https://doi.org/10.17816/RJLS46378

Features of the Legal Regulation of the Use of Biometric Personal Data[1]

Petrova Daria,
PhD in Political Science,
Associate Professor
School of Law
Far Eastern Federal University
E-mail: Petrova.dan@dvfu.ru

Martianov Nikita,
3rd year Student
School of Law
Far Eastern Federal University
E-mail: martianov.nr@mail.ru

Abstract. *In this paper, the authors highlight the legal basis for the use of biometric personal data, and also pay attention to the main initiative of the state in this area: the creation of a unified biometric system.*
The study is particularly relevant in connection with the release of the new Federal law No. 168-FZ on June 8, 2020: "On the unified Federal information register containing information about the population of the Russian Federation." In particular, an acute problem is the ability to integrate information from the unified biometric system and the Federal register that is being created.

Keywords: *Unified biometric system, digitalization, legal policy, digitization, personal data, biometric personal data.*

In the modern world, the line between the abstract category of "information" and the real person, the carrier of this information, is blurred. Information about a person, their personal data, has now turned into an expensive product that can be used in different ways:

- by using advertising to sell something directly to the data owner. Currently, contextual advertising technologies based on the processing of Internet user data are widely used;
- by creating a dossier on a person from various sources, reflecting the level of their income, food preferences, frequently-used sites, circle of acquaintances in social networks, etc., and then transferring this information to interested organizations. This practice is engaged in by information brokers or data broker/companies specializing in the collection and sale of personal data;
- by denigrating, exposing the user in a bad light, creating a negative reputation;
- by blackmailing, committing fraudulent and other illegal actions in order to gain profit or benefit[2] [1, c. 45].

Due to the seriousness of the issue, personal data protection can be equated with the protection of a real person, so the state regulates activities related to personal data. To begin with, it is necessary to establish the terminology and define "personal data" as any information related directly or indirectly to a certain identifiable individual (personal data subject) (clause 1, Article 3 of Russian Federal Law 27.07.2006 No. 152-FZ "On Personal Data")[3]. Despite the discussion in scientific circles [2, p. 16], only an individual has personal data.

In accordance with paragraph 5 of the Resolution by the Government of the Russian Federation from 01.11.2012 No. 1119, "On approval of

[1] This work was financially supported by the Russian Federation Presidential Grant No. НШ-2668-2020.6 "National-Cultural and Digital Trends in the Socio-Economic, Political, and Legal Development of the Russian Federation in the 21st Century."

[2] Urmantseva A. Transition to personal: In 2019, twice as much personal data was leaked. Izvestiya iz. URL: https://iz.ru/958561/anna-urmantceva/perekhod-na-lichnoe-v-2019-godu-uteklo-vdvoe-bolshe-personalnykh-dannykh (accessed: 04.02.2020).

[3] Federal Law No. 152-FZ of 27.07.2006 "On Personal Data" // SPS ConsultantPlus. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/ (accessed 05.05.2020).

requirements for personal data protection during processing in personal data information systems," personal data is categorized into:

- special categories of personal data (personal data relating to race, national origin, political opinions, religious or philosophical beliefs, health, and sexual life of the personal data subjects);
- publicly available personal data (personal data obtained only from publicly available sources created in accordance with Article 8 of the Federal Law "On Personal Data");
- biometric personal data;
- other personal data that do not pertain to these categories;
- personal data of the operator's employees, if the information system processes the personal data of only the specified employees.

This article will focus on the legal regime for the use of biometric personal data and the latest developments in legal policy in relation to this issue.

Paragraph 1, Article 11 of Federal Law 27.07.2006 No. 152-FZ "On Personal Data," cited above, establishes the legal definition of biometric personal data. Biometric personal data refers to information that characterizes the physiological and biological characteristics of a person, on the basis of which it is possible to establish their identity.[4]

Based on this definition, biometric personal data can include physiological information (fingerprints, iris, DNA tests, height, weight, etc.), as well as other physiological or biological characteristics. Other records include the image of a person (photo or video), which allows the operator to establish the subject's identity. In addition, according to the explanation of Roskomnadzor,[5] the Federal Service for Supervision of Communications, Information Technology, and Mass Media, the temperature information obtained by the thermal imager also refers to biometric personal data.

