Research article
DOI: https://doi.org/10.21202/jdtl.2023.36

Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models

Dana Utegen ✉

M. Narikbayev KAZGUU University
Astana, Republic of Kazakhstan

Baurzhan Zh. Rakhmetov

M. Narikbayev KAZGUU University
Astana, Republic of Kazakhstan

Keywords

Biometric authentication,
biometric data,
digital technologies,
facial recognition,
technologies,
identification,
law,
legal regulation,
personal data,
privacy,
security

Abstract

Objective: to specify the models of legal regulation in the sphere of biometric identification and authentication with facial recognition technology in order to elaborate recommendations for increasing information security of persons and state-legal protection of their right to privacy.

Methods: risk-oriented approach in law and specific legal methods of cognition, such as comparative-legal analysis and juridical forecasting, are significant for the studied topic and allow comparing the legal regulation models used in foreign countries and their unions in the sphere of biometric identification and authentication with facial recognition systems, forecasting the possible risks for the security of biometric data, taking into account the prospects of further dissemination of the modern facial recognition technology, and to shape recommendations on legal protection of biometric data.

✉ Corresponding author

Results: the ways are proposed to further improve legislation of the Republic of Kazakhstan and other countries currently developing the legal regulation of biometric data, regarding the admissible criteria for using the facial recognition technology, the elaboration of categorization of biometric systems with a high and low risk levels (by the example of the experience of artificial intelligence regulation in the European Union), and the necessity to introduce a system of prohibitions of mass and unselective surveillance of humans with video surveillance systems, etc.

Scientific novelty: consists in identifying a positive advanced foreign experience of developing legal regulation in the sphere of facial recognition based on biometry (European Union, the United States of America, the United Kingdom of Great Britain and Northern Ireland), which can be used for further improvement of the national legislation in order to create more effective mechanisms of legal protection of personal data, including biometric information.

Practical significance: based on risk-oriented approach and comparative analysis, the research allows elaborating measures for enhancing the legal protection of biometric data and ensuring effective protection of civil rights and freedoms by forecasting further expansion of the modern facial recognition technology.

For citation

Utegen, D., Rakhmetov, B. (2023). Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. *Journal of Digital Technologies and Law, 1*(3), 825–844. https://doi.org/10.21202/jdtl.2023.36

Contents

Introduction

Most of the developed countries invest substantial funds into using facial recognition technology. This technology compares and analyzes two or more images of faces, identifies them using biometric data, and determines who the data belong to with

the available bases[1] (Gill, 1997). The biometric data used for facial recognition are stored in the biometric authentication system (Sarabdeen, 2022). The biometric authentication system is an information system that allows identifying a person based on some of their main physiological and behavioral characteristics[2]. The examples of biometric indicators are fingerprints, face, iris, palmprint, retina, hand geometry, voice, signature, and gait[3]. It is based on hardware systems of data collection, integrating software components which use mathematical algorithms to analyze data and identify a personality[4].

Considering various groups of legal relations in law-application and enforcement activity of executive authorities, chosen in this research for comparative analysis of the states, the implementation of which may use facial recognition technologies, one should distinguish the following objects, referred to vulnerable ones:

1) objects vulnerable in terms of terrorism;
2) critical state objects;
3) strategic objects of economic sectors having strategic significance;
4) hazardous industrial objects;
5) objects of mass gathering of people, etc.

Facial recognition technology is most often used by law enforcement bodies to identify people suspected in committing crimes. Analysis and identification takes places by obtaining photos, videos, driving licenses, public surveillance videos, photos from social networks, etc.[5]. Although facial recognition systems are used, in particular, for law and order protection and public safety provision, citizens are often surveyed without knowing about that, as there is no notification about surveillance. The use of facial recognition systems by law enforcement was criticized as biased, discriminating and lacking transparency.

International community generally supports the initiative of providing safety using digital technologies. According to the Resolution of the UNO Security Council, the member

---

1 Everything about facial recognition technology. *Www.cloudav.ru*. https://www.cloudav.ru/mediacenter/technology/facial-recognition-technology/ ; TAdviser – a portal for choosing technologies and suppliers. (2020). *TAdviser.ru*. https://www.tadviser.ru/index.php/

2 QUII. (2018). Biometric Recognition: definition, challenge and opportunities of biometric recognition systems. *IQUII*. https://medium.com/iquii/biometric-recognition-definition-challenge-and-opportunities-of-biometric-recognition-systems-d063c7b58209

3 Jain, A. (2008). Biometric authentication. *Scholarpedia*, 3(6), 3716. https://doi.org/10.4249/scholarpedia.3716

4 *Ibid*, *2*.

5 Resolutions of UNO Security Council S/RES/2396(2017). https://www.un.org/securitycouncil/ru/content/sres23962017

states call for active measures to combat terrorism threats and to prevent crime[6]. Due to the increased practice of fraud, falsification and forgery of personality identification documents, the recommendations of the UNO body in charge of global peace and safety referred to introducing systems of biometric data identification with a view of surveillance of terrorists or persons suspected in terrorist activity[7].

Besides ensuring safety, one should also mark the impact of the COVID-19 pandemic, which enhanced the use of facial recognition systems in struggling against the infection dissemination and controlling citizens' movement during the quarantine restrictions. The algorithms of facial recognition systems were used to control citizens' movements and wearing masks, checking body temperature in order to administer the measures of public healthcare provision (Chen & Wang, 2023; Johnson et al., 2022; Shore, 2022).

