DOI 10.52468/2542-1514.2025.9(3).64-73

PROBLEMS OF USING BIOMETRIC TECHNOLOGIES IN MUNICIPALITIES**

Anna Yu. Churikova[1,2], **Maria A. Lipchanskaya**[3,4]
[1] *Saratov State Law Academy, Saratov, Russia*
[2] *State University of Management, Moscow, Russia*
[3] *Russian State University of Justice, Moscow, Russia*
[4] *Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia*

Article info
Received –
2024 November 16
Accepted –
2025 June 20
Available
online – 2025
September
20

Keywords
Local government, digital transformation, artificial intelligence, biometric authentication, biometric identification, biometric personal data

Subject. The article analyzes issues related to the regulation and use of biometric technologies and biometric data. The choice of the object of the study is due to the intensive development and implementation of technologies based on the fact that biometric personal data are actively moving and used not only to provide power, but also in private organiza- tions. At the municipal level, the problems of legal regulation and law enforcement are especially acute.

The purpose of the study: based on the analysis of law enforcement practice and consider- ation of different approaches to regulating the use of biometric technologies, formulate specific proposals for improving the legal regulation of the use of biometric digital data when using face measurement technologies.

Methodology. The methodological substantiation of the study was a set of methods of cog- nition, the methods of which were: monitoring of law enforcement practice, comparative legal method, analysis method, systemic-structural method.

Conclusions. Based on the results of the study, the following conclusions were made:

(1) Municipal biometric technologies are used to provide food for the purpose of: ensuring labor safety on the territory of the municipality; biometric identification and authentication, including when providing municipal services; data analysis and planning.

(2) The conditions for limiting the rights and freedoms of an individual when using biometric technologies depend on the level of use of these technologies, as well as on the degree of regulatory regulation of their application. In conditions where the norms and rules are le- gally observed, the risks of negative consequences as a result of the use of data transmission technologies are the lowest. Blanket norms establishing exceptions for the use of biometric data have a negative impact on law enforcement practice.

(3) Excessively strict restrictions, as well as a ban on the use of municipal government organizations and commercial organizations, technologies, actors in real time, do not allow for the organization of an effective public safety system, and therefore it is necessary to establish balanced legal regulation. The harmonization of this area will be facilitated by in- troducing amendments to the current legislation proposed by the authors of the article, aimed at, on the one hand, protecting the rights of an individual when using face and emo- tion technologies in public places, and, on the other hand, ensuring the possibility of using data technologies for the purpose of creating a modern level of security for the population in the territory of a municipality.

** The research was carried out at the expense of the grant of the Russian Science Foundation No. 23-28-01252, https://rscf.ru/project/23-28-01252/, “Transformation of the institution of local self-government in the Russian Federation in the context of the development of modern digital technologies: legal aspects”, financing is carried out through the organization of State University of Management.

1. Introduction

Biometric identification and authentication technologies, including those used in real-time, are increasingly being adopted by municipal government organizations. These technologies can be employed to monitor public spaces and respond quickly to potential threats, allowing for timely prevention of offenses and maintenance of public order [1, pp. 123–125]. In this context, M. S. Ablameiko and R. P. Bogush note that “intelligent video surveillance systems have become an integral part of ‘smart cities’ today” [2, p. 15].

The creation of intelligent video surveillance systems for courtyards and municipal infrastructure facilities is one of the directions of the digital transformation of local self-government both in Russia and abroad [3, pp. 223–225; 4, pp. 3–7; 5, pp. 152–154]. However, the use of biometric technologies, especially in public places, raises several ethical and legal questions concerning the acceptability and limits of interference in citizens’ private lives [6, pp. 167–169; 7, pp. 121–125; 8, pp. 658–660]. The implementation of facial recognition technologies has led to complex problems related to privacy, protection of biometric personal data (hereinafter – BPD), and the lack of legal clarity regarding the capabilities and limits of BPD usage by municipal government organizations, private individuals, and law enforcement bodies [9, pp. 19–20; 10, pp. 80–81; 11; 12, pp. 828–831; 13, pp. 111–114].

This set of unresolved legal and practical issues related to the usage of biometric technologies, coupled with the need for a legal framework governing the use of such technologies by local authorities, underscores the high relevance of this topic.

Therefore, the goal of this study is to formulate specific proposals for improving existing legislation based on the analysis of law enforcement practices and various approaches to regulating the use of biometric technologies.

