



International Journal of Innovative Technologies in Social Science

e-ISSN: 2544-9435

Operating Publisher
SciFormat Publishing Inc.
ISNI: 0000 0005 1449 8214

2734 17 Avenue SW,
Calgary, Alberta, T3E0A7,
Canada
+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE

USE OF ARTIFICIAL INTELLIGENCE IN FACIAL RECOGNITION
SYSTEMS AND PROTECTION OF RIGHTS

DOI

[https://doi.org/10.31435/ijitss.2\(50\).2026.5186](https://doi.org/10.31435/ijitss.2(50).2026.5186)

RECEIVED

02 March 2026

ACCEPTED

15 June 2026

PUBLISHED

22 June 2026

LICENSE



The article is licensed under a **Creative Commons Attribution 4.0 International License**.

© The author(s) 2026.

This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

USE OF ARTIFICIAL INTELLIGENCE IN FACIAL RECOGNITION SYSTEMS AND PROTECTION OF RIGHTS

Rzayeva Gulnaz Aydin

Doctor of Laws, Professor at the UNESCO Department of Human Rights and Information Law of Baku State University

ORCID ID: 0000-0001-5305-7113

ABSTRACT

The article examines the legal and practical problems encountered during the application of facial recognition systems, analyzes the violations committed during the use of these systems from the context of human rights and freedoms, and presents recommendations on resolving the issue of liability for violations. The main goal of writing the article was to interpret the mechanism of operation of facial recognition systems, which are a type of biometric technologies, in a legal context, examine empirical facts, and put forward proposals for eliminating existing problems.

Considering it necessary to determine legal prohibitions in order to prevent violations committed during the application of facial recognition systems, the author analyzed the prohibitions related to biometric technologies in the latest legal regulation in this area, the European Artificial Intelligence Act, and proposed to establish these prohibitions in national law. At the same time, according to the author's position, although the data of facial recognition systems are used in law enforcement activities, especially in criminal and administrative proceedings, it is unacceptable to evaluate this data as "irreplaceable and the most accurate evidence". It is important to subsequently verify the information provided by the system using various methods. The author substantiated his position by referring to cases of violations and discrimination that occurred in practice. The article notes that when solving the issue of liability for violations during the application of facial recognition systems, the guilt of which subject is taken into account using various types of forensic examinations based on the black box method, and the description of the act is carried out correctly by specifying the circle of subjects.

KEYWORDS

Artificial Intelligence, Biometric Technology, Facial Recognition Systems, Right to Privacy, Personal Data, Confidentiality, Legal Liability, Legal Prohibitions

CITATION

Rzayeva Gulnaz Aydin. (2026) Use of Artificial Intelligence in Facial Recognition Systems and Protection of Rights. *International Journal of Innovative Technologies in Social Science*. 2(50). doi: 10.31435/ijitss.2(50).2026.5186

COPYRIGHT

© **The author(s) 2026**. This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

Introduction

Biometric technologies are used to determine, verify or identify a person's identity based on physiological (appearance) or functional-dynamic (behavior) characteristics (European Parliamentary Research Service). It can be said that in the legislation of almost all states, when it comes to biometric information, only physiological and in some cases functional-dynamic characteristics (for example, voice) are taken as a basis. According to the Law of the Republic of Azerbaijan on Biometric Information dated June 13, 2008, physiological signs such as fingerprints and palm prints, facial image, iris and retina of the eye, voice fragment and its acoustic parameters, DNA analysis results, body dimensions, description of special features and physical defects of the body, handwriting and signature, etc. are considered biometric information (Article 1). As can be seen, there is an error in this legal determination itself. Because it is incorrect to identify a voice fragment, handwriting and signature with a physiological sign such as a fingerprint. We believe that a more precise and specific legal definition of biometric information is given in the General Data Protection Regulation (GDPR): Biometric data are personal data resulting from specific technical processing relating to

the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (Regulation (EU) 2016/679).

In accordance with Article 6 of the Law of the Republic of Azerbaijan on Biometric Information, the areas of application of biometric technologies are listed, one of which is the use of facial recognition. We aim to review the legal problems arising from the application of facial recognition technologies, as well as new prohibitive norms.

