Legal Issues of Digital Age. 2025. Vol. 6, no. 2.
Вопросы права в цифровую эпоху. 2025. Том 6. № 2.

Research article
JEL: K00
UDK: 340
DOI:10.17323/2713-2749.2025.2.118.133

Smart Digital Facial Recognition Systems in the Context of Individual Rights and Freedoms

Oleg A. Stepanov[1], Denis A. Basangov[2]

[1, 2] Institute of Legislation and Comparative Law under the Government of the Russian Federation; 34 Bolshaya Cherymushkinskaya Str., Moscow, Russia 117218

[1] soa-45@mail.ru. https://orcid.org/0000-0003-1103-580x

[2] d_basang@mail.ru, https://orcid.org/0000-0002-2776-4241

Abstract

The authors discuss the problem of digital facial recognition technologies in the context of implementation of individual rights and freedoms. The analysis is focused on whether their use is legitimate and on interpretation of the provisions behind the underlying procedures. The authors note a significant range of goals to be addressed through the use of smart digital systems already at the goal-setting stage: economy, business, robotics, geological research, biophysics, mathematics, biophysics, avionics, security systems, health, etc. Higher amounts of data and a broader range of technologically complex decision-making objectives require to systematize the traditional methods and to develop new decision-making methodologies and algorithms. Progress of machine learning and neural networks will transform today's digital technologies into self-sustained and self-learning systems intellectually superior to human mind. Video surveillance coupled with smart facial recognition technologies serves above all public security purposes and can considerably impact modern society. The article is devoted to the theme of legitimate use of digital facial recognition technologies and to the interpretation of provisions laying down the underlying procedures. The authors' research interests assume an analysis of legal approaches to uphold human rights as digital facial recognition systems are increasingly introduced into social practices in Russia, European Union, United Kingdom, United States, China. The purpose of article is to shed light on regulatory details around

© Stepanov O.A., Basangov D.A., 2025
This work is licensed under a Creative Commons Attribution-Sharealike 4.0 International License
https://creativecommons.org/licenses/by-sa/4.0/legalcode.en

the use of AI systems for remote biometric identification of persons in the process of statutory regulation. Methods: formal logic, comparison, analysis, synthesis, correlation, generalization. Conclusions**:** the analysis confirms that facial recognition technologies are progressing considerably faster than their legal regulation. Deployment of such technologies make possible ongoing surveillance, a form of collecting information on private life of persons. It is noted that accounting for these factors requires amending the national law in order to define the status and the rules of procedure for such data, as well as the ways to inform natural persons that information associated with them is being processed.

Keywords

smart digital systems; facial recognition; regulation; remote biometric identification of persons; balancing; private and public interests.

For citation: Stepanov O.A., Basangov D.A. (2025) Smart Digital Facial Recognition Systems in the Context of Individual Rights and Freedoms. *Legal Issues in the Digital Age,* vol. 6 , no. 2, pp. 118–133. DOI:10.17323/ 2713-2749.2025.2.118.133

Background

Digital technologies play a key role in transforming modern societies and in reinventing public governance practices. Meanwhile, their introduction into social relations raises serious concerns over security of individuals and the state.

Awareness of the potential to record someone's actions on a storage device is a major factor containing personal behavior [Gordon B., 2021: 1–29].

A study fulfilled in 2004 by B. Welsh from the University of Massachusetts and D. Farrington from the University of Cambridge has showed: where CCTV cameras were installed, street crime declined by 21 percent, with the highest decline observed in parking lots and in locations that, apart from being provided with cameras, were well-lit.

The progress of such technologies relies today on capabilities of AI systems, with society to adapt to the challenges and opportunities enabled by these systems in the process of automatic remote identification of individuals based on unique physical, biological or behavioral features.

Mordor Intelligence, a market research firm, estimated the facial recognition market at USD 6.61 billion in 2024, with prospects to reach

USD 14 billion by 2029 (at the average growth rate of 16.20 percent over the forecast period of 2024–2029)[1].

1. Facial Recognition Technologies

Technological corporations such as Amazon Web Services, Microsoft Azure and Google Cloud are currently validating different tools that use facial recognition to unlock smartphones, as well as services like Google's *Find My Face* that law-enforcement bodies use to counter terrorist threats and mass riots [Grigoriev V.N., 2021: 334–355].