2. Research Methodology

The research involved monitoring law enforcement practices, searching for court rulings that referenced the use of facial recognition technologies and intelligent video surveillance systems, which helped identify practical issues in the usage of biometric technologies. The comparative legal method was used to explore different regulatory approaches to the use of biometric technologies. An interdisciplinary approach and analytical methods ensured a comprehensive and multi-perspective examination of the topic. In order to ensure a consistent study of the law enforcement issues related to the use of facial recognition technology by local authorities, a system-structural method was applied.

3. Comparative Legal Analysis of the Use of Biometric Identification and Authentication by Local Authorities

Facial and emotion recognition technologies based on BPD, also referred to as biometric technologies [14, p. 90], or biometric identification technologies [15, p. 33], are types of artificial intelligence (hereinafter also – AI) technologies [16, pp. 55–59; 17, p. 407; 18, pp. 55–53]. Under the 2024 Regulation of the European Parliament and Council (hereinafter – the EU AI Act), these are classified as high-risk technologies[1].

This classification in the EU stems from the high probability that these technologies may infringe on human rights and freedoms. The EU AI Act sets restrictions and lists conditions under which BPD may be used for remote biometric identification and categorization for law enforcement purposes. Russia imposes no such direct restrictions on biometric technology usage, but Article 11 of the Law on Personal Data[2] does limit BPD usage, applying a broad subjective approach to defining what constitutes BPD [19, pp. 80, 86].

Biometric technologies may be used by municipal government organizations in various areas and for different purposes, which determines their

[1] See: European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206; C9-0146/2021; 2021/0106(COD)). [Electronic resource] URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html#title1 (date of access: 27.08.2024).

[2] See: Federal Law of 27.07.2006 No. 152-FZ (as amended and supplemented on 08.08.2024, No. 233-FZ) “On Personal Data”. SZ RF. 2006. No. 31 (Part I), Art. 3451; 2024. No. 33 (Part I), Art. 4929.

impact on individual rights and interests. That is, *it is not the facial and emotion recognition technologies themselves that pose a risk, but the combination of their characteristics and areas of use*.

One of the most common applications of such technologies is maintaining public order. Intelligent video surveillance systems can perform real-time biometric identification [20, pp. 293–295; 21, pp. 586–588], aiding in the detection of offenders and identification during municipal control.

The concepts of biometric identification and authentication are defined in both the EU AI Act and the Russian Law on Identification and Authentication[3].

According to the EU AI Act, "biometric identification" is the automated recognition of physical, physiological, and behavioral traits such as facial features, eye movements, body shape, voice, prosody, gait, posture, heart rate, blood pressure, scent, and keystroke dynamics to establish a person's identity by comparing their data with entries in a reference database, regardless of the person's consent. This definition excludes biometric authentication that aims to confirm a person's identity to access a service, unlock a device, or enter a secured area. The distinction of these definitions is based on the differing risk categories associated with different purposes.

Under the EU AI Act, facial recognition to improve security in municipalities is restricted to searching for suspects, convicts, missing persons, or establishing identity in the event that it is impossible to obtain information from the person himself.

Using biometric technologies together with big data analytics can significantly improve the approach to solving management problems at the municipal level. For instance, video surveillance systems with facial recognition can collect data on the attendance of various facilities and events, thereby aiding their planning and organization. Some authors also suggest using facial recognition to tailor and optimize tourist services [22, pp. 1179–1180].

According to Article 9 of the Law on Identification and Authentication, local authorities may identify individuals using BPD via the "Unified System of Identification and Authentication of Physical Persons Using Biometric Personal Data" (ESIA), where identification results in discovering information about a person, while authentication results in confirming the person's identity[4].

S. S. Kuznetsova, A. N. Mochalov, and M. S. Salikov, comparing legal framework models of biometric identification in Russia and abroad, observe that Russian regulation "leans more towards the model adopted by China" [23, p. 263], that is, where public interests outweigh private ones. This approach has both positive and negative aspects. For example, S. Jia and C. Zhang point out that the problems in Chinese legal framework of the use of facial recognition technology lead to BPD leaks and unauthorized use [24, pp. 276–279].

In Russia, *the list of exceptions for BPD usage, established in the Law on Personal Data, is of a referential and non-specific nature*. Literal interpretation of the law would suggest that local authorities and private individuals cannot use BPD without consent to maintain order or provide services, including municipal ones; however, in practice, BPD and related technologies are widely used.