Methodology

The purpose of the research was to examine the legal and practical issues related to the use of artificial intelligence in facial recognition systems, as well as to analyze the protection of human rights and freedoms from such use. The authors used qualitative case analysis, data analysis, thematic analysis, and comparative analysis methods in order to investigate the impact of Internet access on improving human well-being and to recognize Internet access as a unique right, especially as a legal element of the right to a decent life. The research was carried out in Baku, the Republic of Azerbaijan, in 2025-2026.

Results

1. General understanding of facial recognition systems and areas of use

Among the areas where artificial intelligence is applied, facial recognition systems are very widespread. Today, as a result of using facial recognition, people can unlock their smartphones, tag Facebook photos, home security cameras can detect unwanted visitors, airlines can conduct rapid checks at airports, customers can shop without paying in automated stores, etc. There are interesting facts in this regard. For example, the famous pop singer Taylor Swift used facial recognition at her concerts to identify her audience (The Guardian, 2020). In Australia, billboards equipped with facial recognition are used to determine the demographic characteristics of buyers in the retail sector and to reveal the mood of customers. In some cities in China, facial recognition is used to identify drivers who run red lights. The number of such facts can be increased. Although the use of facial recognition systems has made everyday life easier, it has caused serious discussions, especially in the field of human rights. Because at this time the issue of protecting the right to personal integrity comes to the fore.

The areas where facial recognition technology is applied in the literature are grouped as follows:

Security: Facial recognition technology is used in security systems to increase security measures in public places such as airports, train stations, and banks.

Law enforcement: Facial recognition technology can be used by law enforcement agencies to identify suspects and locate missing persons, as well as to compare photos taken at crime scenes with databases.

Marketing: Facial recognition technology can be used in marketing to analyze customer behavior and preferences.

Social media platforms: Social media platforms use facial recognition technology to identify and tag people in photos, as well as to prevent unauthorized access.

Healthcare: Facial recognition technology can be used in healthcare to identify patients, track their medical history, and monitor the progress of treatment (Balasubramanian 2023, 6).

Facial recognition technology is considered a special type of biometric technology, in which a person's facial photo template is compared with other photo templates stored in their database and identification is performed. In a study conducted by the European Parliamentary Research Service in 2021, the mechanism of operation of facial recognition technologies was defined as follows (European Parliamentary Research Service, 2021):

- Identification - Is the image in the photo the face of a natural person?
- Identification - Who does the image in the photo belong to?
- Verification - Do the image in the photo and the image taken from the database belong to the same person?
- Classification - What group characteristics (e.g. age, gender, etc.) can be collected from the image in the photo?

This mechanism can also be applied to biometric technologies as a whole. Here, the terms identification and verification are often confused. While biometric identification answers the question "who are you", biometric verification (or authentication) asks whether you can prove who you are. For example, fingerprint and facial recognition technology used in phones is biometric authentication technology.

As for classification, the use of artificial intelligence is more widely used during classification based on biometric technologies. This does not only serve law enforcement purposes. Thus, in most cases, biometric classification does not require the identification or verification of a person's identity, but artificial intelligence simply assigns the person to a certain category. For example, whether the person is old, young, etc. In many cases, such division into categories serves to provide the person with information related to his or her area of interest.

2. Is the use of facial recognition technology legal?

To determine the legality of facial recognition technology, it is first necessary to determine whether a person's photograph is personal data. In almost all countries of the world, a photograph or facial image is considered personal data. Facial recognition technology is also not considered illegal since it is a type of personal data collection (Guidelines 05/2022). If we look at the ECtHR's (the European Court of Human Rights) experience in this regard, the Court noted that a person's image constitutes one of the main attributes of his or her identity, since it reveals the unique characteristics of the person and distinguishes the person from his or her peers (Guide on Article 8 of the European Convention on Human Rights). However, it is important to distinguish between "real-time" and "post" remote biometric identification systems. "Real-time" biometric identification systems are defined as systems that can capture biometric data based on "live" or "near-live" materials, such as video images generated by a camera or other device, and carry out comparison and identification processes immediately (or without significant delay). "Post" biometric identification systems are systems that allow the detection, comparison and identification of biometric data based on images or video images generated by video surveillance cameras or personal devices (European Parliamentary Research Service, 2021). Usually, security risks and interference with the rights of individuals (especially the right to personal integrity) arise during the operation of real-time biometric identification systems. That is why some countries already impose bans on such facial recognition systems. For example, cities such as San Francisco, Boston and Portland in the USA have banned facial recognition technology in public places (Rachel Metz, 2020). In Europe, the Artificial Intelligence Act also prohibits the use of facial photographs for no purpose (Artificial Intelligence Act, art 5).