A major outcome of their development and dissemination is that biometric data (such as the face geometry), once in the hands of unauthorized persons, cannot be altered since they are directly associated with a particular person[2].

Moreover, biometric identification methods used simultaneously (in parallel) both online and offline will make the boundary between man and his digital twin very much arbitrary. Thus, the existence and operation of the digital twin (avatar) endowed with a number of capabilities in the virtual space will directly impact the rights, duties, freedoms and legitimate interests of the real human person. A leakage of these biometric data will compromise them, only to considerably restrict not only their possible use but also recovery of the violated rights [Kitchin R., Dodge M., 2021: 112, 114, 125].

For instance, Apple's *Face ID*, a facial recognition technology, was hacked by the Vietnamese company B kav immediately after it went on sale. Source data to produce a human face mask by 3D printing at the cost of approximately USD 150[3] may be easily borrowed from a person's profile on social media. This circumstance aggravates the threat from unauthorized use of private data including as part of the critical infra-

[1] Analysis of the facial recognition market size and shares—growth trends and forecasts (2024–2029). Available at: URL: https://www.mordorintelligence.com/ru/industry-reports/facial-recognition-market (accessed: 26.11.2024)

[2] Daly M.P. et al. Biometrics Litigation: An Evolving Landscape (Practical Law Litigation, April–May 2016). Available at: URL: https://uk.practicallaw.thomsonreuters.com/w-001- 8264?lrTS=20170720182117024&transitionType=Default & context Data=(sc.Default)&first Page=true (accessed: 26.11.2024)

[3] Facial recognition from A to Z for video analytics, video surveillance and access control. Available at: URL: https://securityrussia.com/blog/face-recognition.html (accessed: 26.11.2024)

structure operation since technological capabilities to store information are not confined to national borders, with cloud storage available anywhere across the planet [Huang J., 2020: 1283–1308].

The rapid introduction of facial recognition technologies calls for enhancing the regulatory role of law in this process as their use can result in serious problems of non-selective coverage and inordinate number of individuals subject to arbitrary identification whereas only specific persons need to be identified (for example, at airports and railway stations). No-touch nature of such identification already raises problems associated with a lack of proper legal basis to process personal data, only to result in negative implications for the persons concerned.

Thus, in October 2020, a certain Mr. A. Leushin was held in custody by the guards at Moscow's Auchan supermarket before arrival of the police when a facial recognition system identified him as someone who had stolen78 thousand of rubles worth of fine spirits from this supermarket, with the error not admitted until hours later. In February 2023, the hydrologist A. Tsvetkov was detained when boarding a plane when a neural network decided his face was 50 to 60 percent similar to that of a video fit. In custody for a year on charges of murders dating back to 2002, the scientist had a heart attack and was not released until February 2024 following a vigorous public campaign[4].

If, in view of the above cases, we define the facial recognition technologies as digital algorithms which by comparing two or more facial images can identify or verify them using data in databases for biometric authentication to determine the data's owner[5], the use of such technologies can considerably impact the exercise of individual rights and freedoms.

It is worth noting that video surveillance systems have become widely used in Russia since 2016, with the first 1.5 thousand cameras installed outdoors and in doorways in Moscow for testing[6]. In 2018, this system

[4] 5 cases when facial recognition systems nearly destroyed human lives. Available at: URL: https://skillbox.ru/media/business/5-sluchaev-kogda-sistema-raspoznavaniya-lits-edva-ne-razrushila-zhizn-cheloveka-po-oshibke/ (accessed: 27.11.2024)

[5] Sarabdeen J. Protection of the rights of the individual when using facial recognition technology. Available at: URL: https://pubmed.ncbi.nlm.nih.gov/35309394/ (accessed: 28.10.2024)

[6] Facial recognition system allowed to identify almost 1.500 criminals in Moscow over 3.5 years. Available at: URL: https://www.tadviser.ru/index.php/

was expanded following trial at the World Football Cup where surveillance cameras helped to detain almost 180 persons wanted by the federal police. Moscow's surveillance system was also used in 2020 during the pandemic to identify and penalize more than 200 breaches of lockdown and self-imposed isolation[7]. By that time, the *Safe City* public system was deployed in 40 constituent territories of Russia, with smart digital systems for remote facial identification in use across 13 constituent territories (including cities of Saint-Petersburg, Ryazan and Saratov, also Kamchatka and the Crimea)[8]. In 2021, the Moscow City Office arranged for shopping centers to be connected to the video surveillance system under the administrative procedure, to be followed by Moscow schools [Bobrinskiy N.A., 2020: 91].