In this regard, of interest is the experience of legal regulation in the countries currently actively applying a system of biometric databases, aimed at simplifying the criminal investigation procedures and control over movement at borders.

1. United States of America: introduction and regulation of facial recognition technology

By the example of the United States of America, one should mark the practice of using surveillance cameras with facial recognition function in the context of antiterrorist measures after September 11, 2001. Based on the Border Security Act adopted by the US Congress, biometric identity documents were introduced[8]. Since 2004, the country introduced a system of taking fingerprints and including into a database of the images of people coming to the US. Checking biometric data with governmental databases is aimed at revealing the persons suspected in terrorism, wanted criminals or those previously violating the US immigration legislation. Thus, in less than half a year, a biometric database of over five million people was collected. Besides, the US security bodies took measures in relation to 3,800 foreigners based on the information obtained during biometric screening when visiting the USA[9]. The measures included detention of the suspects based on a warrant, refusal of acceptance at the border, or deportation to the country of last residence.

---

6 *Ibid*.

7 Resolution 2396 (2017), adopted by the Security Council on its 8148th session on December 21, 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/27/PDF/N1746027.pdf?OpenElement

8 Markey, E. J. (2021, June 15). Text: S.2052 – 117th Congress (2021–2022): Facial Recognition and Biometric Technology Moratorium Act of 2021. https://www.congress.gov/bill/117th-congress/senate-bill/2052/text

9 Federal Register, Vol. 73, Iss. 245. (2008, December 19). https://www.govinfo.gov/content/pkg/FR-2008-12-19/html/E8-30095.htm

However, the tragic events of the 2001 terrorist attack did not cause but just facilitated the development of the previously existing fingerprints identification system.

In the US and other developed countries, facial recognition and facial expression analysis systems started to be developed in the 1960–1970-s in research laboratories funded by the Ministry of Defense and intelligence services. In 1990, new companies were created to commercialize the technology, which searched for target markets, in particular, among the institutions using their own computer networks, such as financial industry, business, large scale identification systems, passport services, public departments, law enforcement and penitentiary systems (Schweber, 2014). In 1999, he US Federal Bureau of Investigations developed and introduced an automated fingerprints identification system. This system combines records of fingerprints collected by federal law enforcement. It provides opportunities for automated search for fingerprints, electronic storage and exchange of images. In 2008, the system processes on average over 63,000 fingerprints a day, 91% of which scanned into the system in a digital form and the rest stored on a paper carrier[10].

In the recent years, the US practice accumulated a sufficient number of cases associated with the procedures of processing, storage and use of biometric data (Stepney, 2019). In this regard, it seems most important to study and analyze individual solutions in this category of issues, with a view of improving the legislation of the Republic of Kazakhstan.

In 2021, a case of Robert Williams was heard in the USA. The black man was arrested in 2020 for stealing watches from a shop in Detroit, Michigan. Although he had not visited that shop for several years, he was detained in the presence of his two daughters as a suspect of theft. The Detroit police department used facial recognition technology to identify a suspect by surveillance camera images. Thus, they used a database of driving licenses photos of the Michigan police department. However, facial identification appeared to be false, hence, an innocent person was kept in custody for 30 hours[11].

Unfortunately, this case is not the only one – the practice of holding innocent persons liable became frequent (Bowyer, 2004). In connection with the application of facial recognition technology, a research was carried out by the National Institute of Standards and Technology[12]. It showed that color bar takes place most often during facial

[10] FIRS IAFIS (Federal Bureau of Investigation). https://www.fbi.gov/how-we-can-help-you/need-an-fbi-service-or-more-information/freedom-of-informationprivacy-act/department-of-justice-fbi-privacy-impact-assessments/firs-iafis

[11] Harwell, D. (2021, April 13). Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match. *Washington Post*. https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/

[12] NIST (National Institute of Standards and Technology) (2000). https://www.nist.gov/

identification. Also, the facial recognition technology was widely used by law enforcement for identification of persons during meetings and demonstrations, investigations of misdemeanors, and arrests without any evidences of guilt (Buresh, 2021). As a result, the number of people who became victims of the unregulated surveillance and monitoring system is constantly growing[13].

After a number of consequences of faults of facial identification, the US civil society and international non-government organizations formed petitions calling for a mass prohibition of biometric recognition technologies allowing mass and discriminating surveillance[14]. Some of the American states initiated a Moratorium on the use of facial recognition technology. Later, a bill on facial recognition was proposed in the US, which restricts the application of this technology and its unethical use[15]. This document contains a list of restrictions of facial recognition technology application, including:

– immigration control,

– peaceful protests,

– establishing a personality of a criminal suspect.

According to the bill, law enforcement bodies are required to test the facial recognition system and submit annual reports on the efficiency of their implementation. One of the important criteria is deleting from the databases the images of minors, acquitted or released without charge[16].

Although most of the states initiated introduction and regulation of the facial recognition technology, one should highlight the experience of California, which became the first US state to ban the use of facial recognition technology by law enforcement. Later, this practice influenced the ban on using facial recognition technology not only by law enforcement, but also for private organizations[17].