In the Laws of the Republic of Azerbaijan on Personal Data and on Access to Information, a person's photograph or facial image is not listed as personal data. However, Article 1.1.2 of the Law on Biometric Information recognizes a facial image that allows for personal identification as biometric personal data. In this case, the application of facial recognition technologies can be considered as a method of collecting and processing personal data in our republic. We must simply take into account that we are not talking about ordinary surveillance cameras here. Because the data taken from such cameras is then identified through forensic portrait examination. Facial recognition technology covers the process of a camera recognizing a person, identifying them and detecting a certain correspondence. As we have noted, according to Article 6 of the Law on Biometric Information, the identification of a person in a crowd by video surveillance is considered legal. At the same time, paragraph 3 of the Rules for the Organization and Regulation of the Activities of Biometric Information Services by Sector, approved by Resolution No. 50 of the Cabinet of Ministers of the Republic of Azerbaijan dated April 1, 2009, regulates the identification and surveillance service based on facial images, and based on these norms, we can say that the application of facial recognition technologies in our republic is legal.

2.1. Current problems and protection of rights

The authors note a number of problems associated with facial recognition using artificial intelligence: discrimination; violations of the right to privacy; lack of accuracy; obstacles (for example, glasses, hats, etc.) and lighting; ethical issues (Adetunji 2024, 45). Most of these problems require changes in legal regulation in accordance with the requirements of the time. However, we would like to comment on the difficulties associated with the use of artificial intelligence in facial recognition in two directions: First, are there facts about artificial intelligence making mistakes in facial recognition and how the issue of legal liability will be resolved if this is the case. Second, how is personal data collected through facial recognition technologies protected.

Researchers who associate the mistakes of artificial intelligence in facial recognition with the presence of familiar faces and unfamiliar faces understand familiar faces as people we often meet in everyday life, personally acquainted with them, and celebrities and public figures. Unfamiliar faces include people we have seen for a short time and did not know before. The authors attribute the errors to unfamiliar faces (Havard

2025, 4), meaning that the AI system is better at recognizing people whose images are repeated frequently in the system. This approach may be applicable to classical recognition, when the recognition was performed by a person. Since modern facial recognition systems perform evaluations based on algorithms, the familiarity of the face image should not matter.

If we compare chronologically, the errors detected in facial recognition systems from 2016 to 2020 were more likely to be related to discrimination and incorrect comparison of facial features. For example, in 2018, Amazon's facial recognition technology called Rekognition incorrectly matched 28 members of Congress, identifying them as people who had been arrested for a crime (ACLU, 2018). Such errors occurred mainly in relation to black people.

Between 2016 and 2018, the Metropolitan Police in London deployed facial recognition technology in public spaces, and eight tests resulted in 96% “false positives,” meaning the technology incorrectly identified people passing through the area as a match to people wanted in its database and alerted the police.