2. Regulatory Challenges of Facial Recognition in Russia and Elsewhere

The Russian Federation presently does not have statutory regulation of remote facial recognition systems that would strike a balance between individual interests to safeguard privacy and those of the state related to security and optimization of specific procedures (such as personal identity verification at transport, sport shows, etc.) [Zharova A.K., 2019: 73].

Since it is not determined to what extent digital video surveillance systems with personal identification capabilities are allowed to invade privacy, the result is prosecutorial bias of judicial and other law enforcement practices.

In Federal Law No. 152-FZ "On Personal Data" of 27 July 2006[9], biometric personal data are defined as describing physiological and biological features that identify an individual. Moreover, this Law regulates how these data are processed in absence of the individual's consent, for example, to uphold the national security and defense or combat terrorism (Article 11).

Проект:Как_устроена_система_распознавания_лиц_в_Москве?ysclid=m2uaa7tv2v145186906 (accessed: 26.11.2024)

[7] Smart Moscow City. Video surveillance system in Moscow. Available at: https://www.tadviser.ru/index.php (accessed: 26.11.2024)

[8] Gaynutdinov D., Koroteev K. Facial recognition: a foretaste of dystopia: a report. Available at: URL: https:// runet.report/static/core/doc/Facial_recognition.pdf (accessed: 28.11.2024)

[9] Collected Laws of Russia, 31.07.2006, № 31 (part 1), Art. 3451.

Meanwhile, the procedures to collect and analyze big data including digital footprints is still not properly regulated by law [Pashentsev D.A., Zaloilo M.V., Ivanyuk O.A., 20]; [Maslovskaya T.S., 2019: 59–69]. Provisions of Federal Law No. 149-FZ "On Information, Information Technologies and Data Protection" of 27 July 2006[10] (Federal Information Law) do not capture the progress of relationships in big data as to legal mechanisms behind public enforcement decisions and follow-up control by public institutions. From the perspective of the constitutional right to privacy, automatic collection and processing of biometric data is not regulated by any statutory provision [Kartashov A.S., 2022: 107].

In this regard, it is only logical to raise the question whether facial images from CCTV cameras installed in public places (shopping centers, airports, railway stations etc.) could be considered biometric data.

Under the Civil Code (para 2, part 1, Article 152.1), if someone's image was taken in a public place, provided that this image is not the main thing being used, no consent will be sought. However, this legal stance for the use of biometric data was formulated long before smart digital systems for remote facial identification started to be deployed in Russia. The content of privacy did not capture someone's presence in public places — moreover, being in a public place at a certain time was opposed to private life[11]. This principle objectively allowed to draw a line between the private and the public sphere before the latter was inundated with smart digital systems for facial identification[12].

Since 29 December 2020, the list of grounds for non-consented biometric data processing was legally extended to notarial needs[13] following

[10] Collected Laws of Russia, 31.07.2006, No. 31 (part 1), Art. 3448.

[11] As was explained by the Roskomnadzor (2013), facial images are not deemed biometric data before they are sent to competent authorities for identification. It is enough for the administration of a public place to make textual or graphic announcements to visitors that they might be under surveillance by photo and/or video cameras. According to the agency, once these conditions are met, no consent to surveillance is required // Explanations on treating photo and video footage, fingerprints and other information as biometric personal data and their processing procedure. Available at: URL: https://pd.rkn.gov.ru/press-service/subject1/news2729/ (accessed: 26.11.2024)

[12] Pozdnyakov V. The legitimacy of facial identification by cameras in public places. Available at: URL: http://www.it-lex.ru/faq/zakonnost-raspoznavaniya-lic/ (accessed: 28.10.2024)

[13] See: Federal Law No. 480-FZ "On Amending the Fundamental Law on the Notarial System and Specific Regulations of Russia" of 27.12.2019 // Collected Laws of Russia, 30.12.2019, No. 52 (part I), Art. 7798; Federal Law No. 537-

connectivity of the notarial system to the universal biometric system of the Russian Federation for biometric identification of those referring to notarial services.

In 2017, the Federal Information Law came to include Article 14.1[14], regulating the process of identification through the use of personal biometric data. This was the first step towards the regulatory framework of the universal biometric system[15] for remote identification of individuals by using control templates with appropriate biometric details. Further legislative changes[16] considerably expanded the opportunities for identification to cover any natural persons, not only Russian nationals. Moreover, the Federal Information Law does not constraint possible use of private information systems to process any biometric personal data including collection and storage.