4. Practical Aspects of Using Biometric Technologies in Identification and Authentication

Despite the legal difficulties in using biometric technologies, they are actively used for identification of individuals by both government bodies and business entities, which makes it possible to form a unified system that helps ensure the safety of the population in a certain territory. For instance, under Order No. 12 of the Leningrad Region Committee for Public Order and Safety (dated May 08, 2024), video surveillance equipment and systems belonging to local government organizations, municipal institutions and enterprises, business entities operating in the Leningrad Region are included in the "Safe City" intelligent video surveillance

[3] See: Federal Law of 29.12.2022 No. 572-FZ "On the implementation of identification and (or) authentication of individuals using biometric personal data, on amendments to certain legislative acts of the Russian Federation and recognition of certain provisions of legislative acts of the Russian Federation as invalid". SZ RF. 2023. No. 1 (Part I), Art. 19.

[4] Letter of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation dated 28.12.2023 No. P24-2-04-070-257558 "On the forwarding of information". URL: https://www.consultant.ru/document/cons_doc_LAW_468549/ (date of access: 10.08.2024).

and video analytics system in the Leningrad Region[5].

Intelligent video surveillance cameras with facial recognition capabilities are commercially available and used by many commercial organizations and individuals, making this technology available not only for use by state and municipal authorities. Facial recognition systems often allow not only to establish a person's identity, but also to detect crimes. For example, in case No. 1-367/2023, *it was possible to establish the fact of theft of funds and detain the person who committed this criminal act thanks to the facial recognition system. The store director received a notification through the "facial recognition control" application about the recognition of an unknown man in the office, which allowed her to promptly approach the premises and prevent the person who entered it from escaping*[6]. In this case, a person whose biometric data was not entered into the system was recognized. However, in case law, there are frequent instances of entering the biometric data of persons without their consent by representatives of commercial organizations into the relevant system. For example, *a store employee, having reviewed the records from the CCTV cameras installed in the store, discovered that a man had entered the store, taken the goods and left the store without paying for the goods. The store employee entered the image of the face of the man who stole the goods into the facial recognition system installed in the network of these stores. On the same day, he received a message from the facial recognition system on his phone that the man whose BPD was entered into the system was in the store. The store security detained this man, despite the fact that this time he did not steal anything*[7].

In case all facial recognition systems used by commercial organizations in the territory of a municipality are considered as an integral part of the security system in the territory of the municipality, then, undoubtedly, there are certain advantages in such use of biometric technologies. However, issues related to the use of facial recognition technologies by commercial organizations in situations similar to those considered are not regulated. It is necessary to take measures to prevent the risks of unfair use of biometric technologies. It also seems necessary to inform municipal authorities about the use of such technologies by commercial organizations in the territory of the municipality, which would contribute to the local governments' development of a system of ensuring the safety of the population in the territory of the municipality.

The use of biometric identification and authentication of individuals in the provision of municipal services is also an important area of application of biometric technologies, which can simplify access to the services provided and, at the same time, ensure reliable identification of the individual. In case law, the consideration of complaints received electronically without appropriate identification, authentication, in the absence of an electronic signature is recognized as illegal, even if these requests were received through the official services of state and municipal authorities. *For example, the decision of the deputy head of the State Administrative and Technical Inspectorate was recognized by the court as illegal, since the complaint on which this decision was made was received through the electronic appeals service to the inspectorate, and not through the public services portal, it was not signed with an electronic signature, and the applicant did not have "the presence of a confirmed ESIA"* [8].

It seems that the requirement for mandatory identification and authentication should not limit the ability of citizens and organizations to interact with municipal authorities in digital format. The rules for such interaction should be explained. At the same time, if it is necessary to submit certain types of

[5] Order of the Leningrad Region Committee for Public Order and Safety dated 08.05.2024 No. 12 "On approval of requirements for local video surveillance systems and additional technological data transmission channels included in the intelligent video surveillance and video analytics system of the hardware and software complex 'Safe City' in the Leningrad Region." URL: https://npa.lenobl.ru/docs/government/view/108656/ (date of access 19.08.2024).

[6] Sentence No. 1-367/2023 of August 21, 2023 URL: https://судебныерешения.рф/77750071 (date of access 18.07.2024).

