514 (Print)

19. Stepanov O.A., Stepanov M.M. Legal regulation of the genesis of digital identity. *Pravoprimenenie = Law Enforcement Review*, 2022, vol. 6, no. 3, pp. 19–32. DOI: 10.52468/2542-1514.2022.6(3).19-32.

20. Stepanov O.A., Stepanov M.M. On the legal response to the consequences of personal behavior in virtual space. *Pravoprimenenie = Law Enforcement Review*, 2024, vol. 8, no. 1, pp. 24–33. DOI: 10.52468/2542-1514.2024.8(1).24-33.

21. Stepanov O.A., Stepanov M.M. On digital identification of actions personality. *Gosudarstvo i pravo = State and Law*, 2024, no. 7, pp. 205–210. DOI: 10.31857/S1026945224070185.

22. Piza E., Welsh B., Farrington D., Thomas A. CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis. *Criminology & Public Policy*, 2019, vol. 18, no. 1, pp. 135–159.

23. Antropov R.V., Litsenberg I.I. The China's social system: the progressive mechanism of reward and punishment or digital dictatorship?, in: *Aktual'nye problemy razvitiya KNR v protsesse ee regionalizatsii i globalizatsii*, Proceedings of the 12th International scientific and practical conference, Chita, Transbaikal State University Publ., 2020, pp. 20–27. (In Russ.).

24. Petrov A.A. Chinese social evaluation system and electronic monitoring mechanisms, in: *Bol'shaya Evraziya: Razvitie, bezopasnost', sotrudnichestvo*, Annual, Proceedings of the Third international scientific and practical conference, Moscow, 2020, pp. 737–756. (In Russ.).

25. Glazunova E.N. Guantanamo: a story to be continued. *Vestnik Moskovskogo universiteta. Seriya 25: Mezhdunarodnye otnosheniya i mirovaya politika = Lomonosov World Politics Journal*, 2011, no. 3, pp. 153–183. (In Russ.).

26. Kryuchkov K.S. The Hoffman Report: Psychologists and Torture. An Ethical Precaution for Psychologists. *Konsul'tativnaya psikhologiya i psikhoterapiya = Counseling Psychology and Psychotherapy*, 2020, vol. 28, no. 1, pp. 148–165. DOI: 10.17759/cpp.2020280109.

INFORMATION ABOUT AUTHORS

Oleg A. Stepanov – Doctor of Law, Professor; Chief Researcher, Centre of Judicial Law
Institute of Legislation and Comparative Law under the Government of the Russian Federation
34, B. Cheremushkinskaya ul., Moscow, 117218, Russia
E-mail: soa-45@mail.ru
ORCID: 0000-0003-1103-580x
ResearcherID: O-9771-2019
Scopus AuthorID: 57208665632
RSCI SPIN-code: 8156-9725; AuthorID: 655914

Mikhail M. Stepanov – PhD in Law, Associate Professor; Leading Researcher, Department of Theory of Law and Interdisciplinary Research of Legislation
Institute of Legislation and Comparative Law under the Government of the Russian Federation
34, B. Cheremushkinskaya ul., Moscow, 117218, Russia
E-mail: stepanovtao@mail.ru
ORCID: 0000-0002-5203-1867
ResearcherID: AAX-2549-2020
Scopus AuthorID: 57215415345
RSCI SPIN-code: 2134-8209

BIBLIOGRAPHIC DESCRIPTION

Stepanov O.A., Stepanov M.M. Approaches to the legal regulation of artificial intelligence application in law enforcement. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 4, pp. 15–25. DOI: 10.52468/2542-1514.2025.9(4).15-25. (In Russ.).