Under the Law on the Universal Biometric System, in force since December 2022[17], primary biometric samples are to be stored in the public system in a coded form, with mathematical data codes (vectors) available to businesses. Also, while the storage of biometric personal data is prohibited by law, UBS vector processing is allowed. It is assumed that personal data of users will be impossible to decode in the event of leakage from the business storage. Since 1 June 2023 the law allows individuals to withdraw from collecting and storing biometric personal data for the purpose of identification and authentication.

Following the passing of Federal Law No. 127-FZ "On Amending Specific Regulation of Russia" of 14 April 2023[18] (Military E-Summons

FZ "On Amending the Federal Law on Non-State Pension Funds of 30.12.2020 Regarding Protection of Rights and Legitimate Interests of Insured Persons in Choosing the Insurer for Mandatory Pension Insurance, and Article 42 of Russia's Fundamental Law on the Notarial System" // Collected Laws of Russia, 04.01.2021, No. 1 (part I), Art. 76.

[14] Federal Law No. 482-FZ "On Amending Specific Regulations of Russia" of 31.12.2017 // Collected Laws of Russia, 01.01.2018, No. 1 (part I), Art. 66 (voided).

[15] While the Ministry of Telecommunications announced the creation of the UBS back in 2016, consistent efforts to draft the regulatory framework for this initiative were made in the following years.

[16] Federal Law No. 479-FZ "On Amending Specific Regulations of Russia" of 29.12.2020 // Collected Laws of Russia, 04.01.2021, No. 1 (part I), Art. 18.

[17] Federal Law No. 572-FZ "On Identifying and/or Authenticating Natural Persons through the Use of Biometric Personal Data, Amending Specific Regulations of Russia and Voiding Specific Provisions" от 29.12.2022 // Collected Laws of Russia, 02.01.2023, No. 1 (part I), Art. 19.

[18] Federal Law No. 127-FZ "On Amending Specific Regulations of Russia" of 14.04.2023 // Collected Laws of Russia, 17.04.2023, No. 16, Art. 2764.

Law), digital facial recognition will be used to identify those evading conscription.

In 2024 the Ministry of Digitization, Ministry of Transport and the RZhD (Russian Railways) have announced an experiment to verify passengers by their biometric data. The use of biometric data for identification when boarding the train will be voluntary, with the service not to be denied to those who refuse[19].

In accordance with Federal Law No. 197-FZ "On Amending the Federal Law on Motor ways and Road Management in Russia and on Amending Specific Regulations" of 29 May 2023, the information on location of stationary and mobile speed cameras and/or transport routes with installed speed cameras should be made public since 1 September 2024 at the official website of the Ministry of Interior[20].

However, no agency in Russia assumes overall responsibility for processes related to facial recognition, and no mechanism allows to check compliance with the procedure for deletion of incorrect biometric data from smart CCTV systems as the key is to define to what extent the biometric identification by facial geometry and other anthropometric data is allowed. Moreover, it is crucial is to account for the difference between footage from video cameras scattered across public places and those integrated into a single smart system for remote facial recognition.

In this connection, it is of interest to discuss A. Popova's appeal against the IT Department of Moscow and Moscow's Head Office of the Ministry of Interior in 2019 regarding the municipal CCTV system. In support of her claims at the trial, the appellant has indicated that the said system violated a number of individual rights guaranteed by the Constitution (Articles 23, 24). In her view, any biometric data processing by the operator should be consented by the affected individual. If this requirement is violated, the constitutional right to privacy is not guaranteed[21].

---

[19] Mass media reported the RZhD planned experiment to identify passengers by their faces. Available at: URL: https://www.forbes.ru/tekhnologii/493537-kommersant-uznal-o-planah-poeksperimentirovat-s-licami-passazirov-poezdov?ysclid=m2vk5w5wjd40876130 (accessed: 26.11.2024)

[20] Starting from 1 September 2024, speed cameras are subject to specific requirements. Available at: URL: https://www.consultant.ru/law/hotdocs/80387.html (accessed: 16.01.2025)

[21] Information on case No. 02A-0577/2019- Available at: https://www.mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc (accessed: 26.11.2024)

In dismissing the claims[22], the Savyolovsky District Court of Moscow has noted that the use of this technology did not constitute prohibited methods of information processing. Where no personal identification procedure is invoked, video images of an individual cannot amount to biometric personal data. For this reason, public agencies do not need to seek a person's consent for processing biometric personal data.