Although dynamic advances in the application of technologies after 2020 have tried to eliminate the errors caused by facial recognition technologies, shortcomings still persist. In particular, cases of discrimination still persist in countries such as the United States (Criminal Legal News, 2025). There are even positions that insist on the need to stop the sale and use of facial recognition technology until the algorithms are properly checked for bias and regulations are established (Brianna Grine, 2023). Such errors in artificial intelligence systems can lead to the investigation being directed in the wrong direction during the investigation of crimes, and in many cases, even the real criminal being “missed”. Because let's face it, excessive trust and confidence of law enforcement officers in technologies can not only slow down investigative procedures, but also violate the right of individuals to effective investigation. For example, in 2021, a black man named Williams sued the Detroit police department, which had arrested him for a crime based on algorithmic identification, and as a result of the case, it was determined that the facial recognition technology had made a false identification. Therefore, the limits of legal liability in cases of violation must be clearly defined. Errors made by artificial intelligence cannot be interpreted only in the context of civil liability. Based on the facts we have listed, criminal liability should already be established in cases of unfounded accusations and arrests of a person. In this case, who will be subject to sanctions – the manufacturer or the user organization? In this case, we should pay attention to two grounds: unfounded accusations of a person, that is, insufficient examination of the evidence (at least the information from the facial recognition technology can be verified by forensic portrait examination) and the incorrect functioning of the facial recognition technology. In the first case, of course, the responsibility for the failure to properly and thoroughly examine the evidence lies with the law enforcement agency. This is not just about the investigation of criminal cases. When imposing administrative penalties for various administrative offenses (in particular, offenses for violating traffic rules, offenses related to environmental pollution, etc.), reference may be made to the data of facial recognition systems. In each case, the identification of a person by the appearance of a facial image on a video camera should be compared with other possible evidence in the case and verified by existing methods. For example, since the correct angle is not selected due to the fact that the person caught on camera is moving, the artificial intelligence system may make a false recognition. This error can be eliminated by various types of forensic examinations.

As for the lack of a proper operating mechanism for facial recognition technology, a distinction is made between a black box and a white box (Raposo 2024, 1860). Facial recognition technology works using a black box method. The black box method means that it is not necessary to know the internal mechanism of the device in order to use any technology. For this, it is enough to log in and out of the system so that it is possible to observe the operating mechanism of the device. At the same time, the fact that technology manufacturers do not fully disclose the operating mechanism of artificial intelligence systems in order to protect their intellectual property rights makes the existence of the black box method even more necessary. But is the principle of transparency violated in this case? – As one of the main principles of the Ethical Rules for Trustworthy Artificial Intelligence, the principle of transparency (explainability) requires that all processes for the application of artificial intelligence systems must be transparent, their capabilities and purposes must be clearly communicated, and the results of use must be explained as directly and indirectly as possible. In these circumstances, other disclosure measures (for example, transparent communication about traceability and system capabilities) may be required, provided that the system as a whole respects fundamental rights and freedoms. Because violations in Artificial Intelligence systems that can be traced and communicated will be immediately detected and prevented. We should also note the following three interrelated principles included in the Asilomar Artificial Intelligence Principles (Rzayeva and Ibrahimova 2020, 37-38) that should be guided by the issue of liability.

Transparency in determining harm: When Artificial Intelligence systems cause harm to humans and other animate and inanimate objects, the factors that caused the harm, the causal relationship between the act and the result, and the extent of the harm must be clearly determined;

Transparency of the trial: In the event of any violation involving Artificial Intelligence, whether by judicial or non-judicial institutions, it must be clearly determined which entity caused the violation, the guilt of all entities that are likely to be responsible must be determined, and a fair decision must be made in the end;

Liability: The manufacturer, software developer, owner of the mechanism, or other relevant entities are liable for any material or moral damage resulting from the use of artificial intelligence systems for unintended or illegal purposes or the application of artificial intelligence. The scope of liability must be measurable and the limit must be determined in advance.

The main point to be considered in resolving the issue of liability is whose fault the violation caused by the artificial intelligence system occurred. Given the plurality of subjects, victims of violations caused by artificial intelligence are faced with the task of identifying artificial intelligence systems as the source of damage and proving it. Because what constitutes a mistake in that system is often unclear. For example, if an artificial intelligence diagnostic tool makes an incorrect diagnosis, there can be no question of any obvious malfunction that could be the basis for the possibility that the algorithm is defective (Bruyne and Ooms 2025, 163). In addition, if the manufacturer presented its product with complete openness and transparency, but the user later replaced any defective element with another device not specified in the instruction manual (for example, replacing a webcam with a camera from another manufacturer), the liability will fall on the user. Taking this into account, it is important to have specialists who are able to correctly evaluate the information provided by these technologies, as well as biometric technologies in general, in order for them to function as intended, as well as those who have the skills to professionally monitor the process of working with these technologies. A study conducted by Accenture PLC identified some completely new and original jobs directly related to the use of artificial intelligence systems and classified them into three groups (Wilson, H.James, Paul R.Daugherty, Nicola Morini-Bianzino, 2017):

- Trainer – Trainer of the tone and meaning of customer language, intelligent machine interaction modeler, worldview trainer;
- Explainer – Content designer, transparency analyst, artificial intelligence strategist;
- Sustainer – Automation ethics specialist, automation economist, machine connectivity manager.