---

13 Rauenzahn, B., Chung, J., & Kaufman, A. (2021, March 20). Facing Bias in Facial Recognition Technology. *The Regulatory Review*. https://www.theregreview.org/2021/03/20/saturday-seminar-facing-bias-in-facial-recognition-technology/#:~:text=According%20to%20the%20researchers%2C%20facial

14 The Computer Got It Wrong: Why We're Taking the Detroit Police to Court over a Faulty Face Recognition "Match". (2021, April 13). *American Civil Liberties Union*. https://www.aclu.org/news/privacy-technology/the-computer-got-it-wrong-why-were-taking-the-detroit-police-to-court-over-a-faulty-face-recognition-match

15 Paul, K. (2019, May 15). San Francisco Is First US City to Ban Police Use of Facial Recognition Tech. *The Guardian*. https://www.theguardian.com/us-news/2019/may/14/san-francisco-facial-recognition-police-ban

16 Ban Biometric Surveillance. *Access Now*. https://www.accessnow.org/ban-biometric-surveillance/

17 California Law Enforcement Prohibited from Using Facial Recognition Technology in Body Cameras under Ting Bill Signed by the Governor. Assemblymember Phil Ting Representing the 19th California Assembly District. https://a19.asmdc.org/press-releases/20191008-california-law-enforcement-prohibited-using-facial-recognition-technology

Following the example of California, there were established the grounds in terms of providing a search warrant and a requirement to present sufficient evidences of committing a crime. Besides, restrictive measures referred to using the facial recognition technology during protests and meetings in order to prevent violation of civil rights and freedoms. The bill was widely supported by international non-government organizations controlling the government activity, civil freedoms groups and the law enforcement[18]. Large companies like IBM, Amazon and Microsoft especially supported the decision on suspending selling facial recognition tools to governments[19].

As a result, the adopted act on facial recognition prohibits coincidence to be single evidence establishing sufficient grounds for arrest, this being the most adequate protection measure to prevent mistakes in an indictment order (Gates, 2002).

Illinois also adopted a law on regulating facial recognition systems, namely, Biometric Information Privacy Act[20] (Zuo et al., 2019). It stipulates prohibitions on exchange, transfer without consent, trading or deriving profit from selling biometric data[21] (Hill et al., 2022).

Based on the analysis of various US states, one may notice a certain fragmentation of approaches. While not all states restricted the use of surveillance cameras with the facial recognition function, most of the states have adopted laws restricting the use of such cameras by law enforcement[22]. Not all US citizens and foreigners residing in the US may reckon on safety in case of faults in identification. The bill provides just a basic protection for the Americans, allowing the civil society to promote initiatives on limiting the uncontrolled use of such systems.

According to the drafters, the formulated approach to restricting the use of facial recognition function and regulating collection and processing of data will allow reducing the

---

18 Use of facial recognition systems by police will be restricted in the US. (2022, September 30). *ForkLog*. https://forklog.com/news/v-ssha-ogranichat-ispolzovanie-politsiej-sistem-raspoznavaniya-lits

19 Muravyev, D. (2020, June 19). Why IT companies rejected the facial recognition technology and what this has to do with protests in America. *Teplitsa sotsialnykh tekhnologiy*. https://te-st.ru/2020/06/19/why-it-companies-against-facial-recognition/

20 740 ILCS 14/ Biometric Information Privacy Act. *Www.ilga.gov*. www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

21 Deadline for filing a lawsuit in a multimillion-dollar settlement with Snapchat is approaching. (2022, October 13). *Chicago24online*. https://chicago24online.com/news/priblizhaetsya-krajnij-srok-podachi-iska-v-mnogomillionnom-uregulirovanii-processa-so-snapchat/ ; Thornley v. Clearview AI, Inc., No. 20-3249 (7th Cir. 2021). *Justia Law*. https://law.justia.com/cases/federal/appellate-courts/ca7/20-3249/20-3249-2021-01-14.html

22 Face Off: Law Enforcement Use of Face Recognition Technology. (2018, February 23). *Electronic Frontier Foundation*. https://www.eff.org/wp/law-enforcement-use-face-recognition

probability of abuse caused by discriminative monitoring and ensuring measures for privacy protection[23].

Thus, one may conclude that facial recognition and surveillance technologies allow faults and enhance discrimination, especially when police continue to make decisions on arrests and detention without additional means of crime investigation (Givens et al., 2004). If restriction measures are taken, the facial recognition system will be used only for necessary and justified purposes, and will restrict the broad discretion powers of the law enforcement (Nissenbaum, 2004). Besides, it will enhance the right to delete one's information in case of an acquitting judgment. The legislator's initiative on restricting the facial recognition system is also due to the privacy protection, preventing bias and discrimination of citizens by color and race.

2. European Union: risk-oriented approach in legal regulation

Regarding the practice of the European Union (further – EU), one should pay attention to adoption of the legislation restricting the use of facial recognition systems in real time. Beside misuse by law enforcement, detaining citizens without due reasons, it was found that the artificial intelligence and facial recognition tools can be used for surveillance of migrants, religious groups and minorities[24]. The established position of the members of European Parliament associates the surveillance methods with threats to privacy and civil freedoms, and considers them to be enhancing bias and discrimination.