The court also has emphasized that since the surveillance system directly served the public security purposes, it was not the source of personal data in the sense defined by the personal data law.

This decision of the Savyolovsky District Court later constituted the crucial enforcement instrument behind the legitimacy of video surveillance systems both in Moscow and elsewhere in Russia.

Remote biometric identification by smart digital technologies with restricted access to data under the law of criminal procedure and other regulations does not prevent courts from recognizing it automated personal data processing [Andreeva I.O., 2019: 12]. However, biometric data processing should envisage specific guarantees to avoid misuse of this digital technology, a provision needed to avoid violation of constitutional rights of individuals in absence of uniform enforcement practices [Zorkin V.D.].

According to the lawyer E. Abashina, no provision indicates to what extent two images should be similar for corrective action to apply to an individual, be it additional law enforcement intelligence or court action on administrative offense[23]. This prompts a more profound scrutiny of the question on behavior of someone not involved in a misdeed, in particular, whether it is legitimate to process behavioral data in the continuous mode where the person did not consent to be identified by the smart system[24].

Detractors of facial recognition technologies believe they arbitrarily expand the scope of authority of the police and other special services by offering a tool too attractive and uncontrolled to avoid misuse.

---

[22] The Moscow City Court upheld this decision as the appellate instance.

[23] How the authorities use cameras and facial recognition against protestors. Available at: URL: https://ai-news.ru/2022/01/kak_vlasti_ispolzuut_kamery_i_raspoznavanie_lic_protiv_protestuushih.html (accessed: 23.11.2024)

[24] Dual use cameras: dangers of the facial recognition system. Available at: https://www.rbc.ru/spb_sz/10/10/2019/5d9efecb9a794718418b1e64?ysclid=m2orb29ofm715521384 (accessed: 26.11.2024)

These concerns are caused by the technological possibility to set up cameras to detect only faces of a certain race or ethnicity where it may be reasonable from the statistical point of view.

These concerns are shared by the European Data Protection Board (EDPB), digital sector regulator, whose representatives in 2021 invited the governments to give up expansion of the surveillance camera network and dismantle those already installed. In their view, the current facial recognition practices violated the European rights to privacy and freedom of movement.

Also in 2021, the Advisory Committee of the Council of Europe[25] proposed to prohibit using facial recognition technologies to identify sex, race, color of the skin, ethnicity, social status, health condition, religion and other parameters.

The European AI Act of March 2024[26] allows for restricted use of biometric recognition technologies under very limited scenarios related to crime prosecution and investigation where decisions are to be made promptly such as searching for missing children, preventing terrorist attacks and armed assaults etc. While the Act will not take force before 2026, a number of EU member-states either support the toughest regime of its application or complete prohibition of such technologies in the national territory, especially in the public space.

Thus, the European Union believes law enforcement and judicial uses of AI should not be regarded just as a technological capability but as a policy decision serving the operational purposes of law enforcement agencies and criminal justice systems.

For example, the European Court of Human Rights has handled in 2017 a claim by two professors of mathematics from the University of Montenegro against the installation of surveillance cameras in auditoriums that they believed to restrict the right to privacy[27]. They have

[25] Established under the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981 // Council of Europe. Available at: URL: https://rm.coe.int/1680078c46 (accessed: 26.11.2024)

[26] Artificial Intelligence Act. Available at: URL: https://www.europarl.europa.eu/RegData/ etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (accessed: 26.11.2024)

[27] European Court of Human Rights judgment of 28.11.2017 on case of Antovic and Mirkovic v. Montenegro. ECHR 1068. Available at: URL: https://hudoc.echr.coe.int/eng#{%22sort%22:[%22kpdate%20Descending%22],%22itemid%22:[%22001-178904%22]} (accessed: 26.11.2024)

argued that surveillance was unlawful while the university administration did not exercise any necessary control of the relevant procedures. In dismissing the claim, the national courts have noted that since video surveillance was in public places (public space), the university administration did not restrict the right to private life. However, the European Court was critical of the arguments brought by national courts.