Personnel training in the listed areas will serve to eliminate existing shortcomings in a timely manner. It is no coincidence that the measures to be taken in the Artificial Intelligence Strategy of the Republic of Azerbaijan for 2025–2028 include strengthening the human resource potential in artificial intelligence and data management, and for this purpose, the launch of the Artificial Intelligence Academy in 2026-2028, the training of 500 engineers in the field of artificial intelligence, the formation of an artificial intelligence community of 3,000 people, etc. are planned to be implemented.

As we have noted, another of the current problems with the application of facial recognition technologies is related to the protection of personal data collected through these technologies. In particular, serious shortcomings arise during the cross-border transfer of the collected data. At what level of legal protection is this implemented? What part of this data will be accessible to third parties and on what grounds? Which state authorities will use this data and for what purposes? – Although many large technology companies deny it, there are numerous facts about hacker attacks on servers and databases. In 2020, the Clearview Artificial Intelligence startup, which has a database of more than three billion photos from Facebook, YouTube and Twitter, was attacked by hackers. Considering that most of its customers are US law enforcement agencies, we can conclude how many people's privacy is being intruded upon (BBC, 2020). Consequently, along with its positive aspects, the spread and power of information technologies leads to an increase in some concerns. Allowing a person to be continuously monitored, excluding the individual from the flow of information, collecting and storing unlimited personal data without the person's knowledge, and the possibility of personal data being misused for various purposes are some of the concerns and shortcomings on the agenda of the time. The increase in the number and diversity of transactions, especially in electronic environments, has made it necessary to take new measures and make regulations to protect and ensure the confidentiality of personal data. Along with respect for private and family life, the right to the protection of personal data has also begun to be legally recognized in various European countries. The issue of personal data protection was first raised within the framework of the Council of Europe in the late 1960s.

2.2. Prohibitions on biometric technologies envisaged in the European Artificial Intelligence Act

The first article of the Artificial Intelligence Act, which provides a uniform legal regulation in this area in the European space, guided by the provisions of the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law of the Council of Europe, expresses concern about the consequences of the application of artificial intelligence in the European region today. Thus, by including the expression “against the harmful effects of artificial intelligence systems and supporting innovation” and “human-centric” among the main objectives of the Act, the drafters have brought the issue of protecting fundamental human rights and freedoms into the spotlight (Artificial Intelligence Act, Art. 1).

Article 5 of the Artificial Intelligence Act specifically defines the scope of prohibited artificial intelligence systems, several of which are related to biometric technologies:

Prohibition of the use of facial images for no purpose: The placing on the market, putting into operation or use of artificial intelligence systems that create or expand databases of face recognition for no purpose from the Internet or from surveillance camera images is prohibited. Because the use of artificial intelligence systems for this purpose directly infringes on the right to personal integrity.

Prohibition of artificial intelligence systems for recognizing emotions in the workplace or in educational institutions: In accordance with the Artificial Intelligence Act, the marketing, commissioning or use of artificial intelligence systems for revealing the emotions of a natural person in the workplace or in educational institutions is directly prohibited, except in cases where the use is intended for medical or safety purposes.

Recently, Artificial Intelligence of Emotions, which has been widely used in call centers, finance, banking, medicine, etc., offers the ability to detect and predict the feelings of individuals based on biometric data (for example, tone of voice, facial features, etc.). The main point to be paid attention to here is what is understood by emotion. If we pay attention to the explanatory notes of the Act, Commentary 44 on the Act states that such emotions are obtained on the basis of biometric data: Artificial intelligence systems that determine or infer the emotions or intentions of natural persons on the basis of biometric data may lead to discriminatory results and may interfere with the rights and freedoms of the persons concerned.

In fact, the fact that such a ban is envisaged in the Artificial Intelligence Act stems from the widespread use of Artificial Intelligence of Emotions in various industries and companies in the recent past. In this regard, if we look at the facts, even human gestures are now used to detect their feelings (Gozzi, Paola).