A prerequisite to taking restrictive measures is the vast practice of using automated facial recognition technology by police for searching people in public places. These technologies used in street surveillance cameras to ensure public safety caused uproar of civil society activists, who demanded accounts of actual facts of crime prevention with the help of surveillance (Kuteynikov et al., 2022). In their protests, the human rights community emphasized the freedom of speech and the right to peaceful assembly, which are the essential civil freedoms. It was highlighted that the use of facial recognition system by the government hinders expression of opinions, harms entire communities and violates individual freedoms[25].

---

23 Turner, N. L, & Chin, C. (2022, April 7). Police Surveillance and Facial Recognition: Why Data Privacy Is an Imperative for Communities of Color. *Brookings*. https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

24 Review of ECHR decisions as of September, 2018 (2018, September 14). Assistance to those wishing to apply to the European Court of Human Rights in Strasburg. https://european-court-help.ru/obzor-reshenii-espch-za-sentiabr-2018-goda/ ; Face off Report. (2018). *Big Brother Watch*. bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/report/

25 Guariglia, Paige Collings, & Matthew. (2022, September 26). Ban Government Use of Face Recognition in the UK. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2022/09/ban-government-use-face-recognition-uk

A remarkable case heard by a high court in Cardiff was a suit by Ed Bridges supported by a Liberty civil rights group. Bridges claimed that the use of facial recognition technology by police when he was shopping and later during a peaceful protest against weapon sales violates his right to privacy and peaceful protests.

The high court in Cardiff stated that, although the mass surveillance system violates the right to privacy of those scanned by surveillance cameras, automatic facial recognition was performed on legal grounds[26] (Begishev & Khisamova, 2018).

In 2022, the legislative initiatives in Great Britain, regarding the restriction of facial recognition systems were reviewed[27]. According to the Data Protection Act of 2018, biometric and medical data are sensitive data; hence, their collection and processing can be performed only after obtaining an explicit consent[28]. Information Commissioner's Office in Great Britain also informed about an investigation in relation to the organizations introducing the facial recognition systems which carry the risk of using emotion analysis algorithm.

Emotion analysis technologies process such data as glance tracing, mood analysis, facial movements, analysis of pace, heartbeat, facial expression[29] (Begishev & Khisamova, 2018).

Emotion analysis implies collection, storage and processing of a range of personal data, including subconscious behavioral or emotional reactions. Such use of data is much more risky than traditional biometric technologies used for facial identification (Sprokkereef, 2007).

The emerging problems of applying identification systems influences the thorough analysis of legal regulation of authentication systems in the European Union. In April 2021, the European Data Protection Supervisor, having analyzed the current risks and concerns about the use of systems with facial recognition function, called for banning the use of artificial intelligence for automatic identification of persons in public places. Similarly, in January 2021, the Council of Europe called for strict regulation of technologies and marked in its new guidelines that facial recognition must be prohibited if they are used exclusively for determining the skin color, religious or other convictions, gender, racial

---

26 Bowcott, O. (2019, September 4). Police Use of Facial Recognition Is Legal, Cardiff High Court Rules. *The Guardian*. https://www.theguardian.com/technology/2019/sep/04/police-use-of-facial-recognition-is-legal-cardiff-high-court-rules

27 Kaminskiy, B. (2022, July 27). Britain attempted to ban facial recognition in shops. *ForkLog*. https://forklog.com/news/v-britanii-potrebovali-zapretit-raspoznavanie-lits-v-magazinah

28 Data Protection Act 2018. (2018). *Legislation.gov.uk*. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

29 "Immature Biometric Technologies Could Be Discriminating against People" says ICO in Warning to Organisations. (2022, October 27). *Ico.org.uk*. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations/

or ethnic origin, age, state of health or social status of a person. Civil rights groups also urged the EU to ban biometric surveillance on the grounds of incompliance with human rights[30].

The European Commission included into the EC act on artificial intelligence restrictions on using the facial recognition system in public places and for private companies, but left the opportunity of police using it for exclusive purposes. The security agencies may use this technology in such cases as searching for missing children, preventing terrorist attacks and identification of armed and dangerous criminals.

The draft EU act on artificial intelligence presented in April 2021 is aimed at restricting the use of biometric identification systems, including facial recognition technology. Within the project, it is proposed to introduce new requirements regulating the use of technology depending on the criteria – "high" or "low" risk[31].

High risk artificial intelligence systems will include:

– critically important objects which may inflict harm to life and health of citizens;

– biometric identification and categorization of physical persons;

– education and vocational training (for example, calculating scores at exams);

– components of product safety (for example, using artificial intelligence in robotized surgery);

– employment, personnel management and access to self- employment (for example, software for sorting CVs at admission);

– access to the key private and public services and benefits (scoring crediting system, which limits the ability of citizens to obtain credit);

– data of law enforcement;

– data of migration and border forces (verifying the passing documents);

– data of the institutions of justice and democratic procedures (applying of law to a specific set of evidences)[32].

High risk systems will be prohibited for purposeless use or will have to comply with the strict rules of supervisory bodies, and used in serious cases for safety provision. A wide range of facial recognition technologies, used for law enforcement purposes, during border control, in public places, educational establishments, public transport, can be allowed only on the condition of assessing the compliance and observance of safety requirements (Sprokkereef, 2007). The low risk facial recognition technologies will be

30 *Ibid*, 20.