The European Court has noted that the notion of "private life" in the meaning of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms included "private social life" related to the possibility to develop one's own social identity and relationships with other people. Operation of surveillance cameras in public places without a legitimate basis (purpose) as an exclusive way to achieve a purpose restricted, in the Court's view, the guaranteed right to privacy and violated the relevant provisions of the national law.

Another notable case handled in 2020 by the Court of Appeal (England and Wales) concerned Ed Bridges from Cardiff who challenged the legitimacy of the police use of facial recognition. The appellant was subject to unauthorized remote biometric identification during Christmas shopping in City of Cardiff (2017) and during a lawful protest (2018). In the appellant's opinion, this technology for biometric data analysis which had been arbitrarily tracking hundreds of thousands people without their consent clearly violated their right to freedom of movement in the absence of strict control by public authorities. During hearing of the case, the solicitors noted that the procedure for biometric data retrieval through facial scanning in violation of the British law was analogous to non-consented taking DNA or fingerprints.

The Court held there was no legal basis for using facial recognition cameras including a watch list, qualifying criteria for locations to install such surveillance systems, or secure storage and use of biometric personal data. In the Court's view, the police was to make sure the algorithms of digital facial recognition technology were free of a gender or racial bias. To be fair, it should be noted that the Court observed a balanced restriction of human rights by this technology as its benefits to the appellant outweighed the likely constraints on privacy[28].

[28] The UK recognized the facial recognition technology as unlawful. The system was used by the South Wales police. Available at: URL: https:// metronews-ru.turbopages.org/metronews.ru/s/novosti/world/ reviews/v-velikobritanii-priznali-nezakonnym-ispolzovanie-tehnologii-raspoznavaniya-lic-1700348/ (accessed: 23.10.2024)

Meanwhile, there are over 420 thousand cameras in London alone, of which some are capable of identifying suspicious items and recognize faces of individuals wanted by the police[29].

Thus, the UK regulation allows law enforcement agencies to use smart video surveillance systems installed in public places for remote facial identification while the law and enforcement practices provide an exhaustive list of terms and grounds for legitimate and admissible use of such surveillance[30]. The use of hi-tech systems by public authorities accounts for the position of civil society institutions including private interests of the population.

The San Francisco city council prohibited the facial recognition technology since 14 May 2019 as the public believed that it posed a threat to the fundamental right of local inhabitants to privacy and other inalienable civil freedoms. No CCTV system can be used by the municipal authorities and the police. The system is not for use by the police as the underlying facial recognition algorithms are obviously unreliable and non-transparent. "System errors can result in innocent black people being involved in police investigations where their lives may be at risk", said Matt Cagle, lawyer of the American Civil Liberties Union of North California[31].

As a compromise between systems' deployment and their full prohibition, a moratorium could be introduced during the period of perfecting the technology because it can be of considerable benefit to society in criminal investigations such as searching for missing persons, victims of human trafficking, potential terrorists. Meanwhile, facial identification technologies are widely and unrestrictedly used by private firms, and by the administration of the San Francisco international airport and seaport as facilities subject to the federal jurisdiction[32].

---

[29] Sharafiev I. London boasts un unprecedented number of CCTV cameras. Available at: URL: https://hightech.fm/2019/08/01/cctv. (accessed: 26.11.2024)

[30] Surveillance Camera Code of Practice. Available at: URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1010815/Surveillance_Camera_Code_of_Practice__update_pdf (accessed: 26.11.2024)

[31] San Francisco to become the first American city to ban the facial recognition technology. Available at: URL: https://forbes-ru.turbopages.org/forbes.ru/s/tehnologii/376099-vlasti-san-francisko-zapretili-ispolzovanie-tehnologiy-raspoznavaniya-lic (accessed: 26.11.2024)

[32] Ibid.

A number of large U.S. metropolitan centres have imposed a similar ban on this technology for fear of its unauthorized use, with three states — California, New Hampshire and Oregon passing laws to prohibit the use of facial recognition in body cameras of police officers. In 2020, following the *Black Lives Matter* riots in the United States, IBM, Amazon and Microsoft restricted or suspended sales of facial recognition products.

Under the law of the State of Illinois[33], processing of biometric data should be consented by the individual concerned for the sale, exchange or other profiting from data to be legitimate. The requirements to processing biometric personal data are aimed at ensuring privacy, impartiality and non-discrimination [Kharitonova Yu.S., 2021: 490].