In accordance with the above-mentioned Article 11 of the Federal Law "On Personal Data," biometric personal data may be processed only with the written consent of the personal data subject. However, there are exceptions to this rule:

- in connection with the implementation of international treaties of the Russian Federation on readmission;
- in connection with the justice administration and the execution of judicial acts;
- in connection with the mandatory state fingerprint registration;
- in cases stipulated by the legislation of the Russian Federation on defense, security, counterterrorism, transport security, combating corruption, operational and investigative activities, public service, the criminal executive legislation of the Russian Federation, the legislation of the Russian Federation on the procedure for leaving the Russian Federation and entering the Russian Federation, and citizenship of the Russian Federation.

There are two ways to determine whether a photo or video is biometric personal data. The first and simplest pertains to the legislation. Thus, biometric data is recognized as color digital photographic images of the face of the document(s)' owner certifying the identity of that or any Russian citizen leaving or entering the Russian Federation[6]. However, this approach is very narrow and cannot describe the practice of using photographic images.

The second method is to determine the purpose for which the operator processes the data. So, if the photo or video processing is carried out by the operator in order to establish the identity of the personal data subject, in this case, the subject's consent to data processing is mandatory (if it does not fall under the exceptions described above)[7]. That is, until the moment of identification of the personal data subject, a photo or video image is an image, the legal use of which is regulated by Article 152.1 of the Russian Federation Civil Code. From the moment the image is used as an identifier, it is recognized as biometric personal data, the work with which requires mandatory consent in accordance with the Federal Law No. 152 "On Personal Data." Thus, storing photos and photocopies of passports of Russian citizens, if they are not used to establish the identity of a personal data subject (but their processing directly or indirectly follows from the legislation requirements and correlates with the purposes of processing personal data), does not entail legal consequences [3, p. 40].

The use of the image as an identifier is conducted with the help of biometric technologies. Biometric technologies are understood as automatic

[4] Ibid.

[5] Explanations of Roskomnadzor "Features of the use of thermal imagers by employers - operators of personal data-in order to prevent the spread of coronavirus." URL: http://www.consultant.ru/document/cons_doc_LAW_347310/ (accessed: 06.04.2020).

[6] Resolution of the Government of the Russian Federation No. 125 of 04.03.2010 / Official Internet portal of legal information. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102136321 (date of request: 05.05.2020).

[7] Roskomnadzor clarifies the issues of attributing photo, video, and fingerprint data to biometric personal data and the specifics of their processing. URL: https://pd.rkn.gov.ru/press-service/subject1/news2729/ (accessed: 06.07.2020).

or automated methods of recognizing a personality based on their biological characteristics or manifestations. The main components of the biometric method are a scanner for measuring a biometric characteristic and an algorithm that allows it to compare the article with one previously registered as having the same characteristics (a biometric template). There are two possible modes of operating the system verification (comparing one with one) and identification (comparing one with many). With all the theoretical varieties of possible biometric methods (fingerprints, hand geometry, face shape, iris, retina), there are few practical ones among them. There are several basic methods—recognition by fingerprint, by face image (two-dimensional, three-dimensional, or 3D photo), by the eye's iris[8], voice, and veins[9].

In Russia, the beginning of active work with biometric data can be associated with the collection of information about offenders. Fingerprints, for example, are one of the classic evidentiary identifiers in a criminal investigation. Law enforcement agencies, interacting with the suspects, the accused, and the convicted, record the person's height and characteristic signs of appearance. At the same time, it is worth noting that, as mentioned above, in the justice implementation or operational search measures, the subject's consent to the biometric personal data collection is not required.