31 Kasparyants, D. (2021, October 7). Standardization of artificial intelligence in the EU. *"GRChTs" scientific-technical center.* https://rdc.grfc.ru/2021/10/ai-standards/

32 Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. (2021, April 21). *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

restricted to the criteria of transparency and requirements to the rules of information storing and processing[33].

Regardless of the proposed projects of artificial intelligence regulation, there are still serious concerns in Europe about using such categorization and regulation without due public control. Most of the EU member states still advocate for stricter rules, including complete prohibition of such technologies. In particular, the system of remote biometric identification and the facial recognition technology are referred to high risk systems (Firc, 2023). One of the main requirements is complete prohibition of their use in public places for law enforcement purposes.

3. Republic of Kazakhstan: on the way to regulating biometric data

Republic of Kazakhstan faces the trend towards using the foreign experience in biometric authentication in various spheres, such as state governance, banking, medicine, law enforcement, education, etc.

A number of amendments were introduced into the current legislation[34], including a definition of biometric data; the rules of processing and storing biometric data when rendering state services were adopted. The provisions of these rules stipulate the procedures of biometric data processing when rendering state services; such data are submitted voluntary and can be at any time deleted from databases upon a written application of the data subject[35].

In compliance with the Law "On personal data and their protection", the notion of biometric data is defined as a category of personal data characterizing physiological and biological features of the subject, based on which his or her personality may be identified[36].

The definition establishes the belonging of biometric data to personal data, while the process of biometric data identification is qualified as "biometric authentication". According to the Law on informatization, biometric authentication is defined as

---

33 Filipova, I. A. (2022). *Legal regulation of artificial intelligence: tutorial* (2nd ed., renewed and complemented). Nizhniy Novgorod: Nizhniy Novgorod State University. https://www.researchgate.net/publication/359194516_Legal_Regulation_of_Artificial_Intelligence/citation/download ; Madiega, T., & Mildebrath, H. (2021, September). *In-Depth Analysis*. https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

34 On personal data and their protection. *Adilet IPS*. https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm

35 Rules of collection, processing and storage of biometric data of physical persons for their biometric authentication when rendering state services. *Adilet IPS*. https://adilet.zan.kz/rus/docs/V2000021547#z14

36 *Ibid*., 22.

a complex of measures, identifying a personality based on physiological and biological unchangeable features[37].

Besides the said definitions, Republic of Kazakhstan has adopted the Law on dactyloscopic and genome registration. The goals of the Law are determined by the requirements of obligatory collection of fingerprints to create a common database of biometric data. The database of fingerprints will be used during border control, for anti-terrorism measures, criminal investigations, order and safety provision[38].

As for data processing, in 2022 the Program of developing a national payment system in the Republic of Kazakhstan up to 2025 was adopted[39]. The Program stipulates the introduction of biometric authentication during payment operations; as part of the initiative of its implementation, it is stated that it is aimed at increasing the personal data security through introducing a mechanism of the subjects' consent for data processing. As a result, a subject must be aware of the procedure of their application for a state service, the goal of their application, and have an opportunity to give or withdraw consent for access to their data[40].

Besides the procedures of common use of biometric data, the Program of Almaty development up to 2025 and 2030 establishes installing of surveillance cameras with facial recognition function[41]. In 2027, it is planned to broaden surveillance systems by installing cameras on all terrorist-vulnerable objects and in residential quarters[42]. The topicality of installing surveillance cameras increased after mass unrest which took place in January 2022, when in several large cities of Kazakhstan, especially in Almaty, law enforcement and security bodies failed to control mass unrest, looting and public order offenses[43].

Initiatives on installing surveillance cameras with facial recognition function were stipulated by a law draft on digital technologies regulation, according to which, amendments

---

37 Law of the Republic of Kazakhstan No. 418-V of November 24, 2015 "On informatization" (with amendments as of 03.09.2022). *PARAGRAF Information system*. https://online.zakon.kz/document/?doc_id=33885902

38 Raisova, Z. (2021, January 6). Obligatory dactyloscopy of Kazakhstaners: what is it for and how does it work? *CABAR.asia*. https://cabar.asia/ru/zachem-vvoditsya-obyazatelnaya-daktiloskopiya-kazahstantsev

39 On adopting the National development plan of the Republic of Kazakhstan up to 2025 and recognizing invalid certain orders of the President of the Republic of Kazakhstan: Order of the President of the Republic of Kazakhstan No. 636 of February 15, 2018. *Adilet IPS*. https://adilet.zan.kz/rus/docs/U1800000636

40 On adopting the Program for creating the National platform of digital biometric identification for 2021–2024 (2021). *Otkrytye NPA*. https://legalacts.egov.kz/npa/view?id=13895562

41 *Program of Almaty development up to 2030 is socially oriented*. (2022, June 28). https://www.gov.kz/memleket/entities/almaty/press/news/details/394216?lang=ru

42 Alkhabaev, Sh. (2022, September 12). Facial recognition system will be introduced in Almaty. *Tengrinews.kz*. https://tengrinews.kz/kazakhstan_news/sistemu-raspoznavaniya-lits-vnedryat-v-almatyi-477602

43 Kazakhstan: victims of January protest do not find justice. (2022, May 9). *Human Rights Watch*. https://www.hrw.org/ru/news/2022/05/09/kazakhstan-no-justice-january-protest-victims

were made in the current Law on informatization[44]. To ensure national safety and public order, it is planned to introduce a national system of video monitoring as a complex of hardware and software means for collection, processing and storage of video images database[45].