It is noteworthy that 8 out of the top 10 most "watched" cities in the world are in China[34], with CCTV cameras ensuring security of the territory to identify in some cases a misdeed or a person behind it. Once a face is recognized as belonging to the individual on the watch list, the system will signal an outstanding fine, traffic offense, overdue debt or alimony.

The Eyecool smart CCTV system deployed in the majority of airports and railway stations will daily report to the Sky Net mass surveillance system over two million images of suspects.

China's Sky Net national project is a technologically controllable system for comprehensive surveillance of the population using more than 800 million cameras with the facial recognition capability, one per each citizen[35]. Deployed since 2005, the system is not confined to public security: the project is crucial for the anti-corruption system, as well as the Social Credit System that brings together the information from each citizen's trustworthiness digital profile[36].

---

[33] Biometric Information Privacy Act. 740 ILCS 14 // Illinois General Asse mbly. Available at: URL: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (accessed: 26.11.2024)

[34] For comparison, the national surveillance system comprises approximately 50 million cameras in the United States, 5–6 million in the United Kingdom and about 300 thousand in Russia.

[35] How information security is implemented in China. Available at: URL: https://nvo.ng.ru/nvo/2023-01-26/13_1222_security.html?ysclid=m2uiwgandp510405287 (accessed: 26.11.2024)

[36] CCTV with facial recognition to be deployed in Moscow's metro befor e 1 September. Available at: URL: https://www.m24.ru/news/mehr-Moskvy/23012020/104711?utm_source=CopyBuf (accessed: 26.11.2024)

Unlike people in Europe, Chinese nationals perceive the wide deployment of CCTV systems in the national territory quite favorably, with 67 percent approving and nearly 9 percent disapproving the installation of such smart digital systems in China [Kostka G., Steinacker L., Meckel M., 2021: 671–690].

As a result, almost all population of China (over 1.4 billion of human beings) is covered by the facial recognition database.

Digital facial recognition technologies based on access to databases of social media and mobile network operators help the police to identify and penalize traffic violators while also allowing to reduce traffic load, reinforce security and improve the system's performance.

In 2017, the State Council of China developed the New Generation Artificial Intelligence Development Plan[37] that envisages the collection of data and evidence for criminal investigations, and analysis of legal instruments for a smart judicial system.

Under Article 26 of the Personal Information Protection Law of the People's Republic of China (PIPL)[38], that is in force since 1 November 2021, the equipment for image recording or facial recognition will be installed in public places as may be necessary for national and public security in accordance with qualifying criteria to be established. Personal images and identification features may be collected only to serve national security and no other purpose, unless consented by data subjects to serve other needs.

Thus, the whole of biometric data collected through the use of digital video surveillance systems is governed by legal provisions that regulate the requirements to personal data security whereby personal data may be collected only if consented by the data subject exclusively for "legitimate, necessary and specific purposes" [39].

Since 1 August 2021 the Supreme Court of Peoples' Chinese Republic has prohibited private firms from using the outcomes of biomet-

[37] China has missed out on the industrial revolution but will not miss out on the digital one. Available at: URL: https://russiancouncil.ru/analytics-and-comments/analytics/kitay-upustil-promyshlennuyu-revolyutsiyu-ne-propustit-tsifrovuyu/?ysclid=m2uj0etc3c884897317 (accessed: 26.11.2024)

[38] Available at: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021 (accessed: 12.11.2024)

[39] Personal Information Security Specifications, in force since 1 May 2018.

ric video identification, unless consented by the individuals concerned, with the principles of legitimacy, fairness, objectivity and security, protection of state and business secrets, privacy and personal information to be strictly observed for any use of facial recognition technologies[40].

Conclusion

Thus, continuous operation of smart facial recognition systems in the public space serves to record and collect data related, in particular, to private life. This circumstance requires to amend the national law accordingly to define how these data will be processed and to regulate how natural persons will be advised in this respect.

Meanwhile, regulation of social relations associated with the use of smart facial recognition systems should be aimed at striking a balance between private and public interests in retrieving, processing and updating biometric personal data through the use of such digital systems. This calls for a compromise between the observance of human rights and public security requirements based on possibilities to safeguard privacy and on technological conditions behind the use of smart facial recognition systems.

References

1. Andreeva I.O. (2019) Face Recognition Technologies in Criminal Proceedings: Issue of Legal Basis behind the use of Artificial Intelligence. *Vestnik Tomskogo gosudarstvennogo universiteta*=Bulletin of the Tomsk State University, no. 11, p. 12 (in Russ.)