The real peak of the identification systems use came during the coronavirus pandemic. In Moscow, compliance with security measures was monitored, including with the help of automated facial recognition systems. The city's video surveillance system includes cameras installed in courtyards, in the entrances of residential buildings, in parks, schools, clinics, shops, and construction sites, as well as in the premises of administrative buildings and other public places. With the help of this system, the Moscow police found a considerable number of violators of the two-week self-isolation regime. However, this system cannot guarantee absolute accuracy of the collected information. So, on April 19, 2020, a video surveillance camera recorded the twin brother of a citizen who was on mandatory self-isolation, as a result of which a fine of 4,000 rubles was issued for the citizen who did not violate the mandatory self-isolation[10].

In that regard, Russia is currently creating a Unified Biometric System, a digital platform that is one of the key elements of the mechanism for the person's remote identification by their biometric characteristics. This system is being devised on the initiative of the Communications and Mass Media Ministry of the Russian Federation and the Central Bank of the Russian Federation.

The stated goal of implementing a Unified Biometric System is to increase the availability of services that require legally significant proof of identity. The platform makes it possible to replace a personal visit by receiving a remote service via the Internet. The introduction of a single biometric system will first make financial services and then other digital services more accessible to citizens from remote regions, as well as for people with limited mobility, according to the official website of the Unified Biometric System "Rostelecom"[11].

The possibility of creating a Unified Biometric System led to changes in Federal Law No. 149 from 27.07.2020, "On Information, Information Technologies and Information Protection," Article 14.1 was added to the law, which regulates the creation of a Unified Biometric System. Biometric data can be placed in the system "by state bodies, banks, and other organizations in cases defined by federal laws, after identification is carried out in the personal presence of a Russian citizen with his consent on a free basis..." Thus, firstly, the law is far from being limited to the banking sector, and secondly, any organizations defined by the Government can use biometric data.

Plans for a Unified Biometric System (UBS) have already been announced at an expanded meeting of the Public Chamber Commission of Moscow on Civil Society and Public Control. On July 6, 2020, the Deputy Chairman of the CEC of the Russian Federation, Nikolai Bulaev, mentioned the development of a software and technical complex that will be used by the UBS to confirm voter identities. Bulaev also stressed that the biometric voting system will be conceptually ready by the end of 2020, and it will be possible to use it on the Single voting day in September

[8] Maznichenko N.I. Application areas and principles of building biometric systems of personal identification // Bulletin of the National Technical University Kharkiv Polytechnic Institute. Series: Computer Science and Modeling. 2007.URL: https://cyberleninka.ru/article/n/oblasti-primeneniya-i-printsipy-postroeniya-biometricheskih-sistem-identifikatsii-lichnosti/viewer (accessed: 04.03.2020).

[9] Vihman V.V., Yakimenko A.V. Implementation of biometric identification in access control and management systems. Textbook for universities. Moscow: NSTU Publishing House; 2018. p. 25.

[10] Morozov O. A Moscovite with coronavirus was mistakenly fined for violation of quarantine. The facial recognition system confused him with a healthy twin brother. URL: https://snob.ru/society/moskvicha - s-koronavirusom-po-oshibke-oshtrafovali-za-narushenie-karantina-sistema-raspoznavaniya-lic-pereputala-ego-so-zdorovym-bratom-bliznecom/ (accessed 15.05.2020).

[11] About the unified biometric system. URL: https://bio.rt.ru/faq/project/ (accessed 14.04.2020).

2021, including for the elections to the State Duma of the Russian Federation[12].

Despite the fact that the personal data processing, according to paragraph 1 of Article 14.1, is carried out with the citizen's consent, it is necessary to keep in mind paragraph 16 of the same article. According to the specified point, the UBS operator sends the citizen's biometric data "to The Federal Executive Body Responsible for The Development and Implementation of State Policy and Legal Regulation of Internal Affairs, and to The Federal Executive Body of Security to Ensure the Country's Defense, State Security, Law Enforcement and Counter-Terrorism." Thus, the internal affairs and security agencies have access to the citizens' biometric data and the right to process this data without the citizens' consent.