At the same time, the analyzed documents and normative legal acts, referring to personal data protection in the Republic of Kazakhstan, are currently only partially comply with the international standards of human rights protection. Besides, the presence of laws does not provide a substantial guarantee of their protection. Special attention should be paid to the rules of collection, processing and storage of biometric data [46].

Using the cameras with facial recognition function and citizens' collecting fingerprints may allow privacy violation. That is why, for legal regulation of biometric data it is necessary to thoroughly study the international experience of the states which already implement the practice of biometric data collection, in order to avoid the risks associated with personal data leakage (Raissova & Mukhamejanova, 2021).

In the law enforcement practice, it is recommended that biometric data processing complies with the established techniques of using the facial recognition technology in law enforcement and law application activity, which exclude or significantly reduce the possibility to violate privacy, human rights and freedoms:

The use of facial recognition system must comply with the legal goals and be reasonably necessary.

The use of facial recognition system must be open and transparent, which implies reporting to citizens in the form of statistical data and disclosing materials on crime solving using the facial recognition technology.

Possibility to apply to authorized bodies in case of claims and to obtain the information of interest.

The presence of clear rules, policies and procedures for security of biometric data and means of their processing.

Observing the rules of minimization of biometric data collection.

Restriction of access of the third persons not involved into data processing and surveillance.

Compliance with the requirements of laws and safety measures for protection against unsanctioned access and use of biometric data.

Regular implementation of scheduled and unscheduled inspections to provide the quality of biometric data protection and exclude their illegal use or granting access to them.

---

44 On the draft Law of the Republic of Kazakhstan "On making amendments in certain legislative acts of the Republic of Kazakhstan on the issues of digital technologies regulation": Decree of the Government of the Republic of Kazakhstan No. 1001 of 28.12.2019. *Adilet IPS*. https://adilet.zan.kz/rus/docs/P1900001001

45 On adopting the Rules of functioning the National video monitoring system. *Adilet IPS*. https://adilet.zan.kz/rus/docs/V2000021693

46 Research of the probable economic, social and legal consequences of the Law of the Republic of Kazakhstan "On dactyloscopic and genome registration" (2021, June 23). *Soros Kazakhstan Foundation*. www.soros.kz/ru/study-of-the-law-of-the-republic-of-kazakhstan-on-fingerprint-and-genomic-registration/

Conclusion

This research describes the experience of using facial recognition technologies and biometric identification as a tool to ensure safety. Description of state restrictions allowed formulating the approaches to the legal regulation of the sphere under study, the advantages and risks of their implementation.

To prevent any violations of privacy, discrimination, limitation of rights and freedoms by the government or private organizations, it is necessary, based on the carried out analysis of the experience of the states which have implemented national projects on biometric data regulation, to identify the guarantees and increase the level of state-legal protection. Analysis of the experience of the states showed that adoption of the respective laws, regulating the biometric data protection, is inevitable, as the current legislation does not fully comply with the criteria of the safe use of facial recognition technology by governmental and private organizations.

As a result of the carried out analysis and the studied experience of foreign states, one may highlight the following important proposals to further improve legislation in the Republic of Kazakhstan:

– to complement the current legislation in terms of defining the admissible criteria of using facial recognition technology;

– to introduce a prohibition of mass and unselective surveillance using video surveillance systems;

– to ban the use of images of the citizens of the Republic of Kazakhstan, taken from publicly accessible sources, to complete databases of biometric data;

– to elaborate categorization of biometric systems with high and low risk level by the example of artificial intelligence regulation in the European Union;

– to introduce a prohibition of using the biometric identification system in real time by all users except law enforcement.

Based on the studied experience of the European Union and the US, the said proposals may be taken into account both in the Republic of Kazakhstan and in other countries, which are currently developing biometric data and their legal regulation. When using facial recognition systems, state bodies must promote the implementation of the principles of transparency, legitimacy and necessity, as well as to formulate the policy of the third persons' data processing.

References

Begishev, I. R., & Khisamova, Z. I. (2018). Criminological risks of using artificial intelligence. *Russian Journal of Criminology*, *12*(6), 767–775. (In Russ.). https://doi.org/10.17150/2500-4255.2018.12(6).767-775

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19. https://doi.org/10.1109/mtas.2004.1273467

Buresh, D. L. (2021). Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws? *Santa Clara High Technology Law Journal*, *38*(1). https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, *47*(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, *9*(4), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Gates, K. A. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media*, *3*(2), 235–238. https://doi.org/10.1177/152747640200300217

Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura: Feminism, Culture, and Media Studies*, *14*(1–2), 161–179. https://doi.org/10.1215/02705346-14-1-2_40-41-161

Givens, G., Beveridge, J. R., Draper, B. A., Grother, P., & Phillips, P. J. (2004). How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2004. https://doi.org/10.1109/cvpr.2004.1315189

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, *24*(3), 325–335. https://doi.org/10.1177/14613557221089558

Johnson, Th. L., Johnson, N. N., McCurdy, D., & Olajide, M. M. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, *39*(4), 101753. https://doi.org/10.1016/j.giq.2022.101753