We conducted a study on several news portals and, according to the results, the emotions of users were first used in the field of advertising. For example, the technology used by the emotional artificial intelligence company Affectiva, founded in 2009, allows the use of data transmitted from a person's phone or laptop camera to determine the customer's reactions when watching a certain advertisement. In this case, based on three expressions of customers (confusion, bored expression or, conversely, interest), artificial intelligence determines the sequence of further advertising and which customers are interested.

In general, how useful can such emotion recognition systems be both in practical and legal terms? – This already depends largely on the area where the applied system is being implemented. As Brynjolfsson says, recognizing emotions on African-American faces can sometimes be difficult for a machine trained on Caucasian faces (Meredith Somers, 2019). We should also remember that facial expressions have different meanings in different cultures. For example, a smile can mean one thing in Germany and another in Japan. Mixing these meanings can lead to poor decisions. Imagine a Japanese tourist in Berlin who needs help while browsing a store. If a store uses emotion recognition to prioritize which customers to assist, the shop assistant might mistake the customer's smiles as a sign of politeness at home, rather than an “indicator that help is not needed.” (Prudy Mark, Zealley John, Maseli Omaro, 2019). Indeed, a smile is a manifestation of various emotions. Artificial intelligence may have difficulty identifying these emotions.

Interestingly, the Artificial Intelligence Act prohibits the use of artificial intelligence systems to detect emotions in workplaces and educational institutions. This does not prevent the use of these systems in various learning programs. For example, it is possible for an English language learning program to build a conversation based on emotions. In this regard, according to the researchers who identified five capabilities of emotional artificial intelligence, emotional artificial intelligence during English language learning allows for human-like conversations, creates personalized learning content and determines tasks, etc. However, providing emotional support alone may not be enough to support student learning (Yuhan, Zhang, Jiang, Chen, Wang 2024, 106). Therefore, the analysis of emotions in such programs is only part of machine learning, and therefore it would be somewhat incorrect to evaluate it as detecting emotions in the field of education.

As for the application of emotional artificial intelligence in workplaces, it is excluded for safety purposes, in other cases, the use of artificial intelligence systems can reveal emotions is prohibited. This serves solely to ensure the inviolability of personal life. Because when artificial intelligence determines the feelings, or more precisely, the mood, of an employee, it is inevitable that it will reveal information about his personal life. This leads to the employer knowing the private aspects of his life without his consent. As the authors state, the Artificial Intelligence of Emotions violates emotional inviolability (Roemmich 2023, 2).

Prohibition of artificial intelligence systems for biometric classification of individuals: The placing on the market, putting into operation or use of artificial intelligence systems that classify individuals individually on the basis of biometric data on the basis of criteria underlying the right to equality shall be prohibited. This prohibition shall not cover the lawful labelling, filtering or classification of biometric data sets obtained in the course of law enforcement activities (for example, sorting images by hair colour or eye colour) in accordance with Union or national law (Commentary 30 on the Act).

When we look at the provisions of international norms prohibiting discrimination, we see that there are differences with the criteria laid down in the Artificial Intelligence Act. For example, classification by property status is not provided for in the Act. This can be explained by the fact that the Act covers biometric data. Personal data on property status are not biometric data. However, the question arises on what basis membership in a political party or trade union is considered biometric data. The point is that in Article 3 of the Act, biometric data means personal data resulting from special technical processing of the physical, physiological or behavioral characteristics of a natural person. When interpreting this context, membership in any political party cannot be considered biometric data. We believe that the scope of biometric classification systems for individuals should be clarified and specified.

Prohibition of artificial intelligence systems for real-time remote biometric identification in publicly accessible places for law enforcement purposes: The final prohibition provided for in Article 5 of the Artificial Intelligence Act is that the use of real-time remote biometric identification systems in publicly accessible places for law enforcement purposes is prohibited, except for use for one of the following purposes:

- targeted search for specific victims of kidnapping, human trafficking or sexual exploitation, as well as search for missing persons;
- the prevention of a specific, significant and imminent threat to the life or physical safety of natural persons, as well as a real and present or real and imminent threat of a terrorist attack;
- the localization or identification of a person suspected of having committed an offence listed in Annex II and punishable by deprivation of liberty (for a period of at least 4 years) in the relevant Member State for the purposes of operational-search activities, criminal prosecution or the execution of penalties.