[7] Sentence No. 1-975/2023 of October 12, 2023 URL: https://судебныерешения.рф/78098889 (date of access: 19.07.2024).

[8] Decision No. 12-564/2024 of July 15, 2024 [Electronic resource] URL: https://судебныерешения.рф/83504537 (date of access 18.08.2024).

complaints or requests with identification and authentication specifically through the website of state and municipal services, then redirection of users should be ensured when attempting to submit these complaints or requests through other services of state or municipal authorities.

Problems also arise when supplying equipment and software. Thus, in case No. 22-2544/2023, the investigating authorities accused the director of a municipal state institution (acquitted due to the absence of a criminal offence in his actions) of failing to take measures to organize proper control over the verification of the quality characteristics of video surveillance cameras supplied under a municipal contract for the provision of services for the creation of an intelligent video surveillance system for courtyards. From the testimony of an engineer interrogated as a witness, it follows that during the work there were difficulties with setting up the cameras due to failures in face recognition, in addition, after replacing the cameras, without firmware and writing software, the new cameras would not perform their functions. This demonstrates the practical importance of creating equipment and developing high-quality domestic software that allows the use of biometric technologies. In this regard, we consider the proposal by K. A. Ponomareva on the need to establish support measures for IT companies in national legislation, as well as the need to "provide for special rules for calculating and paying income tax for foreign digital companies and, meantime, expand tax incentive measures for Russian companies" [25, p. 618], to be justified.

5. Proposals for solving the identified problems of legal regulation and law enforcement

In order to provide for the possibility of using facial recognition technology by municipal organizations for the purposes of ensuring security and law and order on the territory of the municipality, as well as for the purposes of protecting the human and civil rights and freedoms when using this technology in public places, we propose introducing the following changes to the current legislation:

1) Add Part 1.1 to Article 11 of the Personal Data Law with the following content: "1.1. In places where technologies are used that allow identification of a person using biometric personal data, information about the use of this technology is mandatorily provided by placing identification marks.";

2) Add to Part 2 of Article 11 of the Personal Data Law the following sentence: "Biometric personal data may be entered into the facial recognition system without the informed voluntary consent of the person if there are factual documented grounds, including photo, video and audio data, allowing to suspect illegal behavior of the person. Notification of the entry of biometric personal data into the facial recognition system without the consent of the personal data subject, as well as the reasons for entering such information within 24 hours must be sent to the authorized body for the protection of the rights of personal data subjects".

It would also appear necessary to create a mandatory list of organizations that use biometric technologies in the territory of a municipality, which will facilitate fast and effective interaction between local government organizations, law enforcement agencies and representatives of business entities.

5. Conclusion

The conducted research allows making the following main conclusions and proposals:

1) in the European Union, significant restrictions are established on the use of biometric technologies in cases where their use hinders the exercise of the right to privacy of an individual, as well as other rights and freedoms guaranteed by law. In Russia, it is not the use of the technologies that is limited, but the use of the BPD, which also leads to a narrowing of the list of possibilities for using the relevant technologies;

2) municipal organizations may use biometric technologies for the following purposes: ensuring the safety of the population on the territory of the municipality; undergoing biometric identification and authentication, including when providing municipal services; data analysis and planning;

3) the likelihood of limiting the rights and freedoms of an individual when using biometric technologies depends on the areas of use of these technologies, as well as on the degree of normative regulation of their application. In the absence of legislatively established norms and rules, the most substantial risks of negative consequences from the arbitrary use of these technologies arise. The blanket nature of the rules establishing exceptions for the use of BPD has a negative impact on law enforcement

practice;

4) excessively strict restrictions, as well as a ban on the use of real-time facial recognition technologies by municipal authorities and commercial organizations, will not ensure the organization of an effective public safety system, wherefore it is necessary to establish balanced legal regulation. The harmonization of this area could be contributed to by the adoption of amendments to the current legislation proposed by the authors of the article, aimed at, on the one hand, protecting the rights of the individual when using facial and emotion recognition technologies in public places, and, on the other hand, ensuring the possibility of using these technologies in order to create a high level of security for the population on the territory of the municipality.

REFERENCES

1. Kuteynikov D.L., Izhaev O.A., Lebedev V.A., Zenin S.S. Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification. *Lex Russica*, 2022, vol. 75, no. 2, pp. 121–131. DOI: 10.17803/1729-5920.2022.183.2.121-131. (In Russ.).