Jones, C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *NCJL & Tech.*, *22*(4), 777. https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6

Kuteynikov, D. L., Izhaev, O. A., Lebedev, V. A., & Zenin, S. S. (2022). Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification. *Lex Russica*, *75*(2), 121–131. (In Russ.). https://doi.org/10.17803/1729-5920.2022.183.2.121-131

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Raissova, G., & Mukhamejanova, D. (2021). Nondiscrimination Policy and Privacy Protection in Case of Genetic Passport for Soldiers. *South Asian Journal of Social Sciences and Humanities*, *2*(3), 140–150. https://doi.org/10.48165/sajssh.2021.2309

Sarabdeen, J. (2022, March 11). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, *8*(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

Schweber, H. (2014). Lochner v. New York and the Challenge of Legal Historiography. *Law & Social Inquiry*, *39*(1), 242–274. https://doi.org/10.1111/lsi.12062

Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, *70*, 101815. https://doi.org/10.1016/j.tele.2022.101815

Sprokkereef, A. (2007, August). Data Protection and the Use of Biometric Data in the EU. In *The Future of Identity in the Information Society* (pp. 277–284). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-79026-8_19

Stepney, Ch. (2019). Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law. *Loyola of Los Angeles Entertainment Law Review*, *40*(1). https://digitalcommons.lmu.edu/elr/vol40/iss1/2

Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial Recognition Technology: A Primer for Plastic Surgeons. *Plastic and Reconstructive Surgery*, *143*(6), 1298e–1306e. https://doi.org/10.1097/prs.0000000000005673

Authors information

Dana Utegen – Deputy Director, Senior Lecturer of KAZGUU Law School, KAZGUU University Astana
Address: 8 Korgalzhinskoye shosse, 010000 Astana, Republic of Kazakhstan
E-mail: d_utegen@kazguu.kz
ORCID ID: https://orcid.org/0000-0001-5296-7916

Baurzhan Zh. Rakhmetov – PhD in Politics and International Relations, Assistant Professor of International School of Economics, KAZGUU University Astana
Address: 8 Korgalzhinskoye shosse, 010000 Astana, Republic of Kazakhstan
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ

Authors' contributions

Dana Utegen made the manuscript draft and critically reviewed it, inserting valuable comments of intellectual contentя; developed the methodology design; performed comparative analysis; collected literature; analyzed legislation of the United States of America and the Republic of Kazakhstan; prepared and edited the manuscript; formulated the key conclusions, proposals and recommendations; formatted the manuscript.
Baurzhan Zh. Rakhmetov formulated the research idea, goals and tasks; participated in research design; analyzed and summarized literature; analyzed legislation of the European Union and the Republic of Kazakhstan; interpreted the specific research results; critically reviewed and edited the manuscript; interpreted the general research results; approved the final version of the article.

Conflict of interest

Rakhmetov B. Zh. is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – November 7, 2023
Date of approval – April 23, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:342.721:004:004.8
EDN: https://elibrary.ru/drgddj
DOI: https://doi.org/10.21202/jdtl.2023.36

Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования

Дана Утеген ✉

Университет КАЗГЮУ имени М. С. Нарикбаева
г. Астана, Республика Казахстан

Бауржан Жанатович Рахметов

Университет КАЗГЮУ имени М. С. Нарикбаева
г. Астана, Республика Казахстан

Ключевые слова

Безопасность,
биометрическая аутентификация,
биометрические данные,
идентификация,
неприкосновенность частной жизни,
персональные данные,
право,
правовое регулирование,
технологии распознавания лиц,
цифровые технологии

Аннотация

Цель: выявление моделей правового регулирования в сфере биометрической идентификации и аутентификации технологией распознавания физических лиц для выработки рекомендаций по повышению информационной безопасности человека и государственно-правовой охраны его права на неприкосновенность частной жизни.

Методы: рискориентированный подход в праве и такие специально-юридические методы познания, как методы сравнительно-правового анализа и юридического прогнозирования, имеют для исследуемой проблематики определяющее значение и позволяют сопоставить применяемые в зарубежных странах и их объединениях модели правового регулирования в сфере биометрической идентификации и аутентификации системами распознавания физических лиц, спрогнозировать возможные риски для безопасности биометрических данных с учетом перспективы дальнейшего распространения современной технологии распознавания лиц, сформулировать рекомендации по правовой охране биометрических данных.

✉ Контактное лицо

Результаты: предложены пути дальнейшего совершенствования законодательства Республики Казахстан и иных стран, находящихся в процессе развития правового регулирования биометрических данных, в части определения допустимых критериев использования технологии распознавания лиц, разработки категоризации биометрических систем с высоким и низким уровнем риска (по примеру опыта регулирования искусственного интеллекта в Европейском союзе), необходимости введения системы запретов массовой и неизбирательной слежки за человеком с помощью систем видеонаблюдения и др.

Научная новизна: заключается в выявлении положительного зарубежного передового опыта по развитию правового регулирования в сфере распознавания физических лиц на основе биометрии (Европейский союз, Соединенные Штаты Америки, Соединенное Королевство Великобритании, Северная Ирландия), который может быть использован для дальнейшего совершенствования национального законодательства в целях создания наиболее эффективных механизмов правовой защиты персональных данных, включая биометрическую информацию.