Thus, when paying attention to the list of prohibitions provided for in the Artificial Intelligence Act, it can be concluded that, unlike the regulations made in previous years in Europe, this Act approaches the application of artificial intelligence systems from a broader perspective, not focusing only on issues of civil liability.

Discussion and Conclusion

As a result of the research, it was proposed that the legal definition of biometric information be precise and specific, and it was considered appropriate to define it as “personal data resulting from special technical processing of physical, physiological or behavioral characteristics of a natural person, which allows or confirms the identification of that natural person”.

The problems associated with the use of artificial intelligence in facial recognition were analyzed from two aspects: The first direction covers the resolution of violations and liability issues caused by artificial intelligence in facial recognition. The second problem is related to the protection of personal data during the application of facial recognition technologies. In order to prevent the arbitrary and easy management of personal data using artificial intelligence, the legal protection mechanisms in the existing norms should be redeveloped in order to form a more appropriate protection environment, and in this case, it is important to sequentially resolve the following issues: What rights are we trying to protect; What are the risks posed by new technologies to these rights; To what extent has the current legislation reduced these risks; What risks may the application of the current legislation cause in the current situation; What values and compromises does the current legislation imply.

We believe that the prohibitions provided for in the Artificial Intelligence Act must be established in our republic. However, there is a need to clarify the list of these prohibitions. Thus, out of the 8 prohibitions

reflected in Article 5 of the Act, the following may be considered appropriate to be established in national legislation:

- Prohibition of manipulative artificial intelligence systems;
- Prohibition of exploitative artificial intelligence systems;
- Prohibition of artificial intelligence systems for social assessment;
- Prohibition of artificial intelligence systems for the fight against predictive crime;
- Prohibition of artificial intelligence systems for recognizing emotions in the workplace or in educational institutions;
- Prohibition of artificial intelligence systems for real-time remote biometric identification in publicly accessible places for law enforcement purposes.

Regarding the other two prohibitions, we should note that the prohibition on the “inadmissibility of the use of facial images for no purpose” should not only include photographs, but also videos and audio recordings. This way, deepfake applications can be prevented from harming people.

Regarding the prohibition on biometric classification (prohibition of artificial intelligence systems for biometric classification of individuals), the prohibition of classifications based on personal data, and not on classifications that only include biometric data, should be established in legislation.

REFERENCES

1. American Civil Liberties Union. (2018, July 26). *Amazon's face recognition falsely matched 28 members of Congress with mugshots*. <https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28>
2. Adetunji, T. O. (2024). Advancements in AI-powered facial recognition for secure user authentication in e-learning environment. *Journal of Technology & Innovation*, 4(2), 44–46. <https://doi.org/10.26480/jtin.02.2024.44.46>
3. Agencia Española de Protección de Datos, & European Data Protection Supervisor. (2020). *14 misunderstandings with regard to biometric identification and authentication*. https://www.edps.europa.eu/sites/default/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_authentication_en.pdf
4. Affectiva. (n.d.). *Affectiva*. <https://www.affectiva.com/>
5. European Parliamentary Research Service. (2024). *Artificial Intelligence Act*. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)698792](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792)
6. President of the Republic of Azerbaijan. (2025). *Artificial intelligence strategy of the Republic of Azerbaijan for 2025–2028* [In Azerbaijani]. <https://e-qanun.az/framework/59218>
7. Balasubramanian, S. (2023). Facial recognition using artificial intelligence—Critical analysis and review. *International Journal of Graphics and Multimedia*, 10(1), 1–6. <https://doi.org/10.17605/OSF.IO/7MXU8>
8. BBC News. (2020, February 27). Clearview AI: Face-collecting company database hacked. <https://www.bbc.com/news/technology-51658111>
9. Grine, B. (2023). *The dangers of facial recognition technology* [Honors thesis, Syracuse University]. SURFACE. https://surface.syr.edu/honors_capstone/1580
10. De Bruyne, J., & Ooms, W. (2025). Tort liability and artificial intelligence: Some challenges and (regulatory) responses. In N. A. Smuha (Ed.), *The Cambridge handbook of the law, ethics and policy of artificial intelligence* (pp. 158–173). Cambridge University Press.
11. Criminal Legal News. (2025, February 1). *Federal facial recognition technology fails again*. <https://www.criminallegalnews.org/news/2025/feb/1/federal-facial-recognition-technology-fails-again/>
12. High-Level Expert Group on Artificial Intelligence. (n.d.). *Ethics guidelines for trustworthy AI*. European Commission. <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>
13. European Parliamentary Research Service. (2021). *Regulating facial recognition in the EU*. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf)
14. PricewaterhouseCoopers Australia. (n.d.). *Facial recognition in retail: How to balance innovation with privacy and ethics*. <https://www.pwc.com.au/digitalpulse/facial-recognition-in-retail-industry.html>
15. Gozzi, P. (n.d.). *Human emotion recognition: The latest advances in emotion AI*. Tech4Future. <https://tech4future.info/en/human-emotion-recognition-ai/>
16. European Court of Human Rights. (n.d.). *Guide on Article 8 of the European Convention on Human Rights*. https://www.echr.coe.int/documents/d/echr/guide_art_8_eng
17. European Data Protection Board. (2023). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* (Version 2.0). https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf
18. Havard, C. (2025). *When face recognition goes wrong*. Routledge.