The above-mentioned fact that the state security agencies will process the citizens' biometric data also correlates with the recently adopted Federal Law No. 168-FZ of June 8, 2020, "On the Unified Federal Information Register containing information about the population of the Russian Federation." The list of information entered in the register (defined in paragraph 2 of Article 7) may be expanded by the bodies authorized to solve tasks in the field of ensuring the security of the Russian Federation in the exercise of their powers (paragraph 15 of Article 8). The full list of bodies that can make changes, as well as the procedure for entering information, is determined by a Presidential Decree and a Government Decree. Thus, we can say that the list of information entered in the register is not exhaustive, which leaves the possibility for entering biometric data.

It is also worth noting that more advanced identification algorithms are used in the UBS development. Two types of biometrics are used together for identification: voice and face. According to Rostelecom, this method is the most effective and convenient at the moment. It will also allow authorities to accurately distinguish between twins, as the biometric algorithms embedded in the system are highly accurate. Thus, it can be noted that the above-mentioned situation, when the camera does not distinguish video recording of the twins, can be repeated with a lower probability.

Great importance in the UBS is given to security. The system recognition accuracy threshold is defined by the Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. 321, dated June 25, 2018[13]. The UBS has a recognition accuracy of 10^{-7}, i.e., it will miss one person in 10 million. At the same time, the system uses an additional link with the login and password from Public Services, so, according to the statement of PJSC Rostelecom, it is almost impossible to deceive the system. Also, to ensure the information security of biometric data of the system users, distributed data storage is implemented: the biometric template is stored in an impersonal form separately from personal data—full name, passport data, SNILS (insurance number of the individual personal account), etc., included in the ESIA databases (Public Services portal).

However, according to Kaspersky Lab, an international company that has been working in the field of information security since 1997, the existing biometric authentication systems have significant generic shortcomings, namely, the problems of their information security. The idea of biometric data as a unique, unadulterated person identifier is inherently wrong and can inspire a false sense of security.

Kaspersky Lab pointed out certain features of processing and storing biometric data, including[14]:

1) the accuracy of their recognition by authentication systems, although relatively high, may still be insufficient for many applications; biometric systems usually have non-zero probabilities of false-negative and false-positive triggering;

2) many of a person's biometric characteristics can be falsified by an attacker, and it may be even easier to copy digitized biometric data than physical ones;

3) once compromised biometric data is compromised forever. The user will not be able to change the stolen fingerprint, as it changes the password if it is stolen; potentially, the person can suffer from this problem for the rest of his life. This problem is quite serious, because along with the development of information technologies, fraud, and theft schemes are also being improved. For example, cases of using neuro-linguistic programming have become more frequent, in which victims independently disclose passwords, data, and other requested information to fraudsters. Biometric keys are not exceptions in this scheme.

[12] Biometrics will be used for online voting in the Russian Federation. URL: https://www.interfax.ru/russia/716074 (accessed: 14.04.2020).

[13] Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. 321 dated 25.06.2018 "On Approval of the procedure for processing, including collection and storage, parameters of biometric personal data for identification purposes..." // Information and Legal Support of <url>.URL: http://base.g.,arant.ru/71985302/ (accessed 22.03.2020).

[14] Kruglov K. Security threats for biometric data processing and storage systems. Kaspersky ICS CERT. URL: https://ics-cert.kaspersky.ru/reports/2019/12/02/biometric-data-processing-and-storage-system-threats (accessed 12.02.2021).