Практическая значимость: основанное на рискориентированном подходе и компаративистском анализе исследование позволяет выработать меры по усилению правовой охраны биометрических данных, обеспечению эффективной защиты гражданских прав и свобод на неприкосновенность частной жизни на основе прогноза дальнейшего распространения современной технологии распознавания лиц.

Для цитирования

Утеген, Д., Рахметов, Б. Ж. (2023). Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования. *Journal of Digital Technologies and Law*, *1*(3), 825–844. https://doi.org/10.21202/jdtl.2023.36

Список литературы

Бегишев, И. Р., Хисамова, З. И. (2018). Криминологические риски применения искусственного интеллекта. *Всероссийский криминологический журнал*, *12*(6), 767–775. https://doi.org/10.17150/2500-4255.2018.12(6).767-775

Кутейников, Д. Л., Ижаев, О. А., Зенин, С. С. (2022). Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности. *Lex Russica*, *75*(2), 121–131. https://doi.org/10.17803/1729-5920.2022.183.2.121-131

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19. https://doi.org/10.1109/mtas.2004.1273467

Buresh, D. L. (2021). Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?. *Santa Clara High Technology Law Journal*, *38*(1). https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2

Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommunications Policy*, *47*(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482

Firc, A., Malinka, K., & Hanáček, P. (2023). Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*, *9*(4), e15090. https://doi.org/10.1016/j.heliyon.2023.e15090

Gates, K. A. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media*, *3*(2), 235–238. https://doi.org/10.1177/152747640200300217

Gill, P. (1997). Technostalgia: Making the future past perfect. *Camera Obscura: Feminism, Culture, and Media Studies*, *14*(1–2), 161–179. https://doi.org/10.1215/02705346-14-1-2_40-41-161

Givens, G., Beveridge, J. R., Draper, B. A., Grother, P., & Phillips, P. J. (2004). How features of the human face affect recognition: a statistical comparison of three face recognition algorithms. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2004. https://doi.org/10.1109/cvpr.2004.1315189

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management*, *24*(3), 325–335. https://doi.org/10.1177/14613557221089558

Johnson, Th. L., Johnson, N. N., McCurdy, D., & Olajide, M. M. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly*, *39*(4), 101753. https://doi.org/10.1016/j.giq.2022.101753

Jones, C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *NCJL & Tech.*, *22*(4), 777. https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Raissova, G., & Mukhamejanova, D. (2021). Nondiscrimination Policy and Privacy Protection in Case of Genetic Passport for Soldiers. *South Asian Journal of Social Sciences and Humanities*, *2*(3), 140–150. https://doi.org/10.48165/sajssh.2021.2309

Sarabdeen, J. (2022, March 11). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, *8*(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

Schweber, H. (2014). Lochner v. New York and the Challenge of Legal Historiography. *Law & Social Inquiry*, *39*(1), 242–274. https://doi.org/10.1111/lsi.12062

Shore, A. (2022). Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. *Telematics and Informatics*, *70*, 101815. https://doi.org/10.1016/j.tele.2022.101815

Sprokkereef, A. (2007, August). Data Protection and the Use of Biometric Data in the EU. In *The Future of Identity in the Information Society* (pp. 277–284). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-79026-8_19

Stepney, Ch. (2019). Actual Harm Means it is too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law. *Loyola of Los Angeles Entertainment Law Review*, *40*(1). https://digitalcommons.lmu.edu/elr/vol40/iss1/2

Zuo, K. J., Saun, T. J., & Forrest, C. R. (2019). Facial Recognition Technology: A Primer for Plastic Surgeons. *Plastic and Reconstructive Surgery*, *143*(6), 1298e–1306e. https://doi.org/10.1097/prs.0000000000005673

Сведения об авторах

Утеген Дана – заместитель директора, старший преподаватель Высшей школы права, Университет КАЗГЮУ имени М. С. Нарикбаева
Адрес: 010000, Республика Казахстан, г. Астана, Коргалжинское шоссе, 8
E-mail: d_utegen@kazguu.kz
ORCID ID: https://orcid.org/0000-0001-5296-7916

Рахметов Бауржан Жанатович – PhD в области политики и международных отношений, ассистент-профессор Международной школы экономики, Университет КАЗГЮУ имени М. С. Нарикбаева
Адрес: 010000, Республика Казахстан, г. Астана, Коргалжинское шоссе, 8
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ

Вклад авторов

Д. Утеген осуществляла составление черновика рукописи и его критический пересмотр с внесением ценных замечаний интеллектуального содержания; разработку дизайна методологии; проведение сравнительного анализа; сбор литературы; анализ законодательства Соединенных Штатов Америки и Республики Казахстан; подготовку и редактирование текста статьи; формулировку ключевых выводов, предложений и рекомендаций; оформление рукописи.
Б. Ж. Рахметов осуществлял формулирование идеи, исследовательских целей и задач; участие в научном дизайне; анализ и обобщение литературы; анализ законодательства Европейского союза и Республики Казахстан; интерпретацию частных результатов исследования; критический пересмотр и редактирование текста рукописи; интерпретацию общих результатов исследования; утверждение окончательного варианта статьи.

Конфликт интересов

Б. Ж. Рахметов является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 7 ноября 2022 г.
Дата одобрения после рецензирования – 23 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.