19. Republic of Azerbaijan. (2008). *Law of the Republic of Azerbaijan on biometric information* [In Azerbaijani]. <https://e-qanun.az/framework/15144>
20. Liu, Y., Zhang, H., Jiang, M., Chen, J., & Wang, M. (2024). A systematic review of research on emotional artificial intelligence in English language education. *System*, 126, Article 103478. <https://doi.org/10.1016/j.system.2024.103478>
21. Somers, M. (2019, March 8). *Emotion AI, explained*. MIT Sloan School of Management. <https://mitsloan.mit.edu/ideas-made-to-matter/emotion-ai-explained>
22. *Next time you go through a red light in China, its growing facial recognition network may catch you out*. (n.d.). South China Morning Post. <https://www.scmp.com/tech/innovation/article/3022961/next-time-you-go-through-red-light-china-its-growing-facial>
23. Purdy, M., Zealley, J., & Maseli, O. (2019, November 18). The risks of using AI to interpret human emotions. *Harvard Business Review*. <https://hbr.org/2019/11/the-risks-of-using-ai-to-interpret-human-emotions>
24. Metz, R. (2020, September 9). Portland passes broadest facial recognition ban in the US. *CNN Business*. <https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban>
25. Raposo, V. L. (2024). When facial recognition does not “recognise”: Erroneous identifications and resulting liabilities. *AI & Society*, 39, 1857–1869. <https://doi.org/10.1007/s00146-023-01634-z>
26. European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
27. Roemmich, K., Schaub, F., & Andalibi, N. (2023). Emotion AI at work: Implications for workplace surveillance, emotional labor, and emotional privacy. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1–20). Association for Computing Machinery. <https://doi.org/10.1145/3544548.3580950>
28. Cabinet of Ministers of the Republic of Azerbaijan. (2009, April 1). *Rules for the organization and regulation of the activities of biometric information services by sector* (Resolution No. 50) [In Azerbaijani]. <https://e-qanun.az/framework/16491>
29. Rzayeva, G., & Ibrahimova, A. (2021). *Artificial intelligence, human rights and personal data security* [Textbook; in Azerbaijani]. Nurlar Publishing House.
30. The Guardian. (2018, December 13). Taylor Swift used facial recognition software to detect stalkers at LA concert. <https://www.theguardian.com/music/2018/dec/13/taylor-swift-facial-recognition-stalkers-rose-bowl-concert>
31. Council of Europe. (n.d.). *Convention for the protection of individuals with regard to automatic processing of personal data (CETS No. 108)*. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>
32. Council of Europe. (n.d.). *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. <https://rm.coe.int/1680afae67>
33. *Williams v. City of Detroit*, No. 2:21-cv-10827 (E.D. Mich.). <https://clearinghouse.net/case/44401/>
34. Wilson, H. J., Daugherty, P. R., & Morini-Bianzino, N. (2017, March 23). The jobs that artificial intelligence will create. *MIT Sloan Management Review*. <https://sloanreview.mit.edu/article/will-ai-create-as-many-jobs-as-it-eliminates/>