2. Artemova S.T., Zhiltsov N.A. et al. (2020) Digital Divide and Constitutional Guarantees of Digital Equality. *Konstitutsionnoe i munitsipalnoye pravo*=Constitutional and Municipal Law, no. 10, pp. 41–45 (in Russ.)

3. Bobrinskiy N.A. (2021) Moscow's Punitive Innovation: Tentative Results. *Zakon*=Law, no. 6, pp. 89–95 (in Russ.)

4. Gordon B. (2021) Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v. The Chief Constable of South Wales Police. *Potchefstroom Electronic Law Journal*, no. 24, pp. 1–29.

5. Grigoriev V.N. (2021) Information Technologies in Riot Investigation. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta*. *Pravo*=Bulletin of Sankt Petersburg University. Law, no. 2, pp. 334–355 (in Russ.)

[40] China' Supreme Court has prohibited private firms from using facial recognition without consent. Available at: URL: https://3dnews.ru/1045567/verhovniy-sud-kitaya-zapretil-chastnim-kompaniyam-ispolzovat-raspoznavanie-lits-bez-soglasiya-lyudey/ (accessed: 26.11.2024)

6. Huang J. (2020) Applicable Law to Transnational Personal Data: Trends and Dynamics. *German Law Journal*, vol. 21, no. 6. pp. 1283–1308. https: URL: // doi:10.1017/glj.2020.73.

7. Kartashov A.S. (2022) Realization of Constitutional Rights and Freedoms in 'Smart Cities': Main Risks and Ways to Minimize it. In: Constitutional Reform and Legal Development of Ethnic Groups in Russia. Kazan: Buk, pp. 104–111 (in Russ.)

8. Khabrieva T. Ya. (2018) The Law in the Digitalization Conditions. *Zhurnal rossiyskogo prava*=Journal of the Russian Law, no. 1, pp. 85–102 (in Russ.)

9. Kharitonova Y.S., Savina V.S., Pagnini F. (2021) AI Algorithmic Bias: Ethics and Law. *Vestnik Permskogo gosudarstvennogo Universiteta. Jurisprudencia*=Bulletin of the Perm State University. Jurisprudence, no. 3, pp. 488–515 (in Russ.)

10. Kitchin R., Dodge M. (2021) (Un) security of Smart Cities: Risks, Mitigation and Prevention of Negative Consequences. In: City Networks: People. Technologies. Authorities. E. Lapina-Kratasyuk et al. (eds.). Moscow: Novoe Literaturnoe obozrenie, pp. 105–130 (in Russ.)

11. Kostka G., Steinacker L., Meckel M. (2021) Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding* of *Science*. no. 30, pp. 671–690.

12. Maslovskaya T.S. (2019) Digital Sphere and Constitutional Law: Facets of Interaction. *Konstitutsionnoye i munitsipalnoye pravo*=Constitutional and Municipal Law, no. 9, pp. 18–22 (in Russ.)

13. Pashentsev D.A. et al. (2019) Digitizing Law-Making: Search for New Solutions. Moscow: Infotropic, p. 20 (in Russ.)

14. Rassolov I.M., Chubukova S.G. et al. (2020) Biometrics in the Context of Personal Data and Genetic Information: a Legal Dimension. *Russkiy zakon*=Lex Russica, no. 1, pp. 108–118 (in Russ.)

15. Talapina E.V. (2021) Surveillance (Spying) and Human Rights: New Risks in the Digital Age. *Sravnitelnoye konstitutsionnoe obozrenie*=Comparative Constitutional Review, no. 6, pp. 123–136 (in Russ.)

16. Zharova A.K. (2019) Regulating Information Security in the 'Smart Cities'. *Yurist*=Lawyer, no. 12, pp. 69–76 (in Russ.)

17. Zorkin V.D. (2021) Under the Sign of the Fundamental Law. Constitutional Court at the Turn of the Fourth Decade. *Rossiyskaya Gazeta*=Gazette of Russia. 27 October, no. 247 (in Russ.)

Information about the authors:

O.A. Stepanov — Doctor of Sciences (Law), Professor.

D.A. Basangov — Candidate of Sciences (Law), Senior Researcher.

The article was submitted to editorial office 30.05.2025; approved after reviewing 06.06.2025; accepted for publication 06.06.2025.