According to Kaspersky Security Network, in the third quarter of 2019, malware was blocked on 37% of the computers performing the functions of collecting, processing, and storing biometric data. Every third computer was at risk of malware infection. Among other malicious objects, Kaspersky Lab products blocked modern Trojans for remote access to the system (5.4% of all computers studied), malware used in phishing attacks (5.1%), ransomware (1.9%), and banking Trojans (1.5%)[15].

Besides external threats, there is an equally dangerous internal threat of forced digitalization, which is opposed by a significant part of the population. The initial transfer of biometric personal data requires the consent of the data owner, but the citizens' consent is not required in the future. At the same time, the data of people who have not committed crimes is transmitted to the internal affairs and state security agencies, as well as to all operators working with a UBS. In our opinion, in this case, there are two serious problems that have already become traditional for Russian digitalization. The first is the lack of a citizen's right to influence the processing of their personal data. In the world, there is a practice of obtaining the prior consent of the national authority for personal data protection to ensure proper protection of personal data [4, p. 100]. The second problem is the lack of a mechanism for removing data from accounting systems at the citizen's request. The lack of dialogue on the solving of these problems will only exacerbate the citizens' distrust of the country's government.

References

1. Savel'ev A.I. Problemy primeneniya zakonodatel'stva o personal'nyh dannyh v epohu «Bol'shih dannyh» (Big Data). *Pravo. Zhurnal Vysshej shkoly ekonomiki*. 2015;(1):224. (In Russ.).
2. Petrykina N.I. Pravovoe regulirovanie oborota personal'nyh dannyh. Teoriya i praktika. Moscow: Statut, 2019. P. 16. (In Russ.).
3. Bryzgin A.A., Minbaleev A.V. Pravovoj rezhim biometricheskih personal'nyh dannyh. *Vestnik URFO. Bezopasnost' v informacionnoj* sfere. 2012;(2):40. (In Russ.).
4. Krivogin M.S. Predposylki formirovaniya special'noj pravovoj zashchity biometricheskih personal'nyh dannyh. *Obshchestvo: politika, ekonomika, pravo*. 2016;(8):100. (In Russ.).

Особенности правового регулирования использования биометрических персональных данных[16]

Петрова Дарья Анатольевна,
кандидат политических наук, доцент
кафедры теории и истории государства и права
Юридической школы
Дальневосточного федерального университета
E-mail: Petrova.dan@dvfu.ru

Мартьянов Никита Русланович,
Студент 3 курса
Юридической школы
Дальневосточного федерального университета
E-mail: martianov.nr@mail.ru

Аннотация. *В настоящей работе авторы освещают правовые основы использования биометрических персональных данных, уделяя особое внимание рассмотрению главной инициативы государства в указанной области — созданию Единой биометрической системы.*

Особенную актуальность исследование приобретает в связи с выходом нового Федерального закона № 168-ФЗ от 8 июня 2020 г. «О едином федеральном информационном регистре, содержащем сведения о населении

[15] Kruglov K. Security threats for biometric data processing and storage systems. URL: https://securelist.ru/biometric-data-processing-and-storage-system-threats/95221/ (accessed: 16.05.2020).

[16] Работа выполнена при финансовой поддержке Гранта Президента РФ № НШ-2668-2020.6 «Национально-культурные и цифровые тренды социально-экономического и политико-правового развития Российской Федерации в XXI веке».

Российской Федерации». В частности, острой проблемой является возможность интеграции сведений Единой биометрической системы и создаваемого федерального регистра.

***Ключевые слова**: Единая биометрическая система, цифровизация, правовая политика, оцифровывание, персональные данные, биометрические персональные данные.*

Список литературы

1. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 224.
2. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. М.: Статут, 2019. С. 16.
3. Брызгин А.А., Минбалеев А.В. Правовой режим биометрических персональных данных // Вестник УРФО. Безопасность в информационной сфере. 2012. № 2. С. 40.
4. Кривогин М.С. Предпосылки формирования специальной правовой защиты биометрических персональных данных // Общество: политика, экономика, право. 2016. № 8. С. 100.