2. Ablameyko M., Bogush R. Intelligent video surveillance in "smart city": control and protection of visual personal data. *Sudebnaya ekspertiza Belarusi = Forensic Examination of Belarus*, 2023, no. 1 (16), pp. 15–23. (In Russ.).

3. Mozhaeva S.Yu., Mozhaev S.A. About some issues of using biometric identification for the purposes of identifying crimes and offenses of supervised persons. *Vestnik Voronezhskogo instituta MVD Rossii = Vestnik of Voronezh institute of the Ministry of the interior of Russia*, 2024, no. 2, pp. 223–227. (In Russ.).

4. Bibri S.E., Krogstie J. A Novel Model for Data-Driven Smart Sustainable Cities of the Future: A Strategic Roadmap to Transformational Change in the Era of Big Data. *Future Cities and Environment*, 2021, vol. 7, art. 3. DOI: 10.5334/fce.116.

5. Benkő M., Bene B., Pirity Á., Szabó Á., Egedy T. Real vs. Virtual City: Planning Issues in a Discontinuous Urban Area in Budapest’s Inner City. *Urban Planning*, 2021, vol. 6, no. 4, pp. 150–163. DOI: 10.17645/up.v6i4.4446.

6. Smith M., Miller S. The ethical application of biometric facial recognition technology. *AI & Society*, 2022, vol. 37, iss. 1, pp. 167–175. DOI: 10.1007/s00146-021-01199-9.

7. Mann M., Smith M. Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal*, 2017, vol. 40, iss. 1, pp. 121–145. DOI: 10.53637/KAVV4291.

8. Kavoliūnaitė-Ragauskienė E. Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union. *Journal of Human Rights Practice*, 2024, vol. 16, iss. 2, pp. 658–674. DOI: 10.1093/jhuman/huad065.

9. Babaeva Yu.G., Israelyan V.B. Biometrical image: legal regulation of a person’s digital data. *Vestnik Universiteta Pravitel'stva Moskvy = MMGU Herald*, 2022, no. 3 (57), pp. 17–23. (In Russ.).

10. Zatolokin A.A., Streltsov V.V. Administrative and legal aspects of state regulation of biometric personal data processing. *Obshchestvo i pravo = Society and Law*, 2023, no. 1 (83), pp. 79–83. (In Russ.).

11. Pereira R.S. Remarks on the Use of Biometric Data Systems (and Facial Recognition Technologies) for Law Enforcement Purposes: Security Implications of the Proposal for an EU Regulation on Artificial Intelligence, in: Moura Vicente D., de Vasconcelos Casimiro S., Chen C. (eds.). *The Legal Challenges of the Fourth Industrial Revolution. The European Union's Digital Strategy*, Law, Governance and Technology Series; vol. 57, Cham, Springer Publ., 2023, pp. 193–209. DOI: 10.1007/978-3-031-40516-7_11.

12. Utegen D., Rakhmetov B.Zh. Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. *Journal of Digital Technologies and Law*, 2023, vol. 1, no. 3, pp. 825–844. DOI: 10.21202/jdtl.2023.36.

13. Kovaleva N., Zhirnova N. Issues of Ensuring the Confidentiality of Personal Data When Using Artificial Intelligence Systems. *Zhurnal rossiiskogo prava = Journal of Russian Law*, 2024, vol. 28, no. 7, pp. 109–121. DOI: 10.61205/S160565900027561-1. (In Russ.).

14. Ryvkin S.Yu., Galkina V.A. Biometric technologies – a new level of human identification. *Moya professional'naya kar'era*, 2019, no. 7, vol. 4, pp. 90–95. (In Russ.).

15. Afanasev S.D., Tereshchenko I.A., Yatskevich D.A. Biometric identification and human rights: the line of demarcation. *Zakon*, 2022, no. 3, pp. 33–46. DOI: 10.37239/0869-4400-2022-18-3-33-46. (In Russ.).

16. Kolodenkova A.E. Ontology of human identification by face and body motions in video surveillance systems. *Ontologiya proektirovaniya = Ontology of Designing*, 2023, vol. 13, no. 1, pp. 55–74. DOI: 10.18287/2223-9537-2023-13-1-55-74. (In Russ.).

17. Mishchenko E.Y., Sokolov A.N. Model of Identification of a Person in Databases of Various Sizes, in: *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, IEEE Publ., 2021, pp. 407–410. DOI: 10.1109/USBEREIT51232.2021.9455020.

18. Ivanov V.A., Smirnov A.A., Nikolaev D.A. The real probability of recognizing images of people's faces using artificial neural networks. *Radiotekhnika*, 2022, vol. 86, no. 1, pp. 55–60. DOI: 10.18127/j00338486-202201-09. (In Russ.).

19. Krivogin M.S. Peculiarities of Legal Regulating Biometric Personal Data. *Pravo. Zhurnal Vysshei shkoly ekonomiki = Law. Journal of the Higher School of Economics*, 2017, no. 2, pp. 80–89. (In Russ.).

20. Jaiswal A., Tarar S. Real-Time Biometric System for Security and Surveillance Using Face Recognition, in: Singh M., Gupta P., Tyagi V., Flusser J., Ören T., Valentino G. (eds.). *Advances in Computing and Data Sciences*, 4th International Conference, ICACDS 2020, Valletta, Malta, April 24–25, 2020, Revised Selected Papers, Communications in Computer and Information Science; vol. 1244, Singapore, Springer Publ., 2020, pp. 293–304. DOI: 10.1007/978-981-15-6634-9_27.

21. Fabrègue B.F.G., Bogoni A. Privacy and Security Concerns in the Smart City. *Smart Cities*, 2023, vol. 6, iss. 1, pp. 586–613. DOI: 10.3390/smartcities6010027.

22. Gupta S., Modgil S., Lee C.K., Sivarajah U. The future is yesterday: Use of AI-driven facial recognition to enhance value in the travel and tourism industry. *Information Systems Frontiers*, 2023, vol. 25, iss. 3, pp. 1179–1195. DOI: 10.1007/s10796-022-10271-8.

23. Kuznetsova S.S., Mochalov A.N., Salikov M.S. Biometric identification on the Internet: Trends of legal regulation in Russia and in foreign countries. *Vestnik Tomskogo gosudarstvennogo universiteta = Tomsk State University Journal*, 2022, no. 476, pp. 257–267. DOI: 10.17223/15617793/476/28. (In Russ.).

24. Jia S., Zhang J. Legal protection of a citizen's right to a facial image when applying facial recognition technology in Chinese law. *Pravovedenie*, 2024, vol. 68, no. 2, pp. 271–283. DOI: 10.21638/spbu25.2024.210. (In Russ.).

25. Ponomareva K.A. Legal Issues of Taxation of Digital Business Models. *Vestnik Permskogo universiteta. Yuridicheskie nauki = Perm University Herald. Juridical Sciences*, 2022, iss. 58, pp. 605–620. DOI: 10.17072/1995-4190-2022-58-605-620. (In Russ.).

INFORMATION ABOUT AUTHORS

Anna Yu. Churikova – PhD in Law, Associate Professor; [1]Associate Professor, Department of Information Law and Digital Technologies; [2]leading researcher
[1] *Saratov State Law Academy*
[2] *State University of Management*
[1] 1, Vol'skaya ul., Saratov, 410056, Russia
[2] 99, Ryazanskii pr., Moscow, 109542, Russia
E-mail: a_tschurikova@bk.ru
ORCID: 0000-0003-0299-622X
ResearcherID: AAV-8381-2020
Scopus AuthorID: 58251251000
RSCI SPIN-code: 9809-3156; AuthorID: 713265

Maria A. Lipchanskaya – Doctor of Law, Professor; [1]Professor, Department of Constitutional Law named after N.V. Vitruk; [2]Professor, Department of State and Legal Disciplines of the Institute of Social and Cultural Studies
[1] *Russian State University of Justice*
[2] *Russian Presidential Academy of National Economy and Public Administration*
[1] 69, Novocheremushkinskaya ul., Moscow, 117418, Russia
[2] 82, Vernadskogo pr., Moscow, 119602, Russia
E-mail: lipchan_maria@mail.ru
ORCID: 0000-0002-4410-0578
ResearcherID: ABC-6179-2020
Scopus AuthorID: 57218912583
RSCI SPIN-code: 9665-2557; AuthorID: 360796

BIBLIOGRAPHIC DESCRIPTION

Churikova A.Yu, Lipchanskaya M.A. Problems of using biometric technologies in municipalities. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 3, pp. 64–73. DOI: 10.52468/2542-1514.2025.9(3).64-73. (In